Trust Computing Scheme for Collaborative Cloud Service

Dr K. S. Wagh[1], Sachin Mundhe[2], Suraj Mane[3],Pradnyashil Kamble[4],
[1]*Computer Engineering Department, AISSMS IOIT, Pune, India*
[2-5]*Computer Engineering Department, AISSMS IOIT, Pune, India*

Abstract- Cloud computing became more popular and has attracted many users and business administrators to deliver their computing tasks and most sensitive data to the cloud because of its good characteristics such as low investment, easy maintenance flexibility, fast deployment and reliable service. Cloud computing widely used for computing and IT service delivery. However while working on cloud, trust is a critical factor it becomes even more challenging to work on collaborative cloud environment where user uses services from multiple cloud providers. In real cloud collaborative environment to respond large number of service requests with most relevant, efficient and trustworthy cloud service/provider has became a challenge. This research work aims to propose a unified trust computing scheme for giving most relevant, efficient and trustworthy cloud service provider to the requesting cloud users. Trustworthiness of the cloud service/provider will be evaluated based on various attributes and SLA compliance in collaborative cloud computing environment. Distributed agents will monitor service behaviour of various cloud services/providers and trust computing scheme will analyze this monitored big data to compute trustworthiness of cloud service/provider. We will monitor various Security, QoS and SLA based attributes to evaluate trustworthiness of cloud service provider.

Keywords- Cloud Computing, Service Behaviour monitoring, Trust computing, Big data analysis.

I. INTRODUCTION

Collaborative cloud computing has gradually attracted the attention of the industry and academia. Similar to the Internet becoming an inevitable stage of development of network technologies, collaborative cloud computing is expected to become an inevitable trend of cloud computing development. Collaborative cloud computing successfully uses information technology as a service over networks and provides end-users with extremely strong computational capability and massive memory space at low costs. Collaborative cloud computing also addresses the growing concerns on carbon emissions and environmental impact because collaborative cloud computing advocates improved management of resources.Despite the benefits provided by collaborative cloud computing, this new paradigm still faces several challenges related to trust computing, response speed, and automatic resource matchmaking. These challenges introduce new holistic designs, cooperative strategies, and distribution infrastructures. These innovative designs collectively make the proposed trust computing scheme a quick and lightweight solution that can be used in large-scale cloud service environments. To the best of our knowledge, this work is the first to provide a lightweight and parallel trust computing scheme based on big data analysis for trustworthy cloud services. The theoretical foundations and experimental results of this work are provided in this paper to validate the design of the trust computing scheme. The experimental results show that the proposed scheme outperforms previous existing approaches.

Recently, collaborative cloud computing has gradually attracted the attention of industry and academia. Liking the Internet is the inevitable stage of development of network technologies, the collaborative cloud computing will be an inevitable trend of cloud computing development. The collaborative cloud computing successfully uses information technology as a service over the network and provides end-users with extremely strong computational capability and huge memory space at low cost. Apart from the cost, the collaborative cloud computing also supports the growing concerns of carbon emissions and environmental impact since the collaborative cloud computing advocates better management of resources. Distributed computing technologies like peer-to-peer, grid, cloud etc. advocate collaboration by enabling shared access to resources distributed over different locations. One very good example is Google Apps suite which includes a variety of applications like Gmail, Drive, Calendar, Docs and Sheets etc. which are offered on cloud. All these applications under one umbrella increase productivity and performance of individuals as well as organizations.

Paper is organized as section one gives details of introduction of system, section two briefly gives the state of art of collaborative cloud computing, section three describes architecture of proposed system, section four discussed of propose system architecture and last section concludes the paper.

II. LITERATURE SURVEY

J. Huang and D. Nicol [1], presented paper on Trust mechanisms for cloud computing presents, this paper with a survey of existing mechanisms for establishing trust, and comment on their limitations. We then address those limitations by proposing more rigorous mechanisms based on evidence, at- tribute certification, and validation, and conclude by suggesting a framework for integrating various trust mechanisms together to reveal chains of trust in the cloud.

W. Fan, H. Perros [2], presented paper on A novel trust management framework for multi cloud environments based on trust service providers presents the problem of trust management inmulti-cloud environments based on a set of distributed Trust Service Providers (TSPs). These are independent third-party providers/trust agents, trusted by Cloud Providers (CPs), Cloud Service Providers (CSPs) and Cloud Service Users (CSUs), that provide trust related services to cloud participants. TSPs are distributed over the clouds, and they elicit raw trust evidence from different sources and in different formats. This evidence is information regarding the adherence of a CSP to a Service Level Agreement (SLA) for a cloud-based service and the feedback sent by CSUs. Using this information, they evaluate an objective trust and a subjective trust of CSPs. TSPs communicate among themselves through a trust propagation network that permits a TSP to obtain trust information about a CSP from other TSPs. Experiments show that our proposed framework is effective and relatively stable in differentiating trustworthy and untrustworthy CSPs in a multi-cloud environment.

