Migration Letters

Volume: 21, No: S11 (2024), pp. 923-934

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

A Reliable Approach For Data Security Framework In Cloud Computing Network

Ijaz Ahmad Awan[1], Irshad Ahmed Sumra[2*], Khalid Mahmood[3], Muhammad Akram Mujahid[4], Shouzab Khan[5], Muhammad Imran Zaman[6]

Abstract

Cloud computing is one of the most discussed topics today in the field of information technology. Cloud computing is the emerging technology in the field of network based computing over the internet. Data security is one of the most crucial issue of cloud computing because we access or share our data that is available on the cloud server using the internet. In this paper, it is describing the reliable framework for designing the trusted data and security platform for the cloud computing system. In this research, a solution to the problem of secure data s[1]torage by maintaining the confidentiality and integrity of the data within the cloud is developed. Data privacy, Integrity and trust issues are few severe security concerns leading to wide adoption of cloud computing. This framework checks the authenticity of the user, who want to access the data, which is available on the cloud server. A data security framework also provides the transparency to both the cloud service provider and the cloud user there by reducing data security threats in cloud environment. This paper presents a study on security, privacy and trust issues that are very much prevalent in cloud computing environment. Furthermore, the proposed model measured the trust based on eight attributes: availability, reliability, elasticity, data integrity, adaptability, security, service response time, confidentiality authentication.

Keywords: *cloud data security, secure cloud computing, cloud security framework, Trust.*

INTRODUCTION

The modern improvement of cloud computing technology has exposed its ability to remodel the of information technology by providing new era of how computer resource is worked and purchased. It is a new computing and processing scheme which available on Internet "Cloud'. Cloud computing is a way to delivering the convenient on demand network access to a shared band of computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The Objective of the research is protection of data from various data security threats such as data privacy, data integrity, and data trust lying in cloud environment. It should also provide essential security services, such as to validate the identity, provides services, secure storage, privacy support and provide an efficient and effectively trust decision tool. Thus, the major challenge of the trust management system is ensuring the accuracy of trust information.

[1]Department of Civil Engineering, University of Engineering and Technology, Lahore, Pakistan.
[2*]Department of Computer Science, Lahore Garrison University.(Corresponding author)
[3]Department of the Information Sciences, University of Education, Lahore, Pakistan.
[4]Department of the Information Sciences, University of Education, Lahore, Pakistan.
[5]Department of Computer Science, University of Alabama at Birmingham, Birmingham AL 35294, USA.
[6]Department of Computer Science, COMSATS University Islamabad, Pakistan.

This paper address the most important procedure which to recognize and understand the type of security threats tothe trust information when developing and designing a trust management system. Current security frameworks concentrate on traditional securityaspects such as physical and system security. However, newaspects of security concern such as human-factors security, assetmanagement, and security policy management require moreelaboration. The most important issue with existing securityframeworks is trusting the cloud service provider's side. But, actually, this is not a strong assumption because attacks thatoriginate from the provider's side might not be detected.

2. Related Work

In this paper, we present those issues that are preventing people from adopting the cloud and give a survey on solutions that have been done to minimize risks of these issues. For example, the data stored in the cloud needs to be confidential, preserving integrity and available. Moreover, sharing the data stored in the cloud among many users is still an issue since the cloud service provider is untrustworthy to manage authentication and authorization? In this paper, we list issues related to data stored in cloud storage and solutions to those issues which differ from other papers which focus on cloud as general. [1]

This paper suggests an adaptive multilevel security framework based on cryptography techniques that provide adequate security for the classified data stored in cloud. The proposed security system acclimates well for cloud environment and is also customizable and more reliant to meet the required level of security of data with different sensitivity that changes with business needs and commercial conditions. [2]

This paper proposes a multilevel security framework that is adaptive for cloud environment. The adaptive multilevel security framework proposes to classify the data based on sensitivity and to provide the appropriate required level of security to the classified stored data which is a pioneering way to improve and enhance dependent security in cloud environment. The ultimate goal of this adaptive multilevel security framework is to overcome the drawbacks of any single security method or any common multiple security method for the entire data with different sensitivity which is not a prominent solution. [2]

This paper show how we secure the cloud security, privacy and reliability when a third party is processing sensitive data. In this paper, we have discussed security risks and concerns in cloud computing and broadminded steps that an enterprise can take to reduce security risks and protect their resources. We have also explained cloud computing strengths/benefits, weaknesses, and applicable areas in information risk management. This paper also covers the advantages and disadvantages in the way of cloud computing. This paper also tackles the important aspect of security concerned challenges which the researchers and authors are facing in the security of cloud computing. [3]

In this paper we attempt to review and highlight security challenges, particularly the security of data storage in a cloud environment. Also, provides some offers to enhance the security of data storage in the cloud computing systems. We propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. [4]

Unfortunately, SLA is not strictly pursued; quality of service is not accomplished. In several events, availability of administration is not up to the mark, reliability is traded off. Cloud service broker (CSB) is an entity which can resolve all these issues. The problem which we will take up in the present research paper is the selection of Quality based Cloud service provider. This procedure will be accomplished by Cloud service broker. Optimal CSP is one which fulfills all the quality requirements of user. [5]

Thus, this paper intends to fill the gap by identifying all possible factors that may affect the privacy of cloud users and develop a conceptual framework explaining these effects. The main objective of this paper is to identify the factors that may influence individual users' privacy. We expect our study to identify potential privacy issues which become more important to cloud users. [6]

In this paper we are computing on the security approaches used for increasing the level of security for the data. Purpose is to prevent from attacks, intruders and sniffing of message. Mitigation approach used in this paper works on HMAC (Hashed message authentication code), ECC and MD5. A resource pool of digitization with increasing data rate is observed. Security establishment on the basis of access control, authentication, confidentiality, integrity and encryption is achieved in this work. Experimental analysis of proposed solution concludes that very low overhead has been observed for upload and downloads service time. [7]

In this paper, a number of Cloud practitioners' perspectives are presented to calm the clients' fears against the Cloud concerns. We present a conceptual framework of three components that assist to indicate the levels of Cloud software security that should be taken into account by researchers and practitioners. This paper has faced an important issue, and provided a wide analysis of available solutions, as well as a useful fuzzy framework, helping readers to orient themselves in the field of Cloud software security. [8]

This paper proposes a security framework comprises of three main services for security, key and storage. Security is provided as a service to users. This framework consists of two security services for different types of data. Users have to choose any one security service based on their choice. Key generation is another service in the framework which provides key for security service by the way of sending the key directly to the users. Keys used for security service are not known to other cloud service in the framework. The framework protects attacks from inside and outside the cloud. It enhances the security in the public cloud environment. [9]

In this paper, we have proposed a security framework for cloud security that is able to identify security attacks, threats and risks associated to the cloud deployment. We also analyzed some major security issues of cloud service providers in the domain of integrity, authenticity and availability and discussed concrete solution for security. We believe that more effort should be emphasis by both the cloud service providers to provide a highly protected cloud system and in future, we will implement this model for cloud computing environment that can provide security to organizations as well as users of cloud services. [10]

In this paper we discussed several aspects on secure data processing in cloud computing. A framework on processing data includes data confidentiality, data authentication, availability of data and data integrity gives us the required security to process. Using this framework, the cloud computing can be more reliable to use the services that are needed by the organizations and individuals in near future. [11]

In the proposed work the trust value is estimated with the interaction between the users and the providers. With the help of the ratings provided to the cloud service providers by the users, the trustworthiness is estimated by confidence level, which is determined by the recent interaction and the interaction intensity. The competence is estimated by the parameters like security, availability, policies provided by the providers to the users. The trustworthiness and competence are combined to find the cloud service providers of user needs and the performance is estimated. [12]

In this paper, a survey of different security issues and threats are also presented. A data security framework also provides the transparency to both the cloud service provider and the cloud user

thereby reducing data security threats in cloud environment. This paper talked about various threats associated with data security in cloud computing describing briefly data integrity, data privacy and data trust associated. The model is proposed talks about three level authentication mechanisms for improving security to the data as compared to the old traditional system. Although the additional responsibilities will be added to the provider in implementation of highly secured data access network but the proposed model will minimize the issues discussed in the previous section. [13]

This research paper presented a study of trust in cloud computing, in particular the lack of user trust in cloud computing applications that hinders adoption and widespread use. The outcome of this study was the development of a framework for enhancing user trust in cloud computing applications. The significance of this study will be the enhancement of end-user trust in cloud computing, that will be seen through the improvement in cloud computing application widespread adoption and continued use. [14]

