ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

A Trust Based Authentication and Management System for Cloud Network

J Bhargavi[1], Ambica Venna[2]

Assistant Professor, Dept. of C.S.E, Anurag College of Engineering, Aushapur(V), RR Dist, Telangana, India[1]

Assistant Professor, Dept. of IT, VBIT, RR Dist, Telangana, India. [2]

ABSTRACT: The recent advances in cloud computing have risen a number of unforeseen security related issues in different aspects of cloud environments. Among these, the problem of guaranteeing secure access to computing resources in the cloud is gathering special attention. In this paper, we address open issues related to trust in cloud environments proposing a new trust model for cloud computing which considers a higher level view cloud resources. A simulation of trust calculation between the nodes of the clouds is performed. The simulation was possible to verify that a node is reliable when it reaches the minimum index of trust.

KEYWORDS: Cloud computing, Distributed Computing, Security, Integrity, Confidentiality, Trust and availability.

I. INTRODUCTION

The across the board utilization of Internet associated frameworks and dispersed applications has set off an upset towards the appropriation of pervasive and universal distributed computing situations. These situations permit clients and customers to buy processing power as per need, flexibly adjusting to various execution needs while giving higher accessibility. A few electronic arrangements, for example, Google Docs and Customer Relationship Management (CRM) [2] applications, now work in the product as an administration model. Quite a bit of this adaptability is made conceivable by virtual processing strategies, which can give versatile assets and framework with a specific end goal to bolster versatile on interest offers of such applications. Virtual registering is likewise connected to remain solitary base as an administration arrangements, for example, Amazon Elastic Cloud Computing (EC2) and Elastic Utility Computing Architecture Linking Your Programs to Useful Systems (Eucalyptus) [2]. Subsequently, the distributed computing structures and situations can address diverse issues in current appropriated and pervasive registering frameworks. The accessibility of foundation as an administration and stage as an administration situations gave a crucial base to building distributed computing based applications. It likewise inspired the innovative work of advances to bolster new applications. As a few vast organizations in the interchanges and data innovation segment have received distributed computing based applications, this methodology is turning into an accepted industry standard, being broadly embraced by various associations. Since the selection of the distributed computing worldview by IBM Corporation around the end of 2007, different organizations, for example, (Google App Engine), (Amazon Web Services (AWS), EC2 (Elastic Compute Cloud) and S3 (Simple Storage Service)), Apple (iCloud) and Microsoft (Azure Services Platform) have continuously grasped it and presented their own particular new items in light of distributed computing innovation [11]. Be that as it may, distributed computing still stances dangers identified with information security in its diverse viewpoints (honesty, classification and validness). Distributed computing gives a minimal effort, adaptable, area free framework for information administration and capacity. The quick appropriation of Cloud administrations is joined by expanding

volumes of information put away at remote servers, so methods for sparing circle space and system data transfer capacity are required. A focal best in class idea in this connection is deduplication, where the server stores just a solitary duplicate of every document, paying little heed to what number of customers requested that store that record. All customers that store the record simply utilize connections to the single duplicate of the document put away at the server. Besides, if the server as of now has a duplicate of the document, then customers don't have to transfer it again to the server, accordingly sparing transmission capacity and in addition stockpiling (this is termed customer side deduplication). Allegedly, business applications can accomplish deduplication proportions from 1:10 to as much as

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

1:500, bringing about plate and data transfer capacity investment funds of more 90%. Deduplication can be connected at the document level or at the piece level. In a regular stockpiling framework with deduplication, a customer first sends to the server just a hash of the document and the server checks if that hash esteem as of now exists in its database. In the event that the hash is not in the database then the server requests the whole record. Something else, since the document as of now exists at the server (possibly transferred by another person), it tells the customer that there is no compelling reason to send the record itself. Whichever way the server denote the customer as a proprietor of that document, and starting there on the customer can request that reestablish the record (paying little heed to whether he was requested that transfer the record or not). The customer side deduplication presents new security issues. For instance, a server telling a customer that it need not send the document uncovers that some other customer has precisely the same, which could be touchy data. A malignant customer can utilize this data to check whether particular documents were transferred by different clients, or even run a savage power assault which distinguishes the substance of specific fields in records claimed by different clients, by attempting to transfer numerous variations of the same document which have diverse qualities for that field. The discoveries apply to mainstream record stockpiling administrations, for example, Mozy Home and Drop box, among others. In this paper, we survey the principle distributed computing engineering designs and distinguish the fundamental issues identified with security, protection, trust and accessibility. With a specific end goal to address such issues, we exhibit an abnormal state engineering for trust models in distributed computing situations.This paper is organized as follows. In Section II, we present an overview of cloud computing, presenting asummary of its main features, architectures and deployment models. In Section III, we present related works. In section IV, we introduce the proposed trust model. Finally, in Section V, we conclude with a summary of our results and directions for new research.

II. RELATED WORK

Current trend work with the following two aspects: (A) Authentication; (B) Trust and reputation.

A. Authentication

There are substantial works regarding authentication in cloud . For instance, a user authentication framework for CC is proposed in [18], aiming at providing user friendliness, identity management, mutual authentication and session key agreement between the users and the cloud server. Paying particular attention to the lightweight of authentication since the cloud handles large amounts of data in real-time, shows a lightweight multi-user authentication scheme based on cellular automata in cloud environment. Certificate authority based one-time password authentication is utilized to perform authentication. It first describes the composition
and mechanism of the proposed architecture model. Then it puts forward security mechanism for authenticating legal users to access sensor data and information services inside the architecture, based on a certificate authority based Kerberos protocol. Finally the prototype deployment and simulation experiment of the proposed architecture model are introduced.

B. Trust and Reputation

For efficient reconfiguration and allocation of cloud computing resources to meet various user requests, a trust model which collects and analyzes the reliability of cloud resources based on the historical information of servers With respect to trust in the CC-WSN integration, we should focus on how trust management could be effectively used to enhance the security of a cloudintegrated WSN. Particularly, the security breaches regarding data generation, data transmission and in-network processing in the WSN integrated with cloud are observed in [32] first. Then it shows some examples that trust can be employed to perform trust-aware data transmission and trust-aware data
processing in the integrated WSN as well as trust-aware services in the cloud.

III. CLOUD COMPUTING

Distributed computing alludes to the utilization, through the Internet, of assorted applications as though they were introduced in the client's PC, freely of stage and area. A few formal definitions for distributed computing have been proposed by industry and the educated community. We embrace the accompanying definition: "Distributed computing

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

is a model for empowering helpful, on-interest system access to a mutual pool of configurable registering assets (e.g., systems, servers, stockpiling, applications, and administrations) that can be quickly provisioned and discharged with negligible administration exertion or administration supplier connection" [14]. This definition incorporates cloud structures, security, and organization systems. Distributed computing is as a rule logically received in various business situations so as to get adaptable and dependable figuring situations, with a few supporting arrangements accessible in the business sector. Being founded on various innovations (e.g. virtualization, utility processing, lattice registering and benefit situated structures) and constituting a radical new computational worldview, distributed computing requires abnormal state administration schedules. Such administration exercises include: (an) administration supplier choice; (b) virtualization innovation determination; (c) virtual assets distribution; (d) checking and reviewing keeping in mind the end goal to ensure Service Level Agreements (SLA). Computational trust can be utilized so as to set up an engineering and a checking framework including every one of these requirements and as yet supporting common exercises, for example, arranging, provisioning, versatility and security. Chang et al. [15] present a couple challenges identified with security, execution and accessibility in the cloud.

A. Attributes of Cloud Computing

One point of preference of distributed computing is the likelihood of getting to applications straightforwardly from the Internet, with minor prerequisites of client figuring assets. There are other huge favorable circumstances and burdens [13], as appeared in Table I. Distributed computing consolidates a mutual and measurable administration model. It presents three fundamental attributes [1]: an) equipment framework engineering – in view of minimal effort adaptable groups. The figuring framework in the cloud is made out of an awesome number of minimal effort servers, for example, standard X86 server hubs; b) synergistic improvement of fundamental administrations and applications with maximal asset use, hence enhancing conventional programming designing procedures. In the conventional computational model, applications turn out to be totally reliant on the fundamental administrations; c) the repetition among a few minimal effort servers is ensured through programming. Since countless cost servers is utilized, singular hub disappointments can't be overlooked. Along these lines, hub adaptation to internal failure must be considered in the outline of programming..

TABLE I. ADVANTAