International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(1), pp.680-686
DOI: http://dx.doi.org/10.21172/1.81.88
e-ISSN:2278-621X

DEVELOPING SECURED FRAMEWORK FOR DATA SHARING IN PUBLIC CLOUD COMPUTING

Adesh Kumar[1]

Abstract-In cloud environment for transferring sensitive information in network data are encrypted for securing data from hackers. For secure transmission of information in public cloud network is challenging task due to increased number of threats and number of hackers since it is necessary to implement security mechanism. In this paper for improving security in cloud environment trust based security framework has been developed. Proposed framework uses both combined trust model in system manager for improving security in cloud network. Proposed combined trust model uses behavior based trust, capability based trust and identity based trust where proposed framework provides security in cloud environment. Results of the proposed framework improve performance of cloud network in various terms for performance measure in cloud environment.

Keywords –Cloud computing, data, security

1. INTRODUCTION

Cloud storage is an important service of cloud computing (Mell, P. and Grance, T, 2010). It enables people to easily share their data with friends by uploading their private data into the cloud storage, and rely on the cloud servers to provide data access control (Ke Han et al., 2016). Due to the benefits of cloud computing, increasingly more users have been using public cloud storage for data storing and sharing. However, for the widespread adoption of public cloud storage services, public cloud storage should solve the critical issue of data confidentiality (Yang Lu, Jiguo Li, 2015). This innovative paradigm has generated a significant interest in both the marketplace and the academic world, resulting in a number of notable commercial and individual cloud computing services, e.g., from Amazon, Google, Microsoft, Yahoo, and Salesforce. Top database vendors such as IBM and Oracle are adding cloud support to their databases (Bharath K. Samanthula et al., 2015).

Besides, all of these advantages of outsourced data in Cloud, there are also some significant issues. One of the major issues is the privacy of outsourced data in cloud (Jaeger, T., &Schiffman, J, 2010). i.e., the sensitive information such as e-mail, health records, and government data may leak to unauthorized users or even be hacked (Brunette, G., &Mogull, R, 2009). While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats toward users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data (Cong Wang et al., 2013). The Cloud service providers (CSPs) usually provide data security through mechanisms like firewalls and virtualization. However, these mechanisms do not protect users' privacy from the CSP itself due to remote cloud storage servers are untrusted (Pasupuleti, S. K et al., 2016).

However, for the widespread adoption of public cloud storage services, public cloud storage should solve the critical issue of data confidentiality. That is, the sensitive data must be secured from the unauthorized accesses (Liang, K et al., 2014). To protect the confidentiality of the sensitive data, a common approach is to encrypt the data before uploading them to the cloud. Since the cloud service provider (CSP) does not know the keys used to decrypt the encrypted data, the confidentiality of the data is assured. However, traditional encryption technique brings many inconveniences for data sharing between different users. To share the encrypted data with a friend, a data owner has to download his data from the storage server, decrypt them, re-encrypt them using his friend's public key and then send the re-encrypted data to his friend or re-upload the re-encrypted data to the cloud. Obviously, this strategy is extremely inefficient due to the heavy overhead at the data owner. In addition, it loses the merit of the public cloud storage. Therefore, how to flexibly share the encrypted data stored in clouds becomes a challenge (Ateniese, G et al., 2006).

In this paper proposed a combined trust model for improving the security and performance of cloud network. Proposed trust model share the data to user based on the assigned trust value in the sender. The framework developed based on threshold for trust in the cloud network. Cloud manger share the data only to the authenticated user based on the assigned trust value to individual in group. For performance evaluation proposed trust model is evaluated based on five parameters for measuring performance of proposed approach in terms of availability, reliability, data integrity and turnaround efficiency.

[1] Computer Science, SLBSRSV New Delhi India

2. RELATED WORK

This section aims to present a summary of existing review articles related to the paper secure framework for data sharing within the public cloud computing operation. The study of secure data sharing within the cloud is fairly becoming new nowadays with the advancements of growing population within the cloud. Certain related studies of cloud security and data sharing are discussed below. In the year of 2010 Sushma Karumanchi evaluated about the data transferring process in cloud environment with limited resources in terms of bandwidth, efficiency etc. In this research for storage uses Trusted Platform Module (TPM) for storing data on motherboard of computer using cryptographic technique. Incorporation of TPM provides high data storage and data sharing within the networks. Rizwana Shaikh and Dr. M. Sasikumar (2015) discussed about various aspects of cloud computing in today's scenario. To measure and analyze particular model based on cloud computing topology, basic trust model is evaluated. The basic trust model measured the security level of strength and computed the trust value. For security and validity, trust model act as a basic benchmark to measure the security of the system.

Abishek Patel and Mayankkumar (2013) studied about cloud computing as Storage as a Service (SaaS) network which is detected as good alternative to medium size business. It lacks the capital budget or the technical force to maintain and implement their data storage system. But the main consequence of this computing methodology is to maintain CIA (Confidentiality, Integrity and Authentication) to the data stored within the cloud. In this study, the Trusted Computing Group (TCG) which is the supportive hardware based root of trust is designed for interoperable platforms. Here the TPM methodology is mainly used to encrypt the data before stacking it to the cloud. The Trusted cloud architecture explains about the use of trusted gateway which acts as a mediator while providing services to the clients. Finally Kerberos authentication features are allowed to avoid replay attack, masquerading and eavesdropping within the sharing and storing network with trusted gateway.

Kavitha Margret (2013) analyzed the main problems regarding the sharing of resources within the public cloud computing environment. Based on cloud access control policies the data sharing is carried out within the dynamic group of data sharing to identify and preserve the data from the untrusted cloud. In this paper multi owner attribute authentication is designed based on data sharing scheme for dynamic group within the cloud computing topology. As a result the computation overhead is decreased with storage overhead and encryption cost. KaipingXue (2014) studied about the two main issues of group data sharing in public cloud computing environment. Because of semi-trust nature the cloud provider cannot be considered as a third party provider. The paper discussed the problems of cloud storage resources within the servers and proposed new methodologies to overcome the drawback. The formulated framework combines enhanced Tree- based group Diffie-Hellman (TGDH), proxy re-encryption and proxy signature into one protocol. This feature enables the cloud users to be in online at all the time. The result of the proposed scheme satisfies the basic requirements of the public cloud computing methodologies.

3. PROPOSED FRAMEWORK

The main aim of this research is to improve security in cloud environment using trust based management models. In this research for improving security in cloud network this research proposes a combined trust which uses behavior based trust, capability based trust and identity based trust for enhancing security.

