https://doi.org/ 10.48047/AFJBS.6.10.2024.5867-5874

African Journal of Biological Sciences

Research Paper Open Access

A Trust Model with Weights for Safe Cloud Data Broking and Bursting

[1]Shreyas Pagare , [2]Manoj Verma , [3]Deepesh Shrivas , [4]Ashutosh Khemriya , [5]Tanvee Nema , [6]Kirti Sharma

[1,2,3,4,5,6]Assistant Professor

[1]Department of Computer Science & Engineering

[2,3,4,5,6]Department of Artificial Intelligence and Data Science

[1,2,3,4,5,6]CDGI, Indore, india

shreyas.pagare@gmail.com , manoj.verma1511@gmail.com , deepesh2015a@gmail.com , ashutosh.khemariya07@gmail.com , tanvee.nema@cdgi.edu.in , kirti.sharma018@gmail.com

Article History
Volume 6,Issue 10, 2024
Received:24 May 2024
Accepted : 02 Jun 2024
doi: 10.48047/AFJBS.6.10.2024.5867-5874

Abstract : To control the service of cloud servers, several agencies and companies are involved in cloud infrastructure. Security is a major problem in cloud server data hosting in this setting. This paper introduces the concerns and challenges associated with data broking. In the first stage, a cryptographic solution based on the SHA1 and AES algorithms is supplied, which aids in the secure storage of data on the cloud. Furthermore, a novel trust management approach based on weighted trust is offered for design and implementation in order to address the stated concerns. The key system consists of three parties demonstrating the challenges and solutions. Furthermore, the solution is divided into two modules that gather the quality of brokerage services provided by the broker and the client. Furthermore, the selection is made between the infrastructure and the broker. In this context, behavioral information comprises the brokerage server rating supplied by server users, server response time, communication protocols utilized, and total broken session. Using these factors, a weighted trust value is calculated, which is used to govern trust levels and manage infrastructure access. The suggested model's implementation is offered utilizing JSP technology. Furthermore, their performance is measured to ensure that the suggested model is efficient and secure in attaining the work's objectives.

Keywords : Cloud Computing, Security, Bursting, Cloud Brokerage, Advance Encryption Standard, Server Trust

I. INTRODUCTION

The cloud is becoming the most popular solution among a variety of online service providers for computing and data hosting. A large number of people trust the cloud because of its speed and scalability. Cloud computing not only provides efficient computation, but also allows users to host and transport massive amounts of data. Furthermore, the services are trustworthy in terms of availability. In this context, huge corporations are hosting their information on the cloud in addition to individual users. This data may potentially comprise private and personal information.

Essentially, an infrastructure provider is not simply a service distributor; numerous intermediate brokers also resell compute and data hosting services. In this situation, a risk is recognized for both the end customer and the infrastructure provider: "what happens if the broker host is malicious" or "data leakage occurred through the broker." However, to prevent data leakage concerns in the cloud, cryptographic techniques are utilized to safeguard the data. Furthermore, the data access

policy is constantly revised. In this case, the infrastructure provider must inspect or monitor the service offered by the intermediate host. The trust of intermediary cloud service providers or brokers is explored in this study, and a weighted trust model is developed to improve broker invigilation.
Srijith K. Nair et al. [1] covers the principles of cloud bursting and cloud broking, as well as the open management and security challenges that these two models raise. It also proposes a hypothetical architectural framework capable of powering the brokerage-based cloud services presently being developed as part of the EU FP7 project OPTIMIS.

Cloud Computing

The history of computing has been marked by numerous technological advancements and changes in the way computers are built and used. Mainframes were the first computers to emerge and were considered cutting-edge technology in the mid-1960s. These machines were designed for mission-critical operations and were characterized by their large size, high cost, and centralized computing architecture. Over time, the trend shifted towards smaller, more affordable computers, such as personal computers and servers. These systems were designed to be more accessible and flexible than mainframes, allowing them to be used in a wider range of applications. The development of the internet further fueled this trend, as it allowed users to access computing resources and data remotely. Today, cloud computing has emerged as the dominant computing paradigm, offering scalable and flexible computing resources that can be accessed from anywhere in the world. Cloud computing involves the use of a network of interconnected computers that work together to provide services such as storage, computation, and management. This approach has become increasingly popular due to its cost-effectiveness, scalability, and flexibility, making it an attractive option for businesses and individuals alike. Cloud computing is widely regarded as one of the most impactful advancements in information technology in the recent past. The cloud provides computer resources and services on a pay-as-you-go basis by utilizing resource virtualization.
Today's world is becoming more digital, and cloud computing is the greatest notion for dealing with large datasets. Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) are the three types of cloud computing services. Many large IT businesses now provide strong public cloud services to consumers worldwide, ranging from individuals to enterprises. Examples include Amazon AWS and IBM Smart Cloud. Although the current development and ubiquity of cloud computing is quickly increasing, there are still disputes and reservations about using the cloud. Some of the primary problems in cloud computing adoption are data security and data privacy. as storing data in the cloud, users lose direct control over the data as compared to traditional systems [4, 5].

