Trust based Cloud Brokerage Approach using Cryptographic and Weighed Technique

Priyanka Pandey
Computer Science and Engineering, Medicaps University, Indore
A.B. Road, Pigdamber, Rau, Indore 453441, Madhya Pradesh, India

Hitesh Kag
Assistant Professor
Computer Science and Engineering, Medicaps University, Indore
A.B. Road, Pigdamber, Rau, Indore 453441, Madhya Pradesh, India

ABSTRACT
Cloud computing is emerging as the future Internet technology due to its advantages such as sharing of IT resources, unlimited scalability and flexibility and high level of automation. Along the lines of rapid growth, the cloud computing technology also brings in concerns of security, trust and privacy of the applications and data that is hosted in the cloud environment. In this paper, we design and implemented trust based model of data during the brokerage. For preparing solution, in first step a cryptographic approach using the tiger hash and DES algorithm is provided which helps to preserve data on cloud securely. In addition to that, second step illustrate a new trust management concept using weighted trust technique. Our proposed approach is simplified yet efficient algorithm that can implemented for cloud brokerage application that strictly enforce the user trust that identified server rating. In this approach, we measure number of performance parameters which exemplify system availability in critical phase of the applications.

Keywords
Cloud Computing, Security, Bursting, Cloud Brokerage, Data Encryption Standard, Server Trust, Tiger hash.

1. INTRODUCTION
Between a number of online service providers for computing and data hosting the cloud becomes most popular service now in these days. A significant amount of users believe in cloud due to their performance and scalability. The cloud computing are not only offers the efficient computing it also enables the users to host and transfer a large amount of data. In addition of the services are reliable in terms of availability. In this context not only the individual users the large organizations are also host their information on cloud. This data may also include the private and confidential data too. On the other hand the cloud data storage is not a kind of static place to store it dynamically changing environment. And the data is moving across the network and infrastructure providers.

Basically an infrastructure provider is not only distributor of services various intermediate brokers are also reselling the computing services and data hosting services. In this context a risk for both end client and infrastructure provider is observed "what happen if broker host is malicious" or "data leakage occurred through broker". But for preventing the data leakage issues in cloud the cryptographic concepts are used to secure the data. Additionally the access policy for the data is continuously upgraded. In this context infrastructure provider need to invigilate or monitor the service provided by intermediate host.

In this project work the trust of intermediate cloud service providers or brokers are investigated and a weighted trust approach is proposed for improving the in performance of brokers.

2. PROPOSED WORK
"Methodology" implies more than simply the methods we intend to use to collect data. It is often necessary to include a consideration of the concepts and theories which underlie the methods. Unlike an algorithm, a methodology is not a formula but a set of preparations. Hence, this section provides the complete understanding about the proposed cloud busting and broker model.

3. PROBLEM DOMAIN
A problem domain is the area of expertise or application that needs to be examined to solve a problem. A problem domain is simply looking at only the topics you are interested in, and excluding everything else.

Cloud computing is an advance form of the computational domain, which includes the high performance computational engines, sharable resources, scalable with problems and solutions. The t-broker technique is a trust based scheme for measuring trust according to the behavior of cloud service providers where only the cloud user feedback is the primary factor for trust calculation. In this context for extending the concept the proposed work include different trust factors such as connection broken, communication protocol and server response time, etc.

3.1 Hypothesis
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 1.

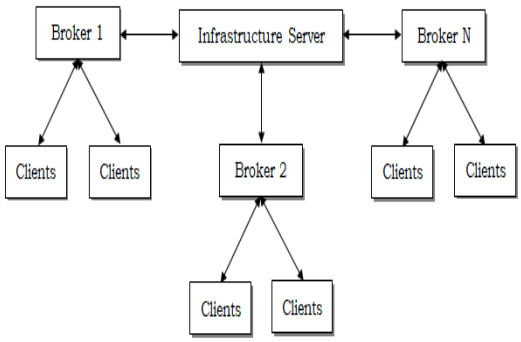

Figure 1 Interrelationship among Parties

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. This is also helps during failure of a particular server. In this time user can access their data through the partner servers.

3.2 Cryptographic Approach

As discussed before for storing the data on cloud infrastructure the proposed model implements cryptographic algorithm. The cryptographic data model for encryption of data is demonstrated in figure 2. That algorithm is used during the file upload, download and data sharing for encryption of data.