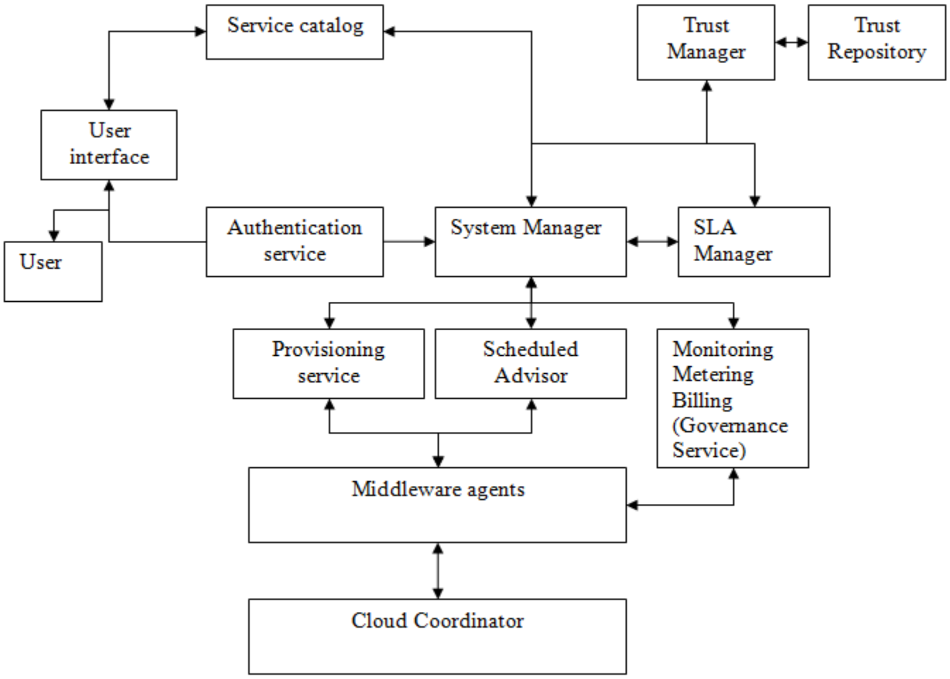

Fig 3QoS Trust based cloud computing framework

The process of browsing, security and security aspects will be involved in the User Interface component and Authentication service. The service catalog provides the list of cloud resources within the network. In cloud environment system manager perform the task of trust management in cloud environment. The system manager checks the availability of the requested cloud services with the other catalog services. It directly communicates and coordinates with other specifications of the system. The user's QoS requirement and negotiation will be managed by SLA manager. It recovers the trust values of the requested cloud resources and helps the system manager to order the cloud resources with trust values. The provisioning service cuts out the PaaS, IaaS and SaaS systems from clouds based on SLA in the form of virtualized system (Takabi, H,2010). It will finally distribute the required images. The other principal jobs of Provisioning Service are subscription, baseline configuration, notification and roles. The governance service provides the framework for access control and policy enforcement to underlying resources. Middleware agent includes sharing, creation and customization of infrastructure. The cloud resources trust values database is repository. The trust manager stores the trust values that are recovered from trust repository. Main aim of this research is to enhance the security in cloud using trust management proposed trust approach must fulfill the requirement of cloud environment.

3.1 Turnaround Time

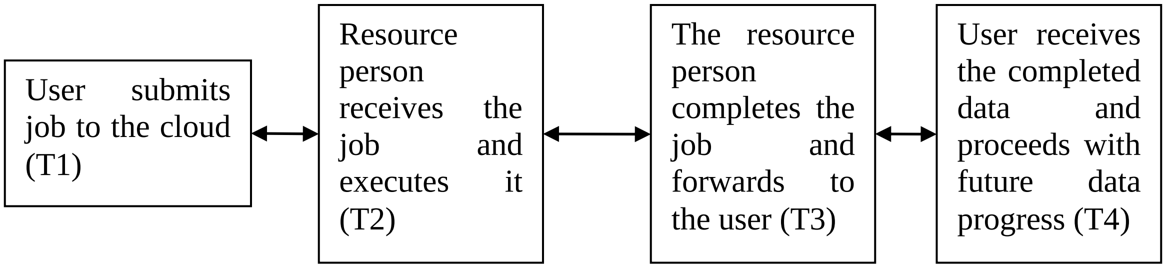
User submits job to the cloud (T1)
Resource person receives the job and executes it (T2)
The resource person completes the job and forwards to the user (T3)
User receives the completed data and proceeds with future data progress (T4)

Fig 4 Turnaround time utilization

The turnaround efficiency is the difference T4 and T1. The actual turnaround time is the accurate time between the submissions of job by the user to the completed job (Zhang, Q et al., 2010). The ratio of promised turnaround time to the actual turnaround time is turnaround efficiency. If the value of promised turnaround is greater than actual turnaround the value is 1. It incorporates throughput based on networking speed and computing power.

3.2 Data Integrity

The term security, accuracy and privacy are included in the term data integrity. Data precision comprises of accuracy and data safety comprises of security. Poor network latency may lead to data loss (Greenberg, A et al., 2008). It is the ratio of number of jobs preserved by resource to the total number of jobs which are completed successfully.

3.3 Reliability

The main important component of trust management is reliability. It is also called as success rate. The capability of the system to execute required functions under stated conditions is reliability (Ran, S, 2003). Successful completion of jobs within the particular environment based on the satisfaction of the user is briefly defined as data reliability.

3.4 Availability

Availability is the degree to which the system component or system is accessible or operational based on the required use of IEEE90 (Manuel, P, 2013). In the field of software engineering, availability is calculated as mean time between mean time to repair and failures. When a cloud source is requested to do a job, the asset is said to be unavailable based on the following issues:

a) The asset is shut down.
b) The user denies a part of the service.
c) The resource will be too much busy to process the request.

The availability is defined as the ratio of total number of jobs accepted by the resource to the total number of jobs submitted to the cloud. The trust value of the resource is defined as the sum of the weights with various cloud availability parameters. The weights are calculated based on the priority. The highest priority is given as data integrity and the lowest priority is given to turnaround efficiency. The trust is developed based on QoS service.

3.5 Cloud selection trust models

Cloudsim provides the extensible and generalized framework simulation that enables the experimentation, simulation and modeling of emerging cloud computing applications and infrastructures which permits the users to focus on particular cloud based infrastructure issue. A user presents several jobs where each job is qualified with several different potentialities of computational parameters such as hard disk memory, network parameters, ram memory and processor speed. The cloud resources are based on two models namely combined trust model and QoS model.

3.6 Combined trust model

The combined trust is the combination of three basic models such as behavior based trust, capability based trust and identity based trust. The combined trust value is calculated based on individual jobs based trust from the below equation (1).

$$CT = (a*T1) + (b*T2) + (c*T3) \tag{1}$$

Where, a is defined as behavior based trust, b is capability trust and c is identity based trust value.

Similarly T1 is the behavior based trust value, T2 is the capability based trust value and T3 is the identity based trust value (Li, M et al., 2010). For each allocated job, QoS requirements based on potential cloud resources is analyzed. From trust repository, the trust values of these clouds are retrieved. Then the values are arranged based on the priority. Finally the job is rendered to the highest cloud resource from the priority list. The user validation of behavior trust model exhibits lack of confidentiality, clarity and integrity. In order to overcome these drawbacks of behavior based trust model, QoS trust model is evaluated.

3.7 QoS trust model

The QoS model value is calculated similar to the trust value of the cloud. The value of individual positive weights is considered to be 1. Highest trust value from the list is chosen for each job as defined in equation (2) (Kim, H et al., 2010)

$$QoS = W1(TE) + W2(RE) + W3(DI) + W4(AV) \tag{2}$$

4. RESULTS AND DISCUSSION

This chapter gives the output efficiency of various cloud based methodological features. For given total amount of 10 allocations, 500 jobs were submitted to the provider. The group model consists of two database server. The database server retrieves the data from one server and stores in another server. Based on this assumption the cloud parameters are evaluated.

4.1 Turnaround time efficiency

In cloud environment where users instances were created on demand and dynamically with minimum turnaround time the administrative resource manipulation boundaries become a major issue which results with decrease in Quality of Service (QoS). The resource management process and users workflow request hosted in the cloud must be fully automated with reduced turnaround time. This allows the users to have resources with minimized duration and specified timeline.

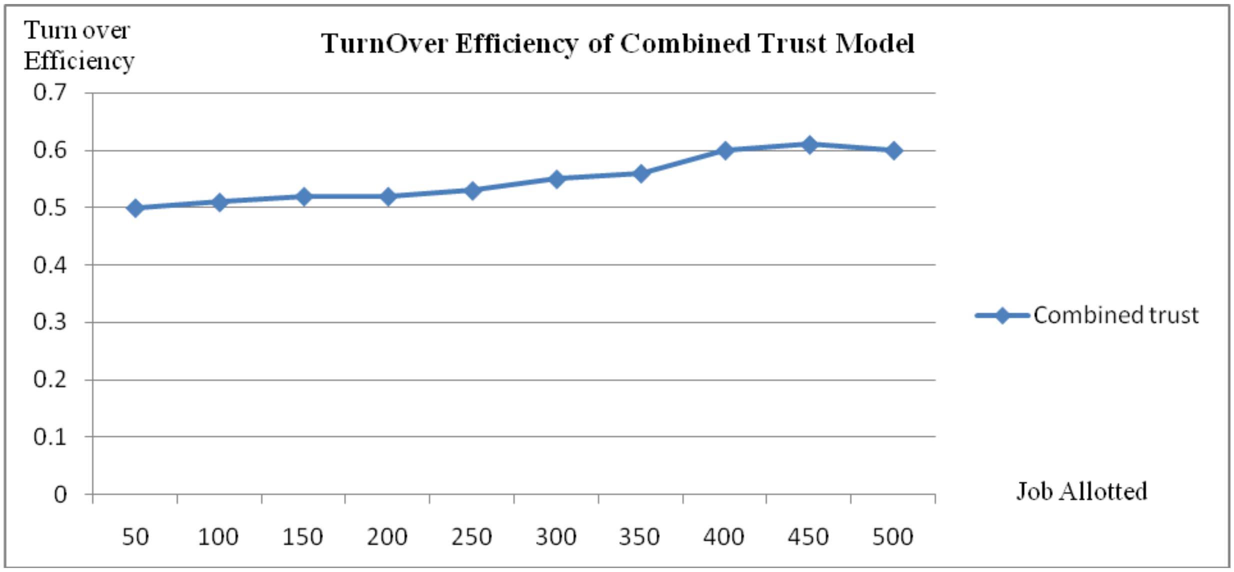

Fig 1 Comparison of turnaround efficiency with two cloud models

Figure 1 shows that the turnover efficiency will be increased based on trust values in public cloud computing. The QoS turnover is higher than combined trust with identity, behavior and capability cloud models.