The study proposes a cloud security framework for Cloud Service Providers (CSPs) in Ghana. It adopted a number of strategies, such as experimental research achieved through integrated simulation and mixed mode research method approach, using SPSS for data analysis to execute the study expectations of proposing a new cloud security framework. It also carried out an investigation into cloud security deployment technologies, and then undertook a comparative study of these technologies. [15]

In this paper, we look at these issues from a business perspective and how they are damaging the reputation of big companies. There is a literature review on the existing issues in cloud computing and how they are being tackled by the Cloud Service Providers (CSP). We propose a governing body framework which aims at solving these issues by establishing relationship amongst the CSPs in which the data about possible threats can be generated based on the previous attacks on other CSPs. The Governing Body will be responsible for Data Center control, Policy control, legal control, user awareness, performance evaluation, solution architecture and providing motivation for the entities involved. [16]

This paper addressed the basic issues and challenges involved in the process of building trust on the cloud at IAAS level. A novel approach of trust is followed for the same. By adopting this approach trust can be built in a practical scenario. Also it can be customized as per the business model and requirements of the market. Also the paper deals with the issues that are related to identify, develop and maintain trust with the clients by providing satisfying the demands on the client side and also in the practical scenario the final report generated is also provided to the client. [17]
Trust management is one of the big challenging problems for the growth and expansion of cloud computing in different areas. Other challenging issues are security, privacy, and availability of cloud service. A cloud service can be trusted if it handles these privacy, security and availability issues. In this paper, we implemented a secure feedback based trust framework that provides Trust as a Service (TAAS).[19]

In A Frame Work Secure and Trustworthy Assessment for Credibility Based Trust Management for Cloud Service, trust is passed on as an organization (TaaS) where TMS navigates a couple coursed centers to direct reactions decentralized. Our Frame work mishandle systems to recognize reliable reactions from harmful customers and enhanced the component of this structure by expanding the SLA time allotment for each and every client, suppliers in perspective of their requesting, TMS have the commitment to manage this endeavor in light of their execution. [20]

In this paper, the cloud computing security techniques are assessed and its challenges regarding data protection are discussed. The main aim of this proposed work is to enhance the data privacy and security for the reliable cloud environment. This comparative research investigation of the existing cloud security approach regarding the data privacy and security

techniques utilized in the cloud computing. It will be useful to enhance the security of data storage in a cloud environment. [21]

This paper proposed a cloud computing security framework in the form of two approaches. The first approach advices the cloud user to keep his sensitive data at a secured region, which may be a local data center or a secured hardware. On the other hand, the second approach keeps the sensitive data encrypted at the cloud service provider while the trusted authority is the only entity that can decrypt and process these data. The second approach is better and more practical than the first approach because it keeps the sensitive data at the cloud and still secures them even against the cloud service provider's attacks. Both approaches gain benefits from using token authentication such supporting load balancing and security against certain kinds of attacks. On the other hand, the second approach costs more in terms of computations compared with the first one. [22]

We proposed a trust management system based on measurement theory for cloud computing platforms. It consists of two metrics: trustworthiness and confidence. It begins from flow measurements. We derived trust of nodes based on all the tasks running on them and all the flows they send or received. Similarly, for tasks, their trust depends on the flows and the nodes which implement the tasks. We provided a way for cloud vendors to estimate nodes and tasks' trust. [23]