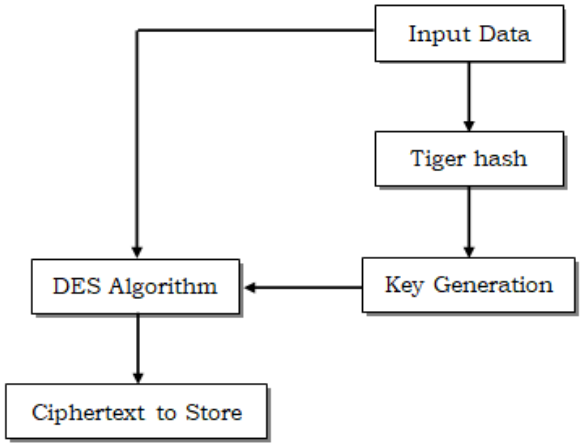

Figure 2 Cryptographic Scenario

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 tiger hash key generator. The tiger hash algorithm is comparatively secure than MD5 thus tiger hash algorithm is used. The tiger hash algorithm generates the 192 bits of binary data as hash code. This 192 bit data is produced into a key generator algorithm keep the first 64 bit from the 192 bits and remaining 128 bits are discarded. This remaining 64 bits are working as key for DES algorithm. Thus DES algorithm accepts two parameters 64 bits of key and the input original file for encryption of the data. This encrypted data is send to server for storage purpose.

This table provides the summarized steps of the process for encryption. Proposed algorithm described using is as follow:

Table 1 Encryption Algorithm

Input: Input Text File **Output:** Ciphertext
Process: $F = \text{InputTextFile}$ $\text{Key}_{\text{tigerhash (192)}} = \text{Tigerhash.generateHash (F)}$ $\text{Key}_{\text{DES (64)}} = \text{keyGenerate.makeKey (Key}_{\text{tigerhash (192)}})$ $C = \text{Ciphertext}$ $C = \text{DES. Encrypt (F, Key}_{\text{DES (64)}})$ return C

3.3 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. Additionally those factors are used between infrastructure server and broker to manage the trust. Following are the trust factor which is used for calculating trust value.

A) *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.

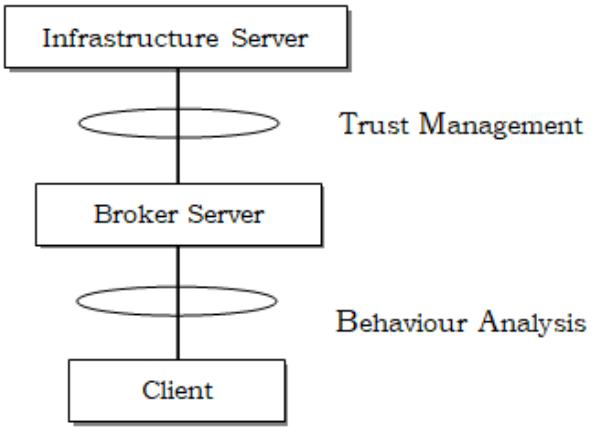

Figure 3 Broker Analysis

Server rating (Average Rating): This 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 Time: 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 (Current Protocol Value): 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 (Running Time): 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.

Particular IP Request (Total Request): In this parameter we will count total number of IP request from the particular user ID. If an individual user have to access number of time, their IP request will come to the server.

B) Trust Calculation

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:

$$W = w_1 * R + w_2 * B + w_3 * P + w_4 * RT + w_5 * IP$$

Where, W is combined weight value for the broker server, R is the average client rating for the server, B is the total broken connection, P is the communication protocol used and RT is the response time of server. Additionally the values w_1, w_2, w_3, w_4 and w_5 are the weighting factors.

These values are depends upon the security system designer and can be taken between 0-1 such that$w_1 + w_2 + w_3 + w_4 + w_5 = 1$.

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.

4. RESULT ANALYSIS

The implementation of the proposed Secure Cloud Trust Brokerage approach to estimate the trust factor of the server is described in previous section. This section provides the detailed understanding about the experimental evaluation and performance computation. Therefore essential parameters which are used for evaluation are listed` with their observations.

A. Encryption Time

The amount of time required to perform encryption using the selected algorithm is termed as the encryption time complexity for cloud security. This can be computed using the following formula.

$$\text{Time consumption} = \text{Algorithm End Time} - \text{Algorithm Start Time}$$

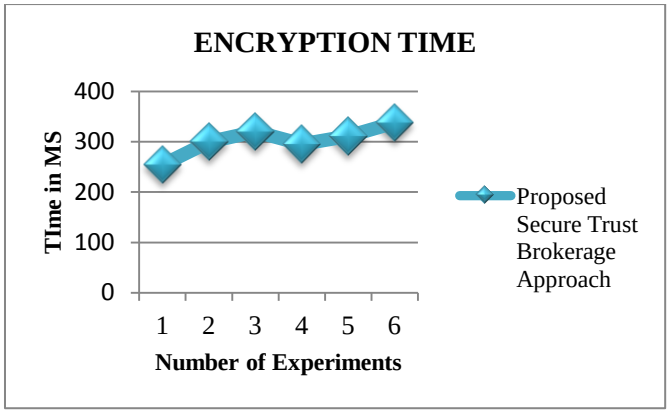

Figure 4: Encryption Time

The encryption time of the proposed Secure Cloud Bursting Approach for primary and secondary server is demonstrated using figure 4 and numeric data will arrange in table 2. In this diagram the X axis shows the different number of experimentation to be performed, and Y axis contains the amount of time consumed for processing the input data file of on server. The estimated time is given here in terms of milliseconds. Furthermore the performance of proposed system is given using blue line. Hence, in overall process for algorithm process of additionally the results shows the amount of time consumed is depends on the amount of data provided for execution. But the respective performance of the system shows their effectiveness over the traditional algorithm. The encryption time show that trust on server hum much capable to preserve user trust factor.

According to the obtained performance outcomes the proposed technique consumes less time as compared to the other related approaches which is studied in literature section.

Table 2 Encryption Time

S. No.	Proposed Secure Trust Brokerage Approach
1	254
2	300
3	320
4	295
5	311
6	338

B. Decryption Time

The amount of time required to recover the original data from the cipher text at the time of downloading is known as the decryption time complexity of the algorithms. The time consumption of the algorithm:

$$\text{Time consumption} = \text{end time} - \text{start time}$$

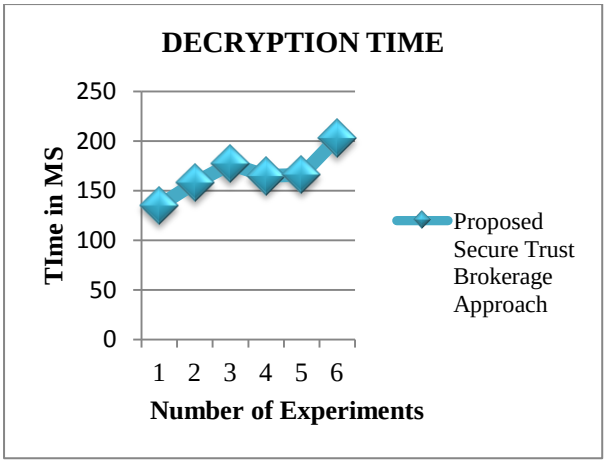

Figure 5: Decryption time

The figure 5 and table 3 shows the obtained performance of the system in terms of decryption time to demonstrate server trust. The time computed in this parameter is measured in milliseconds (MS). To show the performance of implemented technique the blue line shows the performance of proposed Secure Cloud Bursting approach. Additionally, in given figure 5, X axis shows the different number of code execution performed to check efficiency of the project. Additionally Y axis contains the amount of time consumed in milliseconds (MS). According to the observations decryption time of the proposed algorithm is much adaptable which provide secure sharing of the data file using One time password to check authentication of the privileged user.

Table 3 Decryption Time

S. No.	Proposed Secure Trust Brokerage Approach
1	135
2	158
3	177
4	165
5	166
6	203

C. Encryption Memory

The amount of main memory required to execute the algorithm with the input amount of data is known as the encryption memory. The total memory consumption of the algorithm is computed using the following formula.

$$\text{Total Consumed Memory} = \text{Total Memory} - \text{Free Memory}$$

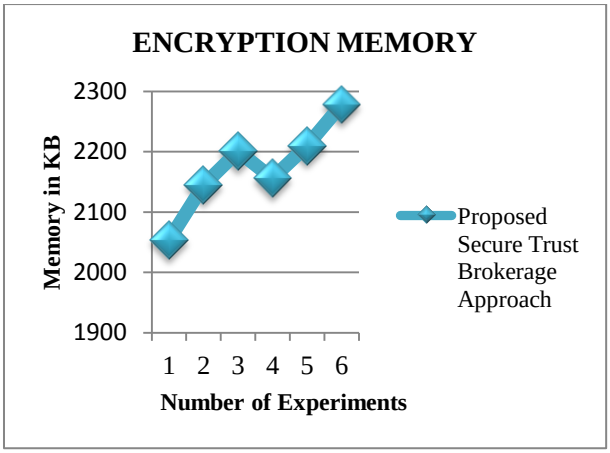

Figure 6: Encryption Memory

The figure 6 and the table 4 show the encryption memory or space complexity of encryption algorithm. In this diagram the amount of main memory consumed in terms of kilobytes (KB) is given in Y axis and numbers of different experiments are demonstrated on X-axis. According to the obtained results the proposed algorithm consumes lesser resources as performing security of cloud data with respect to the server trust value. This will ensure that user trust on server authentication is depending on the performance factor

Table 4 Memory Consumption

S. No.	Proposed Secure Trust Brokerage Approach
1	2054
2	2145
3	2201
4	2156
5	2210
6	2278

D. Decryption Memory

The amount of main memory required to recover the original file from the cipher text is known as the decryption memory consumption or the space complexity of the decryption algorithm. The decryption time required is computed using the following formula as the encryption algorithm.

$$\text{Consumed Memory} = \text{Total Memory} - \text{Free Memory}$$

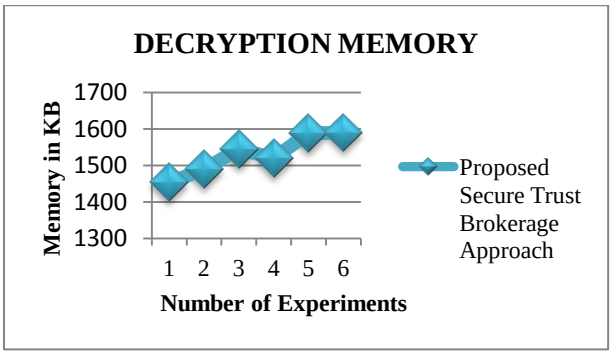

Figure 7: Decryption Memory

The figure 7 and table 5 shows the amount of main memory consumed during the data recovery in secure cloud bursting technique. In this diagram the blue line shows the performance of proposed multi server trust approach. The X axis shows the different code execution and the Y axis shows the amount of main memory consumed during the decryption in terms of kilobytes (KB). According to the results the proposed algorithm consumes less memory as and delivers original text with fewer amount of memory consumption.

Table 5 Decryption Memory

S. No.	Proposed Secure Trust Brokerage Approach
1	1453
2	1489
3	1545
4	1520
5	1588
6	1590

The section provides the conclusion and future extension of work performed in this thesis. During the implementation and design of the proposed concept the obtained facts are given here as conclusion of the work and feasible possibilities of the work is given as future extension.

5. CONCLUSION

Trust plays a crucial role in cloud environment to offer reliable services to the cloud customers. It is the main reason for the popularity of services among the cloud consumers. To achieve this, trust should be established between cloud service provider and cloud consumer. The development of cloud computing technology in various domains is huge for the last two decades. Even though it has many features but then privacy, security and trust are the most important concern. In this paper, we have analysis and implemented cloud brokerage based secure approach in which have compute trust aware security using different parameters along with cryptographic techniques.

In this context the proposed work provide an effective approach for securing the data during the brokerage. In this scenario a three party model is established that involve a shared storage infrastructure, a middle man (broker) and the end client. The end clients are gaining the service from the brokers and brokers are allied with the infrastructure. In this situation, to maintain security and privacy of the system we have implemented cryptographic algorithm with trust management approach.

6. FUTURE WORK

The main purpose of the work is to deliver a secure and efficient approach for cloud brokerage and busting. In this context, we implemented such kind of model which is secure and efficient both. In near future the following extension is suggested to work.

- ✓ This scheme can be further enhanced by uploading very large data and can do compression on those data. Also, enhance to measure the Quality of Service (QoS).
- ✓ In this paper, we are using only one type of file format i.e. text file format. In future, file format can be versatile is any type of file.
- ✓ Current system is working on the basis of weighted technique for combining the different parameters. In near future it is tried to find some kind of machine learning or soft computing approach for making decision dynamically on the basis of real time calculated parameters.

7. REFERENCES

[1] Li, Xiaoyong, Huadong Ma, Feng Zhou, and Wenbin Yao, "T-broker: A trust-aware service brokering scheme for multiple cloud collaborative services", IEEE Transactions on Information Forensics and Security 10, no. 7 (2015), pp. 1402-1415.

[2] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," 2009; http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.

[3] M. Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," Univ. California, Berkeley, Tech. Rep. UCBEECS-2009-28, Feb2009.

[4] Torry Harries, "Cloud Computing", available online at: http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf

[5] Vaishali Jain, Akshita Sharma, "A Taxonomy on Cloud Computing", International Journal of Emerging Technology and Advanced Engineering, Certified Journal, Volume 4, Issue 3, March 2014.

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

[7] BOX, B. "Cloud computing in telecommunications." Available online at: http://www.ramonmillan.com/documentos/bibliografia/CloudComputingInTelecomunications_Ericsson.pdf

[8] . 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

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