4.2 Data Integrity

In cloud platform, various threats like data violation, data loss, service hijacking, malicious insiders and cloud abuse comes under the category of data integrity. Normally, in cloud storage area, the owners store their information. Using Third Party

Auditors (TPA) the users can check the data integrity of the cloud storage systems. The data integrity is also defined as the ability of the system to recover from service failures or infrastructure which gradually requires computer resources to meet mitigation descriptions and demands such as transient network issues and mis configuration. Microsoft azure platform TPA allows the users to purchase quantities when required and instantiate virtual machines. It also allows the service providers to maximize the utilization of sunk capital costs. Data segregation, user access and data quality will come under the category of data integrity as SaaS configuration will allow users to share computing resources amongst the customers.

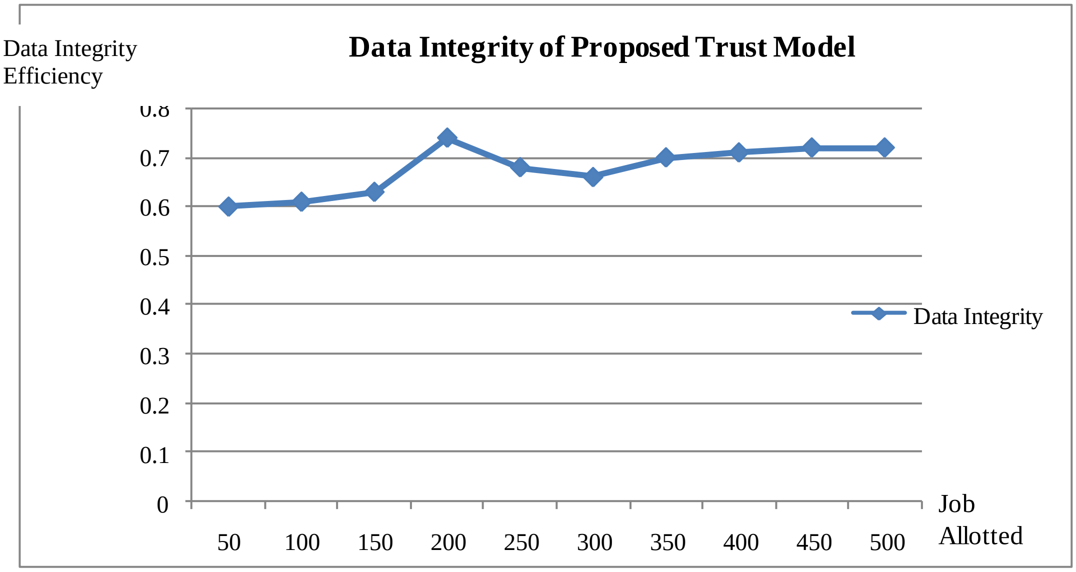

Fig 2 Comparison of data integrity with two cloud models

From Figure 2 it is analyzed that the data integrity of QoS will be greater than that of combined trust models with its performance efficiency. The jobs are measured based on privacy, security and accuracy.

4.3 Reliability

Cloud computing has the potential to solve lots of problems with restrictions of scalability. Here each job requires only one database server. Each job runs on diverse SQL queries. When the total number of database connection pools increase, it will lead to failure of the required jobs. In many cases jobs will also fail due to time-out. These problems can be solved QoS trust model. In cloud model the reliability can be increased in various ways like by properly maintaining the authentication process and authorization in place. By understanding long term capability of the system by consideration of bandwidth, migration, storage and supporting internal and external costs. The data should be encrypted initially before sharing or storing trust values in the cloud.