II. LITRACTURE SERVEY

Cloud Infrastructure

Cloud infrastructure refers to the virtual infrastructure that can be accessed or distributed over the network or the internet. It is usually delivered through Infrastructure as a Service (IaaS), which provides users with on-demand access to computing resources, such as storage, networking, and servers, without requiring physical infrastructure building. The IaaS model of cloud computing enables consumers to have an IT infrastructure that they can utilize without the need for physical infrastructure building. Cloud infrastructure provides a highly automated platform that offers computer resources, storage, and networking services to users. This approach allows users to provision and de-provision computing resources quickly, pay only for what they use, and avoid the costs and complexities of owning and managing physical infrastructure. Cloud infrastructure providers offer a web-based interface or API that allows users to manage resources. The provider is responsible for ensuring the availability, security, and performance of the platform, while the users can scale their operations rapidly and experiment with new technologies without significant upfront investments.

Components of Cloud Infrastructure

Cloud infrastructure refers to the back-end machinery found in most business data centers in a cloud computing architecture. Multisocket, multicore computers, persistent storage, and local area network equipment such as switches and routers are examples – although on a far larger scale [11].

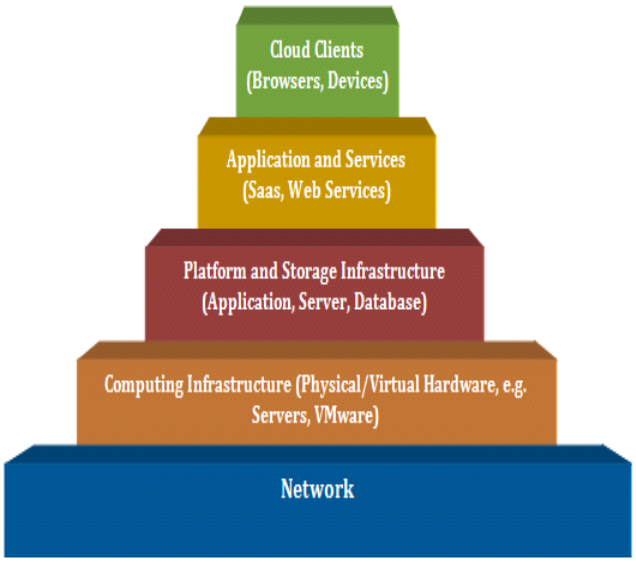


Figure 1: View of typical cloud Infrastructure

Cloud Data Storage

Data outsourcing has grown in popularity over the previous decade. The primary requirements that must be met are data storage and high performance processing. Many cloud computing service providers, such as Dropbox, Google App Engine, Amazon Simple Storage Service (AmazonS3), and others, offer these services. The benefit of putting data on cloud servers is that data owners may save money by not purchasing additional powerful servers and by not paying server administration professionals. Cloud computing is the technology utilized for internet-based development. Data storage is one of the most basic services provided by a cloud provider. Data encryption is a fundamental solution for data security, and encrypted data is uploaded to the cloud.

Issues in Cloud Storage

It is the cloud service provider's responsibility to ensure that the customer has no troubles. Cloud computing, like any other technology, has inherent drawbacks. Because it has such enormous potential for the future, it is critical to grasp the difficulties surrounding cloud computing technology. Some of

the significant challenges that this technology has are as follows:

•Trust:

Trust is a psychological condition that consists of the decision to accept vulnerability based on favorable expectations about another's intention or action [16]. It is a security extension in cloud computing technology that is classified into two categories: Hard Trust and Soft Trust. Hard trust is security-oriented, whereas soft trust is not. We can trust the system if we have control over it. Trust is characterized as a person's or thing's integrity, strength, competence, and certainty [19]. Customers must trust the cloud service provider by delivering dependable services. Any occurrences, such as hacking or service outages, would undoubtedly raise questions in the minds of customers, undermining their faith in the service provider.