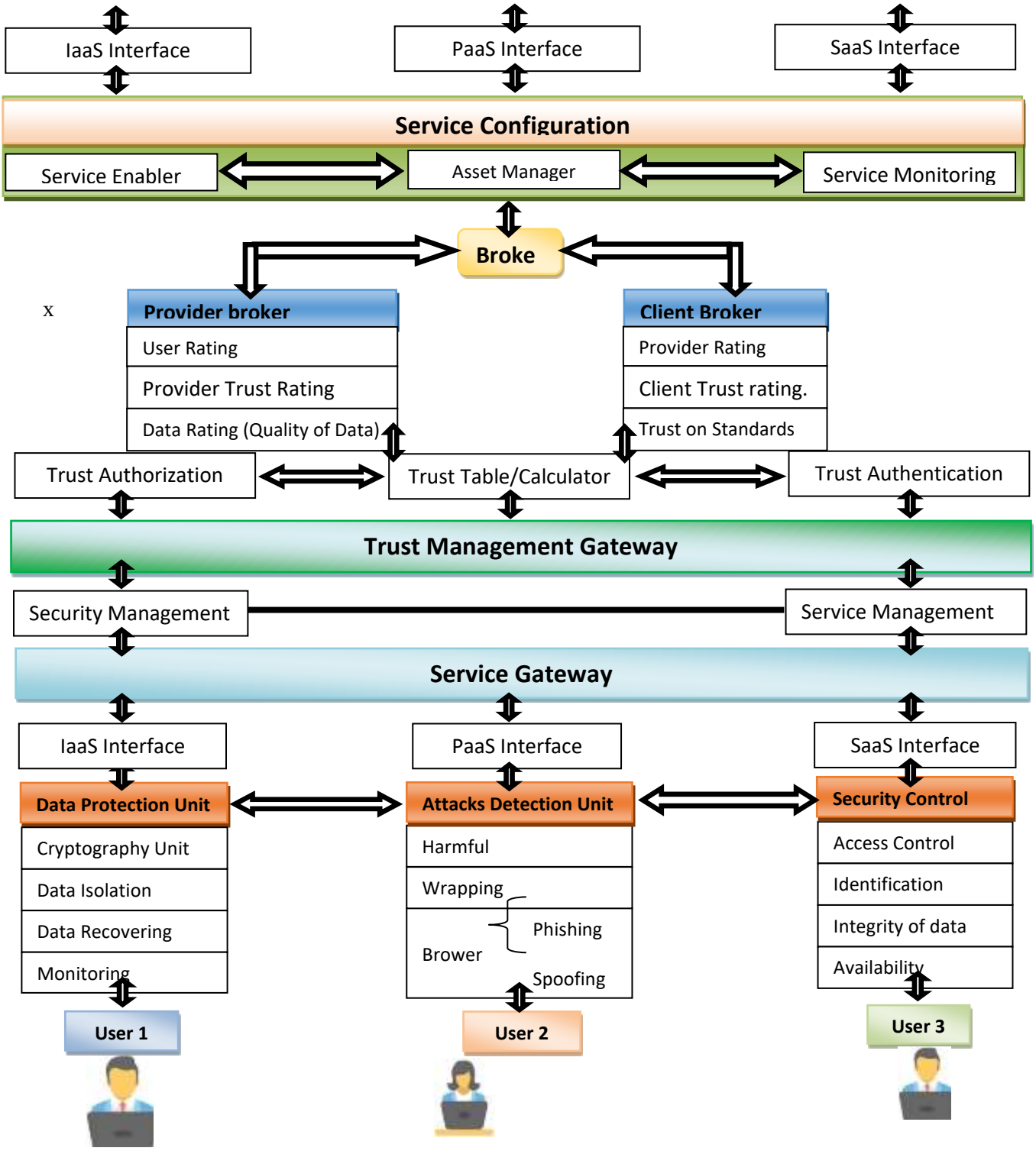
This paper introduces an auditing entity that encrypts the data before uploading as well as audit the integrity of data having been stored in cloud. In addition, the proposed system enables secure deduplication through introducing a Proof of Ownership protocol and preventing the leakage of side channel information in data deduplication. Compared with previous work, the computation by user in this system is greatly reduced during the file uploading and auditing phases. The proposed system is an advanced construction motivated by the fact that customers always want to encrypt their data before uploading, and allows for integrity auditing and secure deduplication directly on encrypted data. [24]

In this paper the trust parameters that a cloud trust model should take into account are presented together with an analysis of how these parameters can be monitored. Furthermore, the need for a trust metric, that will quantify the trust of the cloud provider to the user, has been highlighted. [25]

This process continued until the user database feedback get adequate experience. In the end, the user relied on his/her database rather than the provider or/and the third-party database. With the help of five attributes (Availability, Reliability, Integrity, Confidential and Authentication), the ARICA model gives users the ability to control their data. As a result, the model reduces the fear of customers from using cloud computing technology. [26]

3. FRAMEWORK FOR SECURE CLOUD COMPUTING

Framework for secure cloud computing is based on the security model shown above which describes the details of each component and apply the needed security technologies for implementation between components in cloud computing. This framework acts in both conditions checking security, privacy and trust. When the user sends request to cloud provider and when provider respond to user's request and pass the data through gateways. Access control process on each component is as follows:



- **A. Cloud Service Provider (CSP):** The CSP in control of significant sources and ability in construction and calculating the distributed cloud storage servers possess and direct the live obscure work out method. **Software-as–a-Service (SaaS)** model allows to provide software application as a service to the end users. **Platform-as-a-Service** offers the runtime environment for applications. It also offers development and deployment tools required to develop applications. **Infrastructure-as-a-Service** provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc

- **Service Configuration:** The **service enabler** makes provision for personalized cloud service using user's profile for the integration and interoperation. The SPML can be used to share user's profile. The **asset manager requests** user's personalized resources with SPML to cloud service provider and configuration service via VPN connection. **Service Monitoring:** An automated service monitoring systems to guarantee a high level of service performance and availability.

- **Trust Management Gateway: Due** to the cloud's nature i.e. service oriented, the trust level should also be integrated with the service. One possible approach is integrated with service, and bidirectional. **Authentication** deals with verifying the identity of an entity in the network. An identity may be a user, a resource or a service provider. **Authorization** deals with verifying the action that an entity can perform once the authentication is performed successfully. The Authorization level of the cloud resources is verified based on the type of authorization mechanism used by the service providers.

- **Calculate Trust Resource** Proposed Cloud Trust Management System (CTMS) integrated with the Trust Resource Broker computes the reputation based trust value of the cloud resources in IaaS based. The identity trust is calculated based on the security level of the resources available in the IaaS providers. We measure further trust and quality of data by using these different parameters: availability, reliability, elasticity, data integrity, adaptability, security, service response time, confidentiality authentication.

- **Service Gateway, Service Broker:** Service gateway manages network resources and VPN on the information life cycle of service broker. **Security Management:** Provides the security and privacy specification and enforcement functionality. **Service Control:** The security control component provides significant protection against security threats. Based on the provider's access control needs various access control models can be used.

- **User Service:** model allows to provide different services to select the user via Internet. **Software-as–a-Service (SaaS)**, **Platform-as-a-Service** and **Infrastructure-as-a-Service** etc.

A. Security Control

- **Access Control** authenticated and authorized user should get access of the resources. The user **identification** is usually accomplished by employing usernames and passwords when using web browser to access the cloud. **Integrity of Data** it is responsibility of Security Control to maintain the accurate computing of data that comes from integration of various files and deliver it within specified time. Availability: Availability model ensure the resources for the user in cloud.

B. Attacks Detection Unit

- **Harmful Attacks** an attack can happen in several ways on cloud and every attacker come to spoil the things on cloud. Someone randomly create a threat on cloud and someone do it by specific intention. **Wrapping** of data means attacker wrap the communication between two people in such a way that the individual feels that the data comes from original sources. Unethical **Browsing**

means where bad actions being happens such as **phishing, spoofing,** alteration of browser certificates etc.

C. Data Protection Unit:

- **Encryption** and Decryption: Information is encrypted and decrypted using a secret key (some algorithms use a different key for encryption and decryption). **Data isolation** means every individual will enjoy the separate copy data elements like maintain by any database. **Data Recovery** is ability to restore and recover the data if a disaster occurred. **Monitoring** is the process of evaluating, monitoring, and managing cloud-based services, applications, and infrastructure.

Calculate Trust Resource Broker for IaaS Providers the Proposed Cloud Trust Management System (CTMS) integrated with the Trust Resource Broker computes the reputation based trust value of the cloud resources in IaaS based. The identity trust is calculated based on the security level of the resources available in the IaaS providers. The capability trust is calculated based on the power of processor, memory, bandwidth, and storage capacity of the resources available in the IaaS providers. The behavior of the resources is calculated based on the availability, success rate and the user's feedback about the computational/storage transactions takes place in the cloud resources available in IaaS providers.

- **Preference trust** results from an interactive process between cloud users and cloud services, which depends on one or more attributes that should consist of the preference of individual users expressed using temporal, spatial, and other factors such as behavior and history. Cloud users could then perform trust evaluation on cloud services.

- **Quantification** of service trust is to establish a quantitative evaluation system to apply trust evaluation on cloud services.