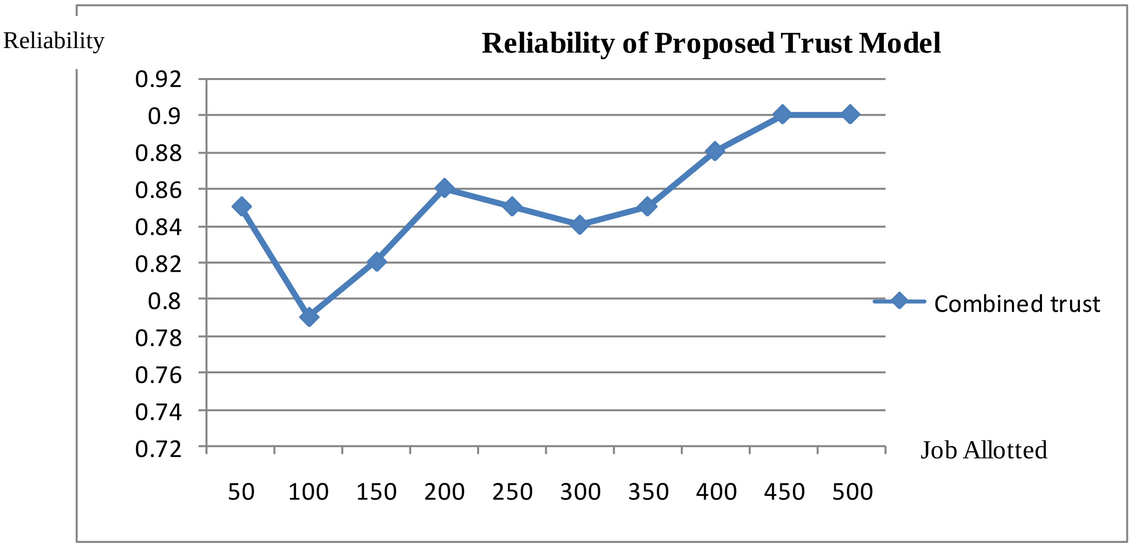

Fig 3 Comparison of reliability with two cloud models

Figure 3 describes the comparison of reliability based on two cloud based models. Sometimes the data written on files may be failed to share resources based on its performance inefficiency and priority analysis. These drawbacks can be reduced with QoS than combined trust models.

4.4 Availability

To achieve high data availability, certain cloud computing steps should be undertaken. They are built in for server failure, built in for cloud failure and built in for zone failure should be constructed. These should be carefully managed to increase the availability of the cloud resources to the users.

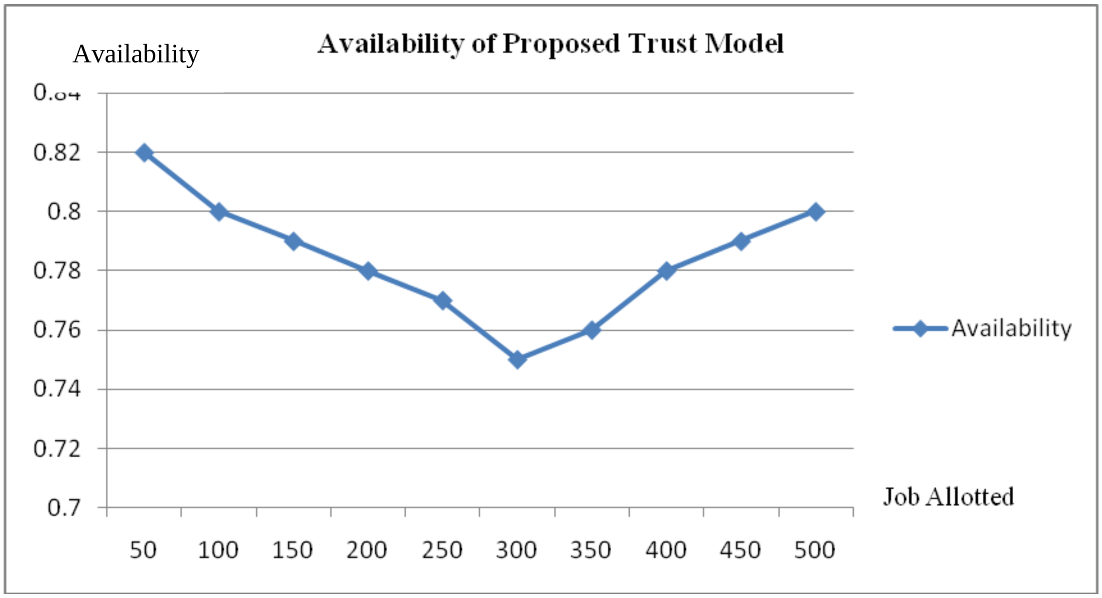

Fig 4 Comparison of availability with two cloud models

Figure 4 gives the comparison of availability with two cloud models. The QoS requirement model gives better performance of availability within the resources when compared to other cloud based models.