•Privacy:

Cloud computing differs from traditional computing models in that it makes use of virtual computing technologies. Users' personal data is dispersed among several virtual datacenters, some of which traverse national boundaries. As a result, the risk of data leakage is quite high, and attackers may readily obtain sensitive data.

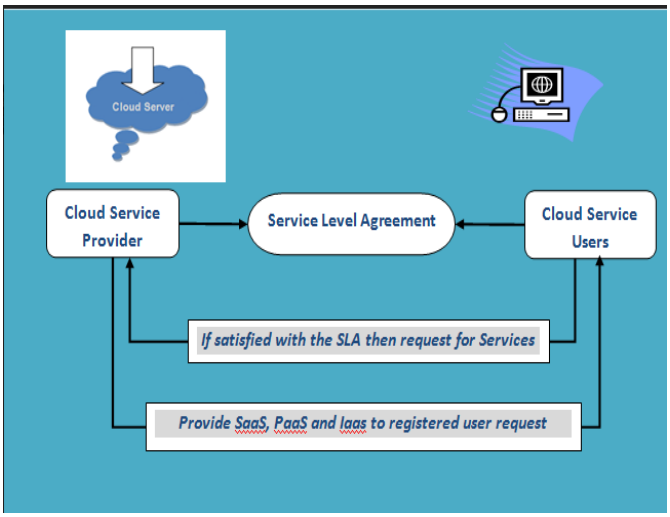
•Security:

The primary concern with cloud computing is security. Security must be implemented on two levels: user and supplier. The service provider should ensure that the server is adequately protected against any threats. Even if the service provider offers adequate security, the user must ensure that there are no dangers to their data.

Service level Agreement

A Service Level Agreement (SLA) is a contractual format that includes a description of the agreed service, level of service specifications, Quality of Service assurances, and provisions for breaches. It is an essential agreement between a service provider and another party, such as a service consumer, broker negotiator, or monitoring negotiator. The primary purpose of an SLA is to provide a clear representation of official agreements around service terms, such as performance, availability, and invoicing.

To be effective, an SLA should use a mix of broad and technical terminology, including business goals, pricing strategy, and qualities of the resources required to operate the service. According to a study by Sun Microsystems Internet Data Center Group, a well-crafted SLA establishes boundaries and prospects for service delivery, leading to increased customer acceptance levels, improved interactions, and higher service quality. An explicit SLA outlines payment and payback principles for services delivered, enabling consumers to evaluate services based on Service Level Objectives (SLO) specified in the SLA. Each element in an SLA corresponds to a Key Performance Indicator (KPI) that determines customer service quality within an organization, based on whether these indicators correspond to the Service Level Objectives (SLOs) of the agreed contract between customers.



Cloud Service Provides

Cloud service providers (CSPs) are companies or organizations that offer cloud computing services and resources to individuals, businesses, and other entities. In most cases, they operate large data centers with powerful hardware infrastructure and provide cloud-based services.

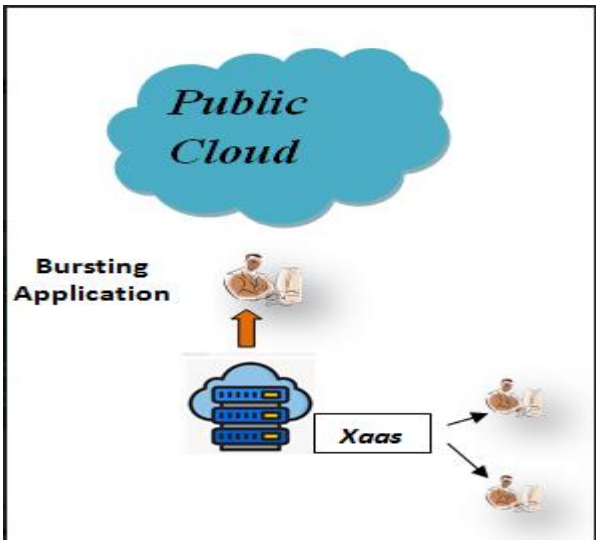
You can get everything from computing power to storage, networking, databases, analytics, machine learning, and more from cloud service providers. Pay-as-you-go services let you scale up or down your resources according to your needs.

Cloud Broker

A cloud broker is a person or company that works as a go-between for cloud service providers (CSPs) and cloud service clients. A cloud broker's major duty is to assist their clients or customers in the selection, integration, and administration of cloud services.The notion of a cloud broker arose as a result of the rising complexity and diversity of cloud services provided by various providers. Cloud brokers strive to ease the process of using cloud services by providing consumers with knowledge, direction, and value-added services.

Cloud Bursting

To accommodate rising demand, cloud bursting is a concept in cloud computing that requires dynamically shifting an application's workload from a private cloud or on-premises infrastructure to a public cloud. When an organization's proprietary infrastructure hits its limits, it can supplement its current computer resources with more capacity from the public cloud. The term "bursting" refers to the capacity to rapidly scale up resources for a brief period of time and then scale them back down after the increased demand has passed. Cloud bursting enables enterprises to withstand abrupt surges in workload or traffic without having to install and maintain extra equipment on-premises indefinitely.



In this paper, Owen Rogers et al. [35] investigate an extension of the WZH model, which was initially introduced in a theoretical research by Wu, Zhang, and Huberman. The WZH model makes use of a third-party middleman, the Coordinator, who employs a range of cloud assets to offer resources to customers at a lower cost while profiting and supporting the provider(s) in resource forecasting. The Coordinator serves as a middleman. Users acquire resources in advance from the broker using an option, which is a type of financial derivative transaction. The broker utilizes the uptake of these options contracts to determine if it should invest in purchasing resource access for an extended length of time; the resources may then be supplied to clients who want them.

As a result, Smitha Sundareswaran et al. [36] offer a unique brokerage-based architecture in the Cloud in this study, where the Cloud brokers are in charge of service selection. We create a one-of-a-kind indexing strategy for handling the information of a big number of Cloud service providers. Authors then create efficient service selection algorithms that rank and aggregate possible service providers as needed. The authors demonstrate the efficiency and efficacy of out technique in an experimental investigation using actual and fake Cloud data.

III. PROPOSED WORK

System Overview

As rapidly the cloud systems are accepted the service providers are worried for security, privacy and availability of data on cloud. The key reason behind this the different parties of involvements and interference in communication between actual host and end client. Basically in real world the infrastructure provider is not capable to distribute their service directly to all the clients some of their clients are developed on the basis of intermediate host or brokers. In these context two major concerns appears:

- preventing the information leakage and discloser on the intermediate servers
- monitoring the intermediate host that are involved in malicious activities

In order to rectify the first issue on cloud the various access policies and cryptographic security techniques are involved for data hosting, exchange and sharing. The cryptographic security is a full proof secure and low cost in implementation. For the next issue need monitoring of intermediate hosts therefore some kind new model is required for designing. In this presented work a trust model is developed that is used to supervise the intermediate host and if it is not remains secure then the infrastructure provider distribute their service through the bypass servers which are already distributing their service without any change on client's data. To demonstrate the core problem identified and also for demonstrating the proposed solution three key parties are involved in this work. First the infrastructure provider seconds the intermediate brokers and the end client who is accessing the services. Additionally on the basis of brokers behavior the trust between infrastructure server and broker is established. In this section a brief overview of the proposed model is described in next section the detailed model design is explained.

Assumption

As discussed initially to demonstrate the key issues and challenges involved in the proposed work there are three individual parties are included. The different parties and their relationships are demonstrated using figure 3.1.

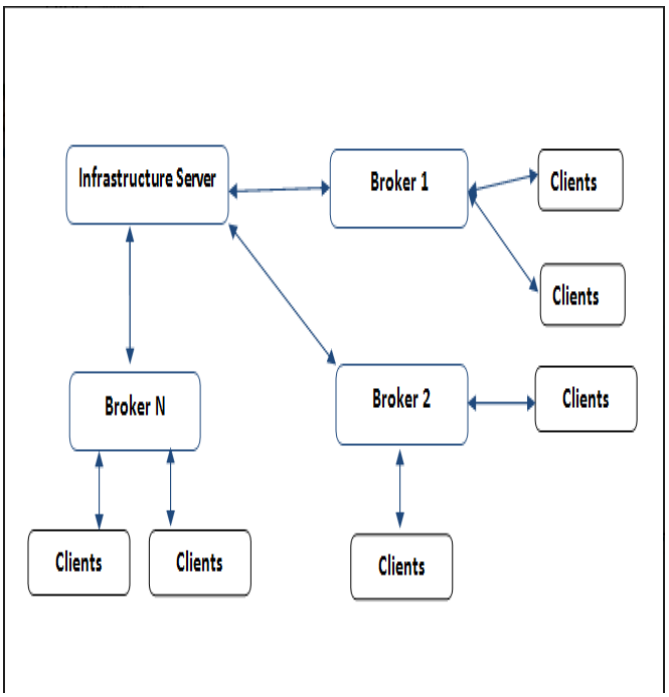


Figure 2: relationships among parties

According to the given diagram it is assumed that there is infrastructure provide which provide the server space for data storage in cryptographic format. Therefore the single storage server is used for hosting all the data arrived on that server. In order to distribute their service N number of brokers is connected through the infrastructure server. These brokers are implementing the same services which are offered by the infrastructure service provider. In this scenario we consider file upload, download and sharing services. Additionally these intermediate servers are connected through the end clients who are utilizing the services offered by the brokers. It is also assumed that for preventing the user's credentials all the user's credential's database is maintained at the infrastructure server. That also helps during failure of a particular server. In this time user can access their data through the partner servers.

Cryptographic Security

As discussed before for storing the data on cloud infrastructure the proposed model implements the cryptographic algorithm. The cryptographic data model for encryption of data is demonstrated in figure 3.2. That algorithm is used during the file upload, download and data sharing for encryption of data.
According to the diagram the original data is provided as input to the algorithm in terms of file. The data is now treated using the SHA1 hash key generator. The SHA1 algorithm is comparatively secure than MD5 thus SHA1 algorithm is used. The SHA1 algorithm generates the 160 bits of binary data as hash code.

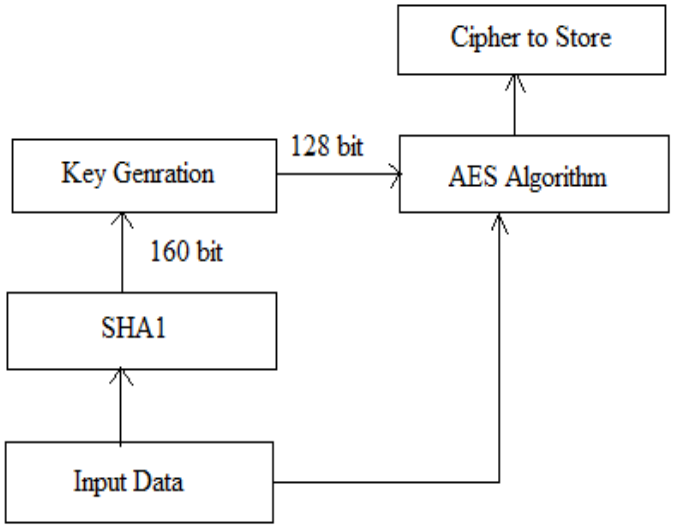


Figure 3: cryptographic algorithm

The SHA1 algorithm generates the 160 bits of binary data as hash code. This 160 bit data is produced into a key generator algorithm keep the first 128 bit from the 160 bits and remaining bits are discarded. This remaining 128 bits are working as key for AES algorithm. Thus AES algorithm accepts two parameters 128 bits of key and the input original file for encryption of the data. This encrypted data is send to server for storage purpose. The steps of above process are summarized using algorithm as:

Input: original text T

Output: cipher text C

Process:

$$K_{160}^{SHA} = SHA1.GenrateHash(T)$$

$$K_{128}^{AES} = KeyGenrator.CreateKey(K_{160}^{SHA})$$

$$C = AES.EncryptData(T, K_{128}^{AES})$$

$return\ C$

Trust Management

This section involves the discussion about the trust management between the infrastructure server and the broker server. Additionally it is also explained how the trust analysis is taken place using the behavior of broker server. Figure 3.3 shows the analysis methodology of server. In this diagram the broker server behavior is investigated by their services reliability between the broker and the end client. Additionally those factors are used between infrastructure server and broker to manage the trust. Thus the trust management is explained in two modules:

Broker Behavior Analysis

In order to evaluate the broker behavior the QoS (quality of service) parameters are considered as the key fact. Therefore there are four different quality of service parameter of broker server is computed towards the client.

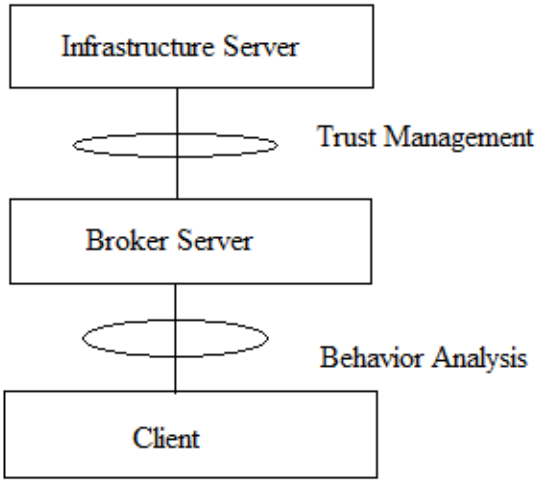


Figure 4 Broker Analysis

Server rating: that is the user input which is provided after the use of server. The rating is depends upon the user experience with the server and effectiveness of service quality. That is accepted between 0-5 according to the user experience.
Number of broken request: it the number of count when the session is broken during use of server. If a server sessions are breaking frequently it means it is not able to serve the user in better way.
Communication protocol: internet communication allows both kinds of communication protocols secure and less secure. If communication is performed on HTTPS protocols then it means the server is effective and secure on the other hand the use of HTTP protocol is less secure as compare to HTTPS. Therefore when the server usages HTTPS services then the count are assumed as 1 otherwise it is 0.
Response time of server: the response time of server is also an essential parameter for quality of server. That is the amount of time between the user request created and the page completely loaded on the user's machine. The time difference between both the events are termed here as server response time.

Trust Management

The evaluated QoS (Quality of Service) parameters between broker server and client are used in this phase to manage trust between infrastructure server and broker server. Therefore a combined weight value is computed on the basis of the broker behavior as:
Where, W is combined weight value for the broker server, R is the average client rating for the server, B is the total broken

request, P is the communication protocol used and RT is the response time of server.
Additionally the values and are the weighting factors. These values are depends upon the security system designer and can be taken between 0-1 such that .
The computed weight value of the server is used decide is the server is trusted or not. Un-trusted is not allowed continue serving more to their client and all the clients are suggested to use partner servers.

IV. RESULT ANALYSIS

Time Required for Encryption The encryption time complexity for cloud security refers to the amount of time necessary to conduct encryption using the chosen technique. That may be calculated using the formula below.

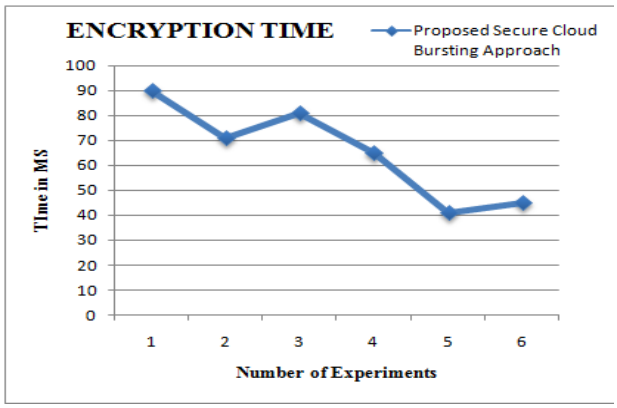


Figure 5: Encryption Time

Figure 5 depicts the encryption time of the proposed Secure Cloud Bursting Approach for primary and secondary servers, while table 5.1 contains numerical data. The X axis in this graphic represents the number of experiments to be done, and the Y axis represents the amount of time required to process the input data file on the server. The estimated time is indicated in milliseconds here.

Time Required for Decryption
The decryption time complexity of the methods is the amount of time necessary to retrieve the original data from the cipher text at the time of downloading. The algorithm's time consumption:

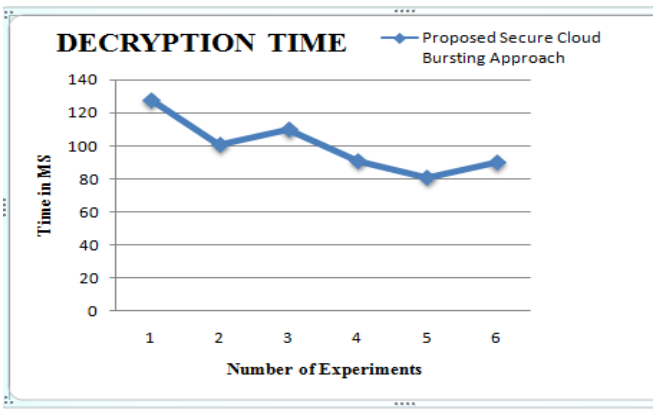


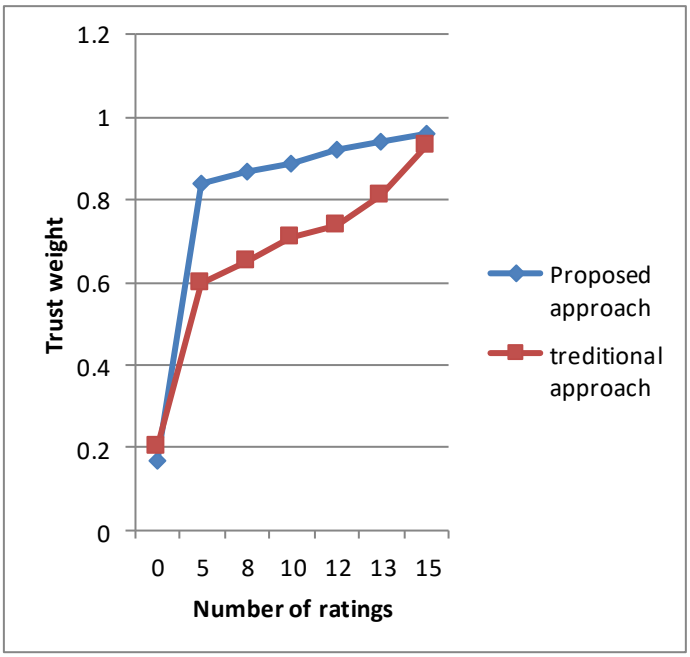
Figure 6: Decryption Time

Figure 6 and table 1 exhibit the system's acquired performance in terms of decryption time to demonstrate server trust. The time calculated in this parameter is in milliseconds (MS). The blue line depicts the performance of the suggested Secure Cloud Bursting solution to demonstrate the performance of the implemented technology. Furthermore, in Figure 5.2, the X axis displays the varied number of code executions executed to test the project's efficiency. The Y axis also shows the amount of time used in milliseconds (MS). According to the findings, the suggested algorithm's decryption time is significantly flexible, allowing for safe data file sharing utilizing a one-time password to verify the privileged user's identification.

S. No.	Proposed Secure Cloud Bursting Approach
1	128
2	101
3	110
4	91
5	81
6	90

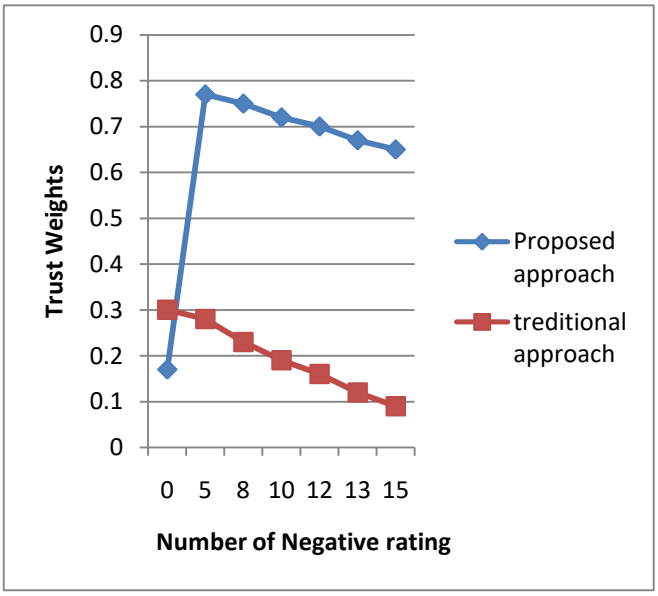
Table :1

Positive Rating and Trust Scale
This section compares trust levels based on the old approach with the new approach. In the old method, the user rating is the only element used to determine a server's legitimacy; however, in our suggested model, the user rating is part of the overall trust computation. As a result, trust is a multifactor component in the suggested strategy. As a result, the suggested approach improves judgements of server legitimacy. Figure 5.5 depicts a comparison graph between positive rating and weighted trust for both approaches. In this case, the X axis represents the number of favorable reviews, while the Y axis represents the trust estimated for decision making.



Weighted Trust and Negative Rating
The previous part highlighted the positive ratings and their influence; this section contrasts the negative ratings and trust weights as the number of negative ratings increases. Figure 5.6 depicts a comparative performance assessment of both

strategies while a server's trust rating is continually improving. Figure 5.6 depicts the number of negative ratings submitted by the end user on the X axis and the related trust scores on the Y axis. According to the collected results, the suggested approach is capable of distinguishing between negative and positive ratings by drawing a distinct line between both types of positive and negative rating servers.



V. CONCLUSION

Cloud computing is well known technology due to its efficient computing and large amount of data storage. A significant amount of organizations, institutions and individuals required such kind of efficient and scalable service. Thus the popularity of the cloud system is increased much rapidly. But to deliver the service of efficient computing and storage not only infrastructure provider various intermediate entities are also involved. In this context the security of data and privacy of data owner is a essential concern. On the other hand for securing the data service providers usages the cryptographic approaches which are acceptable but the issues with middle man is a huge security concern in entire system.

In this context the proposed work provide an effective solution for securing the data during the brokerage. In this context a three party model is demonstrated that involve a shared storage infrastructure, a middle man (broker) and the end client. The end clients are obtaining the service from the brokers and brokers are associated with the infrastructure. In order to keep in track the security and privacy a cryptographic technique is also implemented with a trust management approach. The trust management technique collects the behavioral data from the communication between broker and end client and utilized to compute weighted trust between infrastructure server and broker. The four QOS parameters are involved for measuring the trust and making decisions for the broker behavior namely server rating, umber of broken sessions, server response time and communication protocol used. Using these values a final combined weight is computed and which is used to regulate the trust between the server and broker. The proposed model is promising for brokerage service provider's monitoring and invigilation in real time. Additionally with the time the server trust values are also changing according to their service quality.

References

[1] Nair, Srijith K., et al. "Towards secure cloud bursting, brokerage and aggregation", 2010 IEEE 8th European conference on Web services (ECOWS), IEEE, 2010, pp. 189-196.

[2] Yubiao Wang; Junhao Wen; Wei Zhou "A trust-based evaluation model for data privacy protection in cloud computing" IEEE 2019.

[3] Ms. Pooja Goyal ,Dr. Sukhvinder Singh Deora. "Reliability of Trust Management Systems in Cloud Computing". Sciencegate 2022.

[4]."Data Centric Security Approach: A Way to Achieve Security & Privacy in Cloud Computing", Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018 held at Malaviya National Institute of Technology, Jaipur (India) on March 2018.

[5] Mell, P., &Grance, T. (2009, 7 10). The NIST Definition of Cloud Computing, from NIST Information Technology Laboratory, http://ww.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, retrieved on may 2011.

[6] LuitInfotech Private Limited, "What is cloud computing", available online at: http://www.luitinfotech.com/kc/what-is-cloud-computing.pdf

[7] Aarti P Pimpalkar, Prof. H.A. Hingoliwala, 'A Secure Cloud Storage System with Secure Data Forwarding', "International Journal of Scientific & Engineering Research", Volume 4, Issue 6, June-2013, pp. 3002-3010.

[8] Jineshvaria, "AWS Cloud Security Best Practices", "White Paper", November 2013

[9] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding Cloud Computing Vulnerabilities". 2011 IEEE Security and Privacy, pp. 50-57.

[10] S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "Cloud Computing Research and Development Trend," In Proceedings of the 2010 Second International Conference on Future Networks (ICFN '10). IEEE Computer Society, Washington, DC, USA, pp. 93-970.

[11] Buyya, Rajkumar, and KarthikSukumar. "Platforms for building and deploying applications for cloud computing." arXiv preprint arXiv: 1104.4379 (2011).

[12]. Phulre, A. K., Kamble, M., & Phulre, S. (2020, February). Content Management Systems hacking probabilities for Admin Access with Google Dorking and database code injection for web content security. 2nd International Conference on Data, Engineering and Applications (IDEA). Presented at the 2020 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India. doi:10.1109/idea49133.2020.9170655

[13]. Phulre, A. K., Pagare, S., & Chakrawati, A. (2022, April 29). Automated framework for web content security through content management system. 2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22). Presented at the 2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22), Nagpur, India. doi:10.1109/icetet-sip-2254415.2022.9791492

[14] BOX, B. "Cloud computing in telecommunications." Available online at:

http://www.ramonmillan.com/documentos/bibliografia/CloudComputingInTelecomunications_Ericsson.pdf