1. **Availability**
   The availability is the percentage of time a customer can access the service. It is given
   $$A = \frac{t_s - t}{t_s}$$
   Where (ts) total service time

2. **Reliability**
   Reliability reflects how a service operates without failure during a given time and condition. Therefore, it is defined based on the mean time to failure promised by the Cloud provider and previous failures experienced by the users. It is measured by:
   Reliability = probability of violation × Pmttf
   $$\left(1 - \frac{n_f}{n_t} \times Pmtt_f\right)$$
   where n_f is the number of users who experienced a failure in a time interval less than promised by the Cloud provider, n_t is number of users, and $Pmtt_f$ is the promised mean time to failure. Reliability of storage can be defined in terms of durability, that is the chance of failure of a storage device.

3. **Elasticity:**
   Elasticity is defined as scalability that is how much aloud service can be scaled.
   $$El = \frac{t_m}{c_{\max}}$$
4. **Data integrity:**

Data integrity is the assurance that the information kept on the cloud can only be accessed and modified by the authorized one. It is also defined as the accuracy and consistency of the data

$$D.I = \frac{a_a(\%)}{a_b(\%)}$$

a_a =Percentage of accuracy after modification

a_b =Percentage of accuracy before modification

5. **Adaptability:**

Adaptability is the ability of the service provider to adjust changes in the service based on the customer request.

Adaptability (A)

A_d **= time taken to upgrade the service to a higher level or adopt the changes.**

6. **Security:**

Security is the major criteria for every customer. Hosting data under a third party is always a critical issue which require a stringent security policies employed by the cloud service providers. Security includes confidentiality, data integrity and privacy. Security is the assurance that cloud services are free from viruses, intrusions, spyware, attacks, and other security vulnerabilities that could put them at risk, which can be measured by

$$S = 1 - T_{sb}(t)$$

where represents security and $T_{sb}(t)$ denotes a cumulative distribution function of a random variable indicating the time until the first security breach occurs, measured in unit time.

7. **Service response time:**

To get the better performance, the service response time should be minimum that is how fast the service can be made available for usage. Service measurement can be measured by

$$TR = \sum_i \frac{t_i}{n}$$

Where t_i is the time elapsed between user's request and the response.

8. **Confidentiality Authentication**

Confidentiality is an integral component of security. It ensures that the information stored on the cloud is protected against the unintended or unauthorized access. It is also defined as the percentage of authorized access.

$$C = \frac{n_t - n_u}{n_t}$$

n_u =No. of. Unauthorized access to service

4. CONCLUSION AND FUTURE WORK

Cloud computing is a technology of fast development; however, security problems have become obstacles to make the cloud computing more popular which must be solves. This paper proposed a framework for secure cloud computing environment that identifies security

requirements, attacks, threats, concerns associated to deployment of the clouds. In this paper we discussed several aspects on secure data processing in cloud computing. A framework on processing data includes data confidentiality, data authentication, availability of data and data integrity gives us the required security to process. A trust framework is introduced based on past authorizations and present competences of a cloud service provider. Trust is one of the most important means to improve the reliability of computing resources provided in cloud environment and it plays an important role in commercial cloud environments. Trust is the estimation of capability of a cloud resource in completing a task based on reputation, identity, behavior, and availability in the context of distributed environment. With the help of eight attributes (availability, reliability, elasticity, data integrity, adaptability, security, service response time, confidentiality authentication.), the framework gives users the ability to control their data.

Using this framework, the cloud computing can be more reliable to use the services that are needed by the organizations and individuals in near future. As future work, it is proposed to incorporate additional trust metrics to evaluate the trust values of the cloud resources. The framework implementation is still in progress. The programming language used is Java and cloudsim.

REFERENCES

[1]. Sultan Aldossary , William Allen," Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016.

[2]. Sudha Devi Dorairaj and Thilagavathy Kaliannan, "An Adaptive Multilevel Security Framework for the Data Stored in Cloud Environment", Hindawi Publishing Corporation the Scientific World Journal, Volume 2015.

[3]. Prof. Ashok Deokar" Cloud Computing Security Issues, Challenges and Solution" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2017.

[4]. Mini Batra1 and Anil Arora2, "Implementing Data Security in Cloud Computing "International Journal of Advance Research in Computer Science and Management Studies, Volume 4, Issue 6, June 2016.

[5]. Ravi Khurana1 and Rajesh Kumar Bawa2 "Quality Based Cloud Service Broker for Optimal Cloud Service Provider Selection" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017).