5. CONCLUSION

In this combined trust models for secured cloud sharing system is proposed. The credential models include combined trust models with identity, behavior and capability trust model with trust management requirements. The combined trust based framework is reviewed with its necessary functional attributes such as turnover efficiency, data integrity, reliability and availability. The methodology of cloud management is analyzed by calculating the trust values with its necessary topological equations. While sharing data between the cloud users, there may arise some intruders with certain malicious attacks like data stealing problem, cross site scripting attacks and Denial of Service attacks. These attacks can be reduced with the design of proposed trust management model. Furthermore the functionalities of the proposed architecture can be improved by using virtual switch technology for further research.

6. REFERENCES

[1] Mell, P., & Grance, T. , The NIST definition of cloud computing. Communications of the ACM, 53(6), 2010

[2] Han, K., Li, Q., & Deng, Z., Security and efficiency data sharing scheme for cloud storage. Chaos, Solitons & Fractals,2016.

[3] Lu, Y., & Li, J. A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds. Future Generation Computer Systems,2015.

[4] Samanthula, B. K., Elmehdwi, Y., Howser, G., & Madria, S., A secure data sharing and query processing framework via federation of cloud computing. Information Systems, 48, 196-212,2015

[5] Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. , Privacy-preserving public auditing for secure cloud storage. Computers, IEEE Transactions on, 62(2), 362-375,2013.

[6] Jaeger, T., & Schiffman, J., Outlook: Cloudy with a chance of security challenges and improvements. Security & Privacy, IEEE, 8(1), 77-80,2010.

[7] Brunette, G., & Mogull, R., Security guidance for critical areas of focus in cloud computing v2. 1. Cloud Security Alliance, 1-76,2009

[8] Pasupuleti, S. K., Ramalingam, S., & Buyya, R., An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. Journal of Network and Computer Applications, 64, 12-22,2016.

[9] Ateniese, G., Fu, K., Green, M., & Hohenberger, S., Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Transactions on Information and System Security (TISSEC), 9(1), 1-302006.

[10] 10.Liang, K., Au, M. H., Liu, J. K., Susilo, W., Wong, D., Yang, G., ... & Xie, Q., A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing. Information Forensics and Security, IEEE Transactions on, 9(10), 1667-1680,2014.

[11] Karumanchi, S, A Trusted Storage System for the Cloud,2010

[12] Shaikh, R., & Sasikumar, M., Trust Model for Measuring Security Strength of Cloud Computing Service. Procedia Computer Science, 45, 380-389,2015

[13] Patel, A., & Kumar, M, A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module. International Journal of Advanced Research in Computer Science and Software Engineering, 3(4),2013

[14] Margret, M. K.,Secure Policy Based Data Sharing for Dynamic Groups in the Cloud. ISSN: 2278–1323 International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 2(6),2013.

[15] Hwang, K., & Li, D, Trusted cloud computing with secure resources and data coloring. Internet Computing, IEEE, 14(5), 14-22,2010

[16] Xue, K., & Hong, P,. A dynamic secure group sharing framework in public cloud computing. Cloud Computing, IEEE Transactions on, 2(4), 459-470,2014.

[17] Takabi, H., Joshi, J. B., & Ahn, G. J, Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, (6), 24-31,2010

[18] Zhang, Q., Cheng, L., & Boutaba, R. Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications,1(1), 7-18,2010

[19] Greenberg, A., Hamilton, J., Maltz, D. A., & Patel, P, The cost of a cloud: research problems in data center networks. ACM SIGCOMM computer communication review, 39(1), 68-73, 2008.

[20] Ran, S, A model for web services discovery with QoS. ACM Sigecom exchanges, 4(1), 1-10,2003.

[21] Manuel, P, A trust model of cloud computing based on Quality of Service. Annals of Operations Research, 1-12,2013

[22] Kim, H., Lee, H., Kim, W., & Kim, Y, A trust evaluation model for QoS guarantee in cloud systems. International Journal of Grid and Distributed Computing, 3(1), 1-10,2010