K. Khan, Q. Malluhi [3], presented paper on Establishing Trust in Cloud Computing presents, Cloud computing has opened up a new frontier of challenges by introducing a different type of trust scenario. Today, the problem of trusting cloud computing is a paramount concern for most enterprises. It's not that the enterprises don't trust the cloud providers intentions; rather, they question cloud computing capabilities. Yet the challenges of trusting cloud computing don't lie entirely in the technology itself. The dearth of customer confidence also stems from a lack of transparency, a loss of control over data assets, and unclear security assurances. Unfortunately, the adoption of cloud computing came before the appropriate technologies appeared to tackle the accompanying challenges of trust. This gap between adoption and innovation is so wide that cloud computing consumers don't fully trust this new way of computing. To close this gap, we need to understand the trust issues associated with cloud computing from both a technology and business perspective. Then well be able to determine which emerging technologies could best address these issues.

M. Singhal, S. Chandrasekhar [4], presented paper on Collaboration in multi-cloud computing environments: Framework and security issues presents, A proposed proxy-based multi-cloud computing frame- work allows dynamic, on the y collaborations and resource sharing among cloud-based services, addressing trust, policy, and privacy issues without pre established collaboration agreements or standardized interfaces

S. Chakraborty, K. Roy [5], presented paper on An SLA-based framework for estimating trustworthiness of a cloud presents, work we propose a frame- work to alleviate the above issue. Our framework estimates trustworthiness of a cloud using a quantitative model of trust. We identified and formalized several parameters that can be extracted from SLA or retrieved during the sessions and are used to estimate trust.

M. Muchahari, S. Sinha [6], presented paper on A new trust management architecture for cloud computing environment presents, a trust management architecture which consist of a Cloud Service Registry and Discovery which serves as cloud providers registry and lists their respective trust values, a Trust Calculator that calculates CSPs trust based on feedbacks of two parameters namely SLA and QoS. A Dynamic Trust Monitor keeps watch on the deviating trust values with time and transactions.

J. Abawajy [7], presented paper on establishing trust in hybrid cloud computing environments presents, a fully distributed framework that enable trust-based cloud customer and cloud service provider interactions. The framework aids a service consumer in assigning an appropriate weight to the feedback of different fraters regarding a prospective service provider. Based on the framework, we developed a mechanism for controlling falsified feed- back ratings from iteratively exerting trust level contamination due to falsified feedback ratings. The experimental analysis shows that the proposed framework successfully dilutes the effects of falsified feedback ratings, thereby facilitating accurate and fair assessment of the service reputations.

Li, Xiaoyong, et al. [8] providing high trustworthy service is the most fundamental task for any cloud computing platform. Users are willing to deliver their computing tasks and the most sensitive data to cloud data centers, which is based on the trust relationship established between users and cloud service providers. However, with the development of collaboration cloud computing, how to provider fast response for a large number of users' service requests becomes a challenging problem. In order to quickly provide highly trustworthy services, the service platform must efficiently and quickly reply tens of millions of service requests, and automatically match-make tens of thousands of service resources. In this context, lightweight and fast (high-speed, low overhead) trust computing schemes become the fundamental demand for implementing a trustworthy and collaborative cloud service. An innovative and parallel trust computing scheme based on big data analysis for the trustworthy cloud service environment. First, a distributed and modular perceiving architecture for large-scale virtual machines' service behaviour is proposed relying on distributed monitoring agents. Then, an adaptive, lightweight, and parallel trust computing scheme is proposed for big monitored data. To the best of our knowledge, this paper is the first to use a blocked and parallel computing mechanism, the speed of trust calculation is greatly accelerated, which makes this trust computing scheme very suitable for a large-scale cloud computing environment. Performance analysis and experimental results verify feasibility and effectiveness of the proposed scheme.