[6]. Maher Alghali, M. A. Najwa and I. Roesnita, "A FRAMEWORK TO ASSESS PRIVACY IN CLOUD BASED SYSTEM", ARPN Journal of Engineering and Applied Sciences, FEBRUARY 2016.

[7]. Silki Jain1, Abhilasha Vyas2 "An Improved Security Framework for Cloud Environment using ECC algorithm" International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887 Volume 6 Issue I, January 2018.

[8]. Shadi A. Aljawarneh, Muneer Bani Yassein, "A Conceptual Security Framework for Cloud Computing Issues", International Journal of Intelligent Information Technologies Volume 12 • Issue 2 • April-June 2016.

[9]. S. Balamurugan1, Dr. S. Sathyanarayana2, "Enhanced Security as a Service to Protect Data in Public Cloud Storage", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 4, April 2016.

[10]. Sunil Kumar, Dr. Jayant Shekhar, Jatinder Paul Singh, "Data Security Framework for Secure Cloud Computing", International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 4, Special Issue May 2015.

[11]. L.Mohan, Dr.CH.Srinivasa Rao "A Framework for Secure data Processing in Cloud Computing" Mohan.L ,INDIA / International Journal of Research and Computational Technology, Vol.8 Issue.1 Page:06-09 ISSN: 0975-5662, Jan, 2016.

[12]. S.Rajasree, B.Lydia Elizabeth "Trust Based Cloud Service Provider Selection", International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issue 5 May 2016.

[13]. Preeti Sirohi_and Amit Agarwaly "Cloud Computing Data Storage Security framework relating to Data Integrity, Privacy and Trust" 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015). (35)

[14]. Roxanne Piderit ,Tamsanqa Nyoni "Enhancing User Trust in Cloud Computing Applications" International Conference on Information Resources, 2016.

[15]. Richard Okoampa-Larbi , Frimpong Twum , J. B. Hayfron-Acquah "A Proposed Cloud Security Framework for Service Providers in Ghana "International Journal of Computer Applications (0975 – 8887) Volume 158 – No 1, January 2017.

[16]. Harshit Srivastava1, SathishAlampalayam Kumar2, "Control Framework for Secure Cloud Computing" Journal of Information Security, 2015.

[17]. Ankita Sharma, Hema Banati "A Framework for Implementing Trust in Cloud Computing" © 2016 ACM.

[18]. Xiaohui Li,1,2 Jingsha He,1 Bin Zhao,1 Jing Fang,1 Yixuan Zhang,1 and Hongxing Liang3 " A Method for Trust Quantification in Cloud Computing Environments "Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2016.

[19]. R. N. Mrudula, Prof. V. Purushothama Raju" An Efficient Feedback Based Trust Management Framework for Cloud Computing" R N Mrudula et al, International Journal of Computer Science & Communication Networks,Vol 7(5),147-151, October-November 2017.

[20]. Shivashankar singh1, Sagarika Behera2 "A Framework, Secure and Trustworthy Assessment for Credibility Based Trust Management for Cloud Services." International Journal on Recent and Innovation Trends in Computing and Communication, May 2016.

[21]. B. Rex Cyril1, DR. S. Britto Ramesh Kumar2, "Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey," International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 04 | July-2015.

[22]. Mohammed M. Dawoud, Gamal A. Ebrahim, Sameh A. Youssef, "A Cloud Computing Security Framework Based on Cloud Security Trusted Authority" INFOS '16, May 09-11, 2016, Giza, Egypt © 2016 ACM.

[23]. Yefeng Ruan, Arjan Durresi "A Trust Management Framework for Cloud Computing Platforms", 2017 IEEE 31st International Conference on Advanced Information Networking and Applications.

[24]. DR.R.RAMACHANDRA1, SG NAWAZ 2, Y. GAYEETRI3 "A Framework for Data Integrity, Auditing in Duplicated Files in Cloud Storage "International Journal of innovative technologies, Vol.04,Issue.12, September-2016.

[25]. Zafeiroula Georgiopoulou, Costas Lambrinoudakis "Trust Management Parameters in Cloud Computing Environments" CLOUD COMPUTING 2017.

[26]. Othman Saeed1, Riaz Ahmed Shaikh2 "A User-Based Trust Model for Cloud Computing Environment" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3, 2018.