AN EFFICIENT TRUST COMPUTING SCHEME FOR IMPLEMENTING A TRUSTWORTHY AND COLLABORATIVE CLOUD SERVICE

Swati
PG Scholar, Department of IT
G.Narayamma Institute of Technology and science JNTUH, Hyderabad, Telengana, India.

Abstract— The vital task of cloud computing programme is to provide trusted services to users. The user wants to deliver their critical tasks and information to cloud data centre. So that, the burden of the cloud customer is shifted to cloud data centre. Trust has a prime role between user and cloud service provider. There are many approaches available to calculate trust value in collaborative cloud computing. In the proposed system, to provide security, data uploaded to cloud will be in encrypted format. Parallel trust computing scheme will calculate the trust. A thread will be created for each user request and will be fast as it has to evaluate the trust for single user. Trust will be determined based on successful login, and response time. The response time calculated from each request is added to matrix window, from which we can predict and recommend the best performing cloud services to user. The experimental result support practicality and success of the proposed system.

Keywords—trust, security, cloud computing, trust value, collaborative cloud computing, response time.

I. INTRODUCTION

Cloud computing uses a network of remote cloud servers to provide storage, management, and processing of data on the internet rather than a personal computer system. In simple words, the cloud users can store and access the data and programs using the internet, rather than users own computer hard drive. The conclusive target of cloud computing is to provide infrastructure, platform, and

A. Bhima Sankaram
Assistant Professor, Department of IT
G.Narayamma Institute of Technology and Science JNTUH, Hyderabad, Telengana, India.

software services at minimal cost. The user can also scale up and down their demands on a payment basis [1].

In collaborative computing, the data and programs are stored on a central cloud server, from where they can be distributed and acquired by other users using cloud computing. In collaboration computing, the resources are completely distributed, virtualized and are heterogeneous. There are many benefits of collaborative computing, namely better organization, better access to big files, real time updates [2].

With the advancement of collaborative computing, cloud users can transport their important tasks and information to the cloud datacenter to lessen their burden. The cloud provider store and processes the task on behalf of the user and supply the outcome to the cloud customers.

As, the cloud customers are storing their information to a third party cloud data site, the security concerns have been raised. To reduce the issues of a large number of users, multiple numbers of trust factors should be provided such as security, availability, and reliability. It is the authority of third party cloud data sites to store the resources and provide the response to the user securely and efficiently.

Trust is more than security. From a cloud consumer's point of view, providing trust has the following benefits:

1. Increased security: the potential to take precautions against unauthenticated behaviour.
2. Increased quality of service (QoS): the power to provide a secure service as stated by the SLA [3].

There are many methods to calculate trust but not sufficient to quantify today's big data as multiple number of users are requesting their data and the cloud has to calculate trust for each request and recommend to user.

II. RELATED WORKS

In this paper: T-Broker is a broker which is an intermediary between cloud provider and service user for managing trust and scheduling resources. Soft sensors are going to monitor real time resources for dynamic services behavior and social feedback. Hybrid and adaptive trust model is used to compute the trust by combining dynamic service behavior and social feedback. Maximization deviation practice is used to compute direct trust from the dynamic services behavior unlike traditional methods where attributes of trust are weighted manually or subjectively. This method has faster convergence then the earlier approach. T-Broker uses hybrid and adaptive trust model which combines direct trust (first hand) and indirect trust (social feedback). In current studies, hybrid model either ignores the problem or uses manual or subjective methods to assign weights for the computation of trust [3]. Importance of resource and reputation management: Resources are distributed geographically and utilization of resources and availability of resources dynamically changes. In collaborative cloud computing, different nodes have different QoS in resource provisioning. It may provide low QoS because of system problem such as, insufficient cooling, not willing to provide high QoS to save cost, attacked by viruses etc. Therefore, resource management needs reputation management to measure reputation value based on the evaluations made by others about the performance in selecting the trustworthy services. In previous studies, these two issues were addressed separately and simply combining the issues generate double overhead. Previous resources and reputation methods are not efficient. Therefore, this paper proposes collaborative cloud computing platform, Harmony that is going to integrate resource and reputation management. The contribution can be summarized as: Evaluate reputation of multiple resources by indexing resource information and reputation of each type in same directory node. It becomes easy to access information and reputation of available resources. Client is going to choose the resource based on QoS requirement such as price, distance, storage, efficiency etc. Client pays to resource provider for the resource.

Harmony enables node to adaptively adjust price to maximize profit, maintain reputation and avoid overload.

Drawbacks of this paper: Simply building and combining resource management and reputation management generate high overhead. Previously, in reputation management the method assigns one reputation value for each node for all of its resources. Previously, in resource management, assume single QoS demand of users, such as security and efficiency. Security (overload) oriented reputation management selects one with highest reputation management whereas organization (small success rate) oriented management selects one with highest accessible resources [4]. In this paper, there is high overhead and low dependability.

Limited work on resource efficiency: most of works are unsuccessful to examine the problem of resource constraints of nodes or used complex algorithms to evaluate the trustworthiness of the nodes. Limited work focused on dependability. Existing system, trust management system collects the feedback then aggregate to yield global reputation for the node that can be used to evaluate global trust degree (GTD) of the node. But in WSN, there is large number of malicious nodes. Feedback from these nodes will yield incorrect evaluation. Therefore previous studies lack to solve problem of unauthorized feedback, which influence the dependability feedback accessibility [5].

III. SYSTEM ANALYSIS

Existing Method:

In collaborative computing, providing trust to the cloud consumers is composed of three stages:

1. Real time scanning of data: A scattered and commutable architecture for big data is developed. The real time data is extracted from this scattered and commutable architecture. The agents collect the quality related data and security related data.
2. Trust calculation: Based on big data monitoring by the agents, a high speed and low overhead trust evaluating procedure is build. It uses time window and time decay functions to calculate the trust. By using parallel calculating scheme, the speed of evaluating trust is increased using this architecture.
3. Match making: The cloud resources are provided to the cloud consumers based on trust value. Therefore, supplying of resources to the cloud consumers are directly proportional to the trust values calculated.

The agents in this architecture have following features:

1. Real time scanning of data
2. Pre processing the real time data
3. Trust degree mining of the data
4. Access control based on the trust
5. Authorization

Modules of the existing system:

1. Communication and agent management module
   - I. Cloud service connection and adaptation: This module collects and indexes all the information of resources and form a single set of API. Therefore, the cloud customer needs to be conscious about one set of API.
   - II. Agents publish and agent based data perceiving: The agents are dispersed in remote sites and examine the real time behaviour incorporating security related information and QoS related information.

   If a new version of agent is developed, it is the job of this module to publish the latest version to all the agent managers.
2. Cloud resources management module:

   All the resource information is reserved in this module in the form of catalogues. This module is connected to the highly trusted resources and supplies these resources to the cloud customers through unified service portal.

3. Trust computing module: This module is the chief part of this architecture. Using real time monitoring of information, all the resource information are classified according to their performances and conserved in cloud resource management module. A unified service portal is provided for both user and administrator. A user can open a unified service portal and choose trusted service. Administrator manages the resources and servers on unified service portal [6].

Disadvantages:

1. Calculation of accurate trust: Trust has a dominant part in collaborative computing and clarifies the problem of providing security to the cloud customers. Trust incorporates multiple factors such as, accessibility, dependability, and certainty.

2. There are numerous number of cloud customers sending their request to the cloud server. Therefore, it is inconvenient to provide fast response to the cloud customers.
3. Cloud customers are storing their information to cloud. Therefore, calculating trust becomes difficult.
4. There are chances that the malicious users can get the unauthorized access of the information.