Li, Xiaoyong, et al [9] Oriented by requirement of trust management in multiple cloud environment, this paper presents T-*broker*, a trust aware service brokering scheme for efficient matching cloud services (or resources) to satisfy various user requests. First, a trusted third party-based service brokering architecture is proposed for multiple cloud environments, in which the T-*broker* acts as a middleware for cloud trust management and service matching. Then, T-*broker* uses a hybrid and adaptive trust model to compute the overall trust degree of service resources, in which trust is defined as a fusion evaluation result from adaptively combining the direct monitored evidence with the social feedback of the service resources. More importantly, T-*broker* uses the maximizing deviation method to compute the direct experience based on multiple key trusted attributes of service resources, which can overcome the limitations of traditional trust schemes, in which the trusted attributes are weighted manually or subjectively. Finally, T-*broker* uses a lightweight feedback mechanism, which can effectively reduce networking risk and improve system efficiency. The experimental results show that, compared with the existing approaches, our T-*broker* yields very good results in many typical cases, and the proposed system is robust to deal with various.

Singh, Sarbjeet .et.al[10] One of the major hurdles in the widespread use of cloud computing systems is the lack of trust between consumer and service provider. Lack of trust can put consumer's sensitive data and applications at risk. Consumers need assurance that service providers will provide services as per agreement and will not deviate from agreed terms and conditions. Though trust is a subjective term, it can be measured objectively also. In this paper we present the design and simulation of a collaborative trust calculation scheme in which trust on a service provider is build by participants in a collaborative way. Each collaborator shares its experience of service provider with the coordinator and then shared experiences are aggregated by coordinator to compute final trust value which represents the trustworthiness of service provider. The scheme makes use of fuzzy logic to aggregate responses and to handle uncertain and imprecise information. Collaborative trust calculation scheme makes it difficult for untrustworthy service provider to build its reputation in the system by providing quality services only to a selected set of participants. A service provider has to provide agreed services to all participants uniformly in order to build reputation in the environment. Simulation has been done using MATLAB toolkit. Simulation results show that the scheme is workable and can be adopted for use in collaborative cloud computing systems to determine trustworthiness of service providers.

Li, Xiaoyong, et al [11] Multi-cloud collaborative environment consists of multiple data centers, which is a typical processing platform for big data. This paper focuses on the trust computing requirement of multi-cloud collaborative services and develops a Data-driven and Feedback-Enhanced Trust (DFET) computing pattern across multiple data centers with several innovative mechanisms. First, a trust-aware service monitoring architecture is proposed based on distributed soft agents to serve as middleware for multi-cloud trust computing and task scheduling. A data-driven trust computation scheme based on multi-indicator monitoring data is then proposed. The integration of several key service indicators into trust computing makes this scheme suitable for service-oriented cloud applications. More importantly, according to the intrinsic relationship among users, monitors, and service providers, we propose an enhanced and hierarchical feedback mechanism that can effectively reduce networking risk while improving system dependability. Theoretical analysis shows that DFET pattern is highly dependable against garnished and bad-mouthing attacks. We also build a prototype system to verify the feasibility of DFET pattern and the experiments yield meaningful observations that can facilitate the effective utilization of DFET in the large-scale multi-cloud collaborative environment.

Hasan, Md Mahmud et.al[12] The extensive integration of smart meters to utility communication networks introduces numerous cyber security concerns. Such meters are the primary access points to a smart grid advanced metering infrastructure (AMI). They are physically unprotected devices that are geographically distributed in low-trust environments. Nonetheless, they are expected to transceiver vital information regarding consumption, billing, and load management. The security of such information is an important requirement for operational continuity of a power system. Costs, system complexity, and response time are major considerations in designing security solutions for such cases. It is anticipated that future grids will be powered by the advancement of cloud computing. The security-as-a-service (SECaaS) is a model that exploits the potential of cloud computing to provide cyber security solutions. Its key offerings include cost reduction, simplicity, and faster response. This paper proposes a cloud centric collaborative security service architecture for the monitoring of upstream AMI traffic. It also includes a collaboration aware service placement scheme for the proposed architecture. The placement scheme develops a quadratic assignment problem (QAP) that minimizes latency. Case studies demonstrate the enhanced performance of the proposed scheme under various scenarios.

Chen, Min, et al. [13] With the popularity of wearable devices, along with the development of clouds and cloudlet technology, there has been increasing need to provide better medical care. The processing chain of medical data mainly includes data collection, data storage and data sharing, etc. Traditional healthcare system often requires the delivery of medical data to the cloud, which involves users' sensitive information and causes communication energy consumption. Practically, medical data sharing is a critical and challenging issue. Thus in this paper, we build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet include privacy protection, data sharing and intrusion detection. In the stage of data collection, we first utilize Number Theory Research Unit (NTRU) method to encrypt user's body data collected by wearable devices. Those data will be transmitted to nearby cloudlet in an energy efficient fashion. Secondly, we present a new trust model to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps similar patients to communicate with each other about their diseases. Thirdly, we divide users' medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect the healthcare system from malicious attacks, we develop a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks. Our experiments demonstrate the effectiveness of the proposed scheme.

Zhang, Daniel, et al [14] With the ever-increasing data processing capabilities of edge computing devices and the growing acceptance of running social sensing applications on such cloud-edge systems, effectively allocating processing tasks between the server and the edge devices has emerged as a critical undertaking for maximizing the performance of such systems. Task allocation in such an environment faces several unique challenges: (i) the objectives of applications and edge devices may be inconsistent or even conflicting with each other, and (ii) edge devices may only be partially collaborative in finishing the computation tasks due to the "rational actor" nature and trust constraints of these devices, and (iii) an edge device's availability to participate in computation can change over time and the application is often unaware of such availability dynamics. Many social sensing applications are also delay-sensitive, which further exacerbates the problem. To overcome these challenges, this paper introduces a novel game-theoretic task allocation framework. The framework includes a dynamic feedback incentive mechanism, a decentralized fictitious play with a new negotiation scheme, and a judiciously-designed private payoff function. The proposed framework was implemented on a testbed that consists of heterogeneous edge devices (Jetson TX1, TK1, and Raspberry Pi3) and Amazon elastic cloud. Evaluations based on two real-world social sensing applications show that the new framework can well satisfy real-time Quality-of-Service requirements of the applications and provide much higher payoffs to edge devices compared to the state-of-the-arts.\

Badidi, Elarbi .[15] The growing adoption of cloud computing and the proliferation of Internet-enabled handheld devices are changing the services landscape. Given the abundance and the variety of Software-as-a-Service (SaaS) offerings, we propose, in this paper, a framework for SaaS provisioning, which relies on brokered Service Level agreements (SLAs), between service consumers and SaaS providers. A Cloud Service Broker (CSB) helps consumers selecting the right SaaS provider that can fulfil their functional and quality-of-service (QoS) requirements. Its Selection Manager component ranks SaaS providers by matching their QoS offerings against the QoS requirements of the service consumer. Furthermore, the CSB is in charge of negotiating the SLA terms - using a multi-attributes negotiation model -- with a selected SaaS provider on behalf of the service consumer, and monitoring the compliance to the SLA during its implementation.

III. PROPOSED SYSTEM ARCHITECTURE

In many existing system having lots of issues into distribution as well as scheduling of resources, the below figure show the existing system flow with data centers. It shows the usual setup of high-availability computer system as it is implemented in practice. All network traffic coming from Internet (or intranet) is forwarded to hardware load balancers which usually operate in active-standby mode. Active load balancer uses its internal status tables first to check if all applications servers are available, and then to compute which one of them is currently in turn to receive traffic by using one of configured scheduling algorithms. In this way they distribute traffic between application servers, which usually operate in active-active configuration (all nodes are active). Behind them there is a database cluster in active standby mode of operation, with one node currently active and serving application servers. They use shared storage to hold databases. Actual setups may differ from a typical setup presented in Figure 1. For example, number of application servers or database cluster in active-active mode of operation, or similar minor variants of one of presented components. It is exactly on similar setups that there were recorded and documented issues with hardware load balancers not being aware of the current status on application servers (except the available/not available status) where they continue to forward traffic to an application server which is currently overloaded.

As Trust computing mechanism in collaborative cloud environment design of SLA complaint, evidence based, efficient and accurate trust computing methodology is main focus of the research work, we will start with rigorous survey of various trust computing mechanisms. We will also analyze traditional methodologies and their limitations. We will thoroughly understand and formulate characteristics of trust computing scheme by considering cloud users as well as cloud service providers role in collaborative cloud environment and would come up with efficient and accurate trust computing scheme with the focus on efficiency and accuracy by using big data analysis.

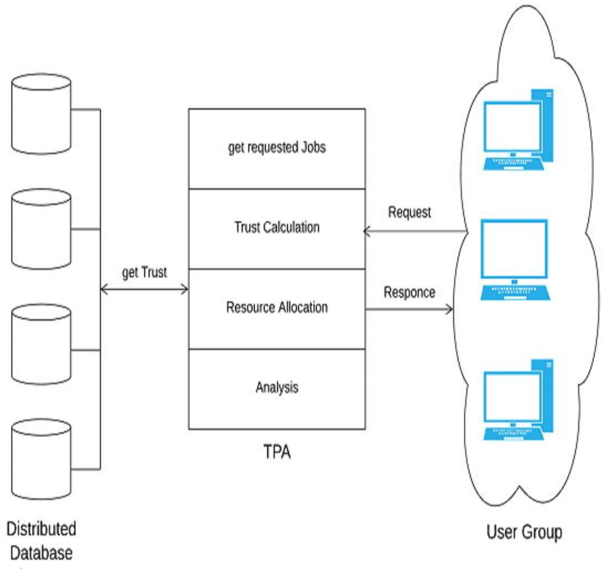

Fig.1: Proposed System Architecture

We would evaluate trust computing scheme from cloud user's perspective based on different data samples. We will perform rigorous experimental analysis of the proposed scheme and we will compare proposed system accuracy and efficiency with existing mechanisms.

Given the input as request from cloud user with their requirements, the system would perform analysis of big data collected by monitoring agents running on several distributed cloud sites. Our system will analyse collected QoS attributes and service specifications of different cloud service providers against cloud user requirements and gives list of most relevant and trustworthy cloud service/ service providers to the user so that user can save his confidential data on these cloud service or can transform his computing tasks to the service providers.

This proposed architecture consists of four modules. First module is job scheduler. The client submits their requests on server which is present in the IaaS cloud environment. When an available resource task is assigned to a cloud, first resource availability in this cloud will be checked by job scheduler. First file uploading and user authentication. Second server load degree calculation and chunk creation. And third module provides the resource scheduling the data between servers base on current loads. Final describe the performance analysis of system.

To provide user security for file transfer system requires proposed system. As in many roll based access system if the user have the access of the file then user can access the file any time but if the user found unauthorized then there is main challenge is revoking the access of that user. System provide that facility of revoking the access of the user also signature concept for the particular file. The figure shows the Architecture of Proposed System. The system consists of four basic modules which are listed and explain below in detail.

IV. PROPOSED ALGORITHMS

Algorithm 1: Compute Load (VM id)

This function can work to take the continuous reading of particular VM of CPU load as well as memory load. When we do the workflow scheduling we need to calculate each VM configuration. Using this algorithm we can calculate all VM details.

Input: I^{th} Node input, required memory RM
Output: Idle or Normal Or Overloaded in percent (%).
Define a load limit of memory L.

Calculate current memory usage as M, and denote available memory A= (L-M).

Find current CPU usage base on Load Weight W.

If (A> RM) set given node as strong node for memory selection.

Return {A,W}

Algorithm 2 : Weighted Dynamic job ordering algorithm
Input : Random jobs with size m.
Output : All ordered jobs {A[1]<size>…….A[n]<size>}
Step 1: Admin creates the m no. of random jobs.
Step 2 : Assign all m jobs to current scheduler.
Step 3: for each job (k into m when != Null)
Step 4: Check k each job size with defined map<key, vol>
Step 5 : Sort map with ascending order.
Step 6 : return map<key[job_id],vol [size]>

V. RESULTS AND DISCUSSION

The performance of Cloud Data processing can be adjusted by fine- tuning system parameters. Slot configuration system parameter has great impact on performance. By dynamically configuring Data processing slots better resource utilization and short make span can be achieved. From the survey, it can be resolved to prefer a dynamic slot distribution technique with optimal scheduling policy for better performance. The system is work with multiple virtual machines. One we deploy the system on EC2 environment it will work fine. The estimated results for the system base on below tables.

In second experiment shows data encryption performance which works to show that the data it determination encrypt in just how much time in seconds. Suppose there is a 100kb data is encrypted in 150 sec so the result will show by design in that time of encryption data from the users. The below figure shows the optimized job with assign VM id details. Once the algorithm execution has done, finally it will assign right VM to right job.

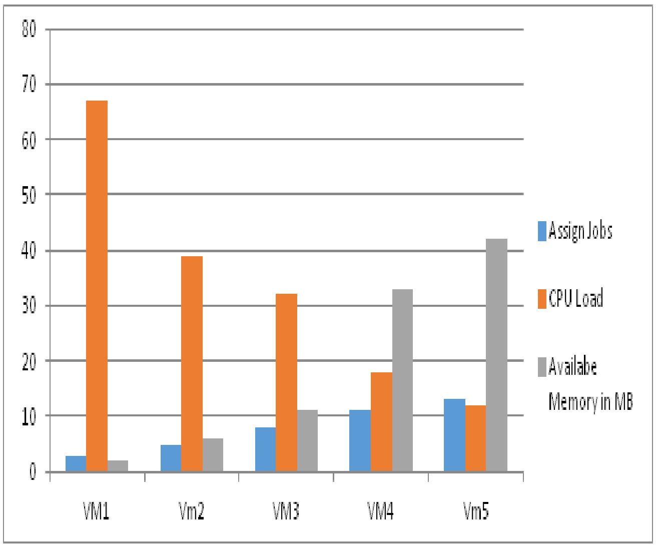

Fig.2: VM Load details

VI. CONCLUSION

Dynamic allocation is single of the main factors while giving out a large data set with Data processing paradigm. It optimizes the show of Data processing framework. Each job can be present scheduled using any one of the scheduling policies by the master scheduler. The task managers which are current in the task tracker allocate slots to jobs. After the observed paper, it is concluded to select a dynamic slot allocation strategy that takes in active jobs workload estimation, optimal slot assignment, and scheduling policy. Dynamic slot configuration is single of the main factors while giving out a large data set with Data processing paradigm. It optimizes the show of Data processing framework. Each job can be present scheduled using any one of the scheduling policies by the job tracker. Then, after integration with the active replica placement model, a dependable scheduling algorithm is developed to enhance the reliability and security of the computing platform.

VII. REFERENCES

[1]. J. Huang and D. Nicol, Trust mechanisms for cloud computing, Journal of Cloud Computing, 2013.

[2]. W. Fan, H. Perros, A novel trust management framework for multi cloud environments based on trust service providers, Knowledge-Based Systems, vol. 70, pp. 392-406, 2014.

[3]. K. Khan, Q. Malluhi, Establishing Trust in Cloud Computing, IEEE IT Professional, vol. 12, no. 5, pp. 20-27, 2010.

[4]. M. Singhal, S. Chandrasekhar, T. Ge, et al., Collaboration in multi cloudcomputing environments: Framework and security issues, IEEE Computer, vol. 46, no. 2, pp.76-84, 2013.

[5]. S. Chakraborty, K. Roy, An SLA-based framework for estimating trust- worthiness of a cloud, in: Proceedings of 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (Trust Computing), 2012, pp. 937942, 2012.

[6]. Muchahari, S. Sinha, A new trust management architecture for cloud computing environment, in: Proceedings of 2012 International Symposium on Cloud and Services Computing (ISCOS), pp. 136140, 2012.

[7]. J. Abawajy, Establishing trust in hybrid cloud computing environments, In: Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications,IEEE Computer Society, Washington, DC, USA.TRUSTCOM 11, pp 118125, 2011. doi:10.1109/TrustCom.2011.18. http://dx.doi.org/10.1109/TrustCom.2011.18

[8]. Li, Xiaoyong, et al. "Fast and Parallel Trust Computing Scheme Based on Big Data Analysis For Collaboration Cloud Service." *IEEE Transactions on Information Forensics and Security* 13.8 (2018): 1917-1931

[9]. Li, Xiaoyong, et al. "T-broker: A trust-aware service brokering scheme for multiple cloud collaborative services." *IEEE Transactions on Information Forensics and Security* 10.7 (2015): 1402-1415.

[10]. Singh, Sarbjeet, and Jagpreet Sidhu. "A collaborative trust calculation scheme for cloud computing systems." *Recent Advances in Engineering & Computational Sciences (RAECS), 2015 2nd International Conference on*. IEEE, 2015.

[11]. Li, Xiaoyong, et al. "Data-driven and feedback-enhanced trust computing pattern for large-scale multi-cloud collaborative services." *IEEE Transactions on Services Computing* 11.4 (2018): 671-684.

[12]. Hasan, Md Mahmud, and Hussein T. Mouftah. "Cloud-Centric Collaborative Security Service Placement for Advanced Metering Infrastructures." *IEEE Transactions on Smart Grid* (2017).

[13]. Chen, Min, et al. "Privacy protection and intrusion avoidance for cloudlet-based medical data sharing." *IEEE Transactions on Cloud Computing* (2016).

[14]. Zhang, Daniel, et al. "Cooperative-Competitive Task Allocation in Edge Computing for Delay-Sensitive Social Sensing." *2018 IEEE/ACM Symposium on Edge Computing (SEC)*. IEEE, 2018.

[15]. Badidi, Elarbi. "A cloud service broker for SLA-based SaaS provisioning." *Information Society (i-Society), 2013 International Conference on*. IEEE, 2013.