Proposed method:

Now a days, users wants to transfer their crucial information and data to the cloud sites to lessen their own burden, now it is the job of cloud sites to reserve all the information of the cloud customer. But, trust has a dominant role in between the cloud customer and cloud server sites. Therefore, trust agents evaluate the trust and provide these outcomes to the user for recommendation and predict the best services to the users.

Working of the proposed system:

There is numerous numbers of techniques available to calculate trust, but for collaborative computing these techniques are not sufficient. Steps included in the proposed system are:

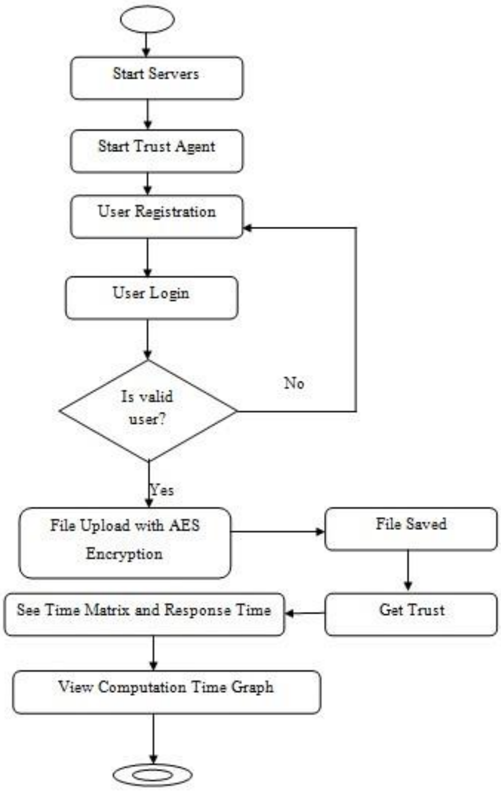


Fig: Working of the system.

I. The user must have to start the servers, because the information of the cloud customers is going to be stored at the servers.

II. Trust agents must be started because; the trust agents are calculating the trust and provide it to cloud customers.

III. The user shifts their information to the cloud server sites to reduce their own burden. Therefore, registration is necessary to get the authorization.

IV. Only authorized users can gain the access. Therefore, for authentication purpose login is required. If the cloud customer is valid, the access is gained otherwise the access is denied.

V. The user can upload their information if the access is authentic. To provide security, the file is encrypted prior to upload, to halt the information from unauthorized users. The file is encrypted using AES method.

VI. Now, the information is stored at the cloud server.

VII. To calculate trust, this system is considering successful login and response time and encryption is provided using AES encryption method.

With each request, a separate thread will be created and the entire request will be appended to the matrix window. Therefore, response time will calculate trust. If the response is less, the server is trusted otherwise not. If the data provided by the cloud user is not valid, the access is denied.

VIII. The time matrix and response time information is shown to the cloud customer so that it can be utilized for recommendation and predict the best service.

IX. Finally, the computation time graph is shown, in which the parallel and non parallel calculation is pictured and the response time is shown.

ADVANTAGES:

1. Parallel trust computing calculation: This concept makes this system faster.
2. Thread creation: When a user is requesting to the cloud server site, a separate thread is created, which will be processed. All the requests will be appended to the matrix window and the response time will be evaluated.
3. Encryption: To provide security to the system, when the file is upload. The file is encrypted first and then it is conserved at the cloud server.

   Therefore, the cloud consumer's data is protected from unauthorized users.

IV. **ALGORITHM DETAILS**

This venture has following modules,

- User
- Trust agent
- AES Algorithm.

TRUST AGENT MODULE DESCRIPTION

Trust agent module is going to evaluate the trust based on response time and successful login. If the response time is less, the cloud site is considered to be trusted otherwise it is not. If the cloud customer supplies wrong information, the access is denied. Therefore, only authorized cloud consumers can gain the access of the resources.

CLIENT MODULE DESCRIPTION

Client registers themselves and login to this system by supplying their personal information such as name, password, and email id. They have to put their information to the system to gain the access. If the information is correct, the access is granted otherwise it is denied.

In this architecture, AES algorithm is used. This algorithm is much faster and safer than DES [5]. The users information is encrypted using this algorithm and is uploaded to the cloud site. Therefore, only authorized cloud consumers can get the access and it is protected from unauthorized access.

EVALUATION:

Trust has a major part and is beyond security. Using parallel trust evaluation, the speed of the system is increased because all the requests are processing at the same time and can be calculated by response time. All the requests are appended to the matrix window.

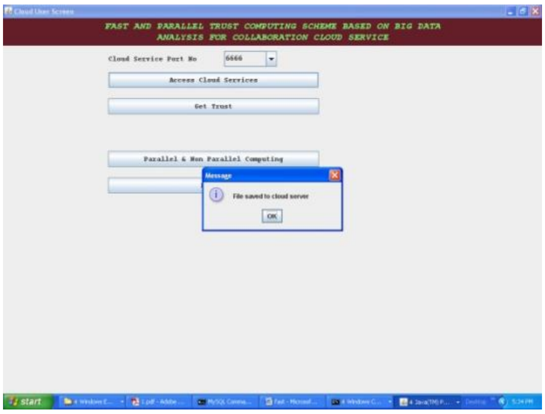
For authorization, successful login is provided, if the user is valid the entry is provided to the cloud consumer otherwise, the access is denied.

To provide security, the file is encrypted before it is uploaded to the cloud site. The file is encrypted using AES method. This is an advanced type of DES and is much stronger and faster than DES algorithm.

VI. RESULTS

The user is transferring their information to the cloud centers, to reduce their own burden and the cloud server will reserves the information of the user on their behalf. But this is genuinely based on trust. The cloud customer should trust a cloud server. Therefore, the trust agent has a major part in this architecture. The trust agent calculates the trust incorporating multiple factors such as response time, login, and encryption to provide trust values to the user. The trust agent calculates the trust so that it can be advocated to the users.

The trust agents show the time matrix window, trust values to the cloud customers and the computation time graph which differentiates the parallel and non-parallel computation. So that, the cloud user can recommends and predict the best services.

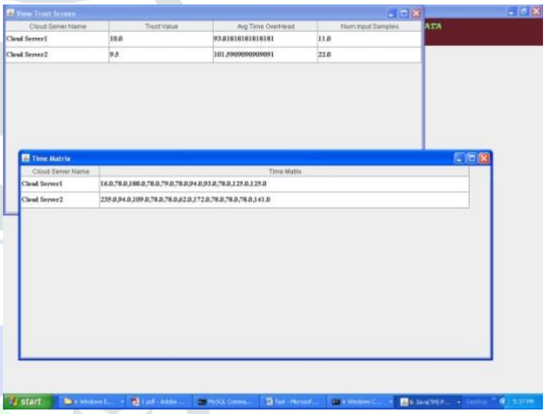


FAST AND PARALLEL TRUST COMPUTING SCHEME BASED ON BIG DATA ANALYSIS FOR COLLABORATION CLOUD SERVICE

Cloud Service Port No 6666

File saved to cloud server

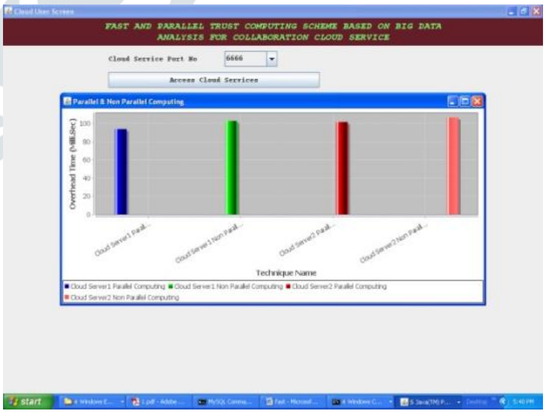
Fig 2: The cloud customer uploads the file to the cloud site so that can get the trust value.



Cloud Server Name	Trust Value	Avg Time OverHead	Num Input Samples
Cloud Server1	10.0	93.81818181818181	11.0
Cloud Server2	9.5	101.5909090909091	22.0

Cloud Server Name	Time Matrix
Cloud Server1	16.0,78.0,188.0,78.0,79.0,78.0,94.0,93.0,78.0,125.0,125.0
Cloud Server2	235.0,94.0,109.0,78.0,78.0,62.0,172.0,78.0,78.0,78.0,141.0

Fig 3: Trust agent showing the trust values of the cloud server.



FAST AND PARALLEL TRUST COMPUTING SCHEME BASED ON BIG DATA ANALYSIS FOR COLLABORATION CLOUD SERVICE

Cloud Service Port No 6666

Fig 4: Comparison between parallel and nonparallel trust computing.

CONCLUSION AND FUTURE WORKS

As a supportive method with earlier security methods, trust clarifies the problem of accessibility, security, and reliability. We introduced a new scheme to provide trust to the cloud consumers. We have proposed a system that calculates trust and predict the best service.

In our system, the cloud customer login for validation. If the user is valid, access is granted otherwise access is denied. Then the file is encrypted using AES method and stored at the cloud server. Then, the trust agent calculates the trust and provides the trust value stating that which server is providing the response much faster. So that it can be recommended to the users. Then finally, computation time graph is shown to provide the difference between the parallel and non-parallel computing, such that the best services can be predicted.

The proposed system can be evaluated on different cloud environment for future enhancement. Such as remote computing and distributed data sharing. Providing an accurate trust can also be considered as an important point for future research directions.

REFERENCES

[1] [Online]. Available:https://www.investopedia.com

[2] RR Nadikattu, 2016 THE EMERGING ROLE OF ARTIFICIAL INTELLIGENCE IN MODERN SOCIETY. International Journal of Creative Research Thoughts. 4, 4 ,906-911.

[3] [Online]. Available:https://blog.marconet.com

[4] Sikender Mohsienuddin Mohammad, **"DEVOPS AUTOMATION AND AGILE METHODOLOGY "**, International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 3, pp.946-949, August-2017, Available at :http://www.ijcrt.org/papers/IJCRT1133441.pdf

[5] X. Li, H. Ma, F. Zhou, and W. Yao, "T-broker: A trustaware service brokering scheme for multiple cloud collaborative services," IEEE Trans. Inf. Forensics Security, vol. 10, no. 7, pp. 1402–1415, Jul. 2015.

[6] H. Shen and G. Liu, "An efficient and trustworthy resource sharing platform for collaborative cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 25, no.

4, pp. 862–875, Apr. 2014

[5] R.R. Nadikattu. 2017. ARTIFICIAL INTELLIGENCE IN CARDIAC MANAGEMENT. International Journal of Creative Research Thoughts, Volume 5, Issue 3, 930-938.

[6] [Online]. Available:https://www.geeksforgeeks.org

[7] Sikender Mohsienuddin Mohammad, **"IMPROVE SOFTWARE QUALITY THROUGH PRACTICING DEVOPS AUTOMATION"**, International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.251-256, March 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133482.pdf

[8] Xiaoyong Li ; Jie Yuan ; Huadong Ma ; Wenbin Yao

IEEE Transactions on Information Forensics and Security

Year:2018 | Volume:13, Issue: 8 | JournalArticle | Publisher: IEEE

BIBLIOGRAPHY

Swati has received the B.Tech. degree in computer science engineering from Matu Ram Institute of Engineering and Management college, Rohtak, India, in 2014, and presently pursuing MTech, in computer networks and information security from G.Narayanamma Institute of Technology and Science college, Hyderabad, India.

A. Bhim Sankaram is an assistant professor in GNITS and has seven years of experience in teaching. His areas of interest are Data Structures, Big Data, Operating System, and Data Base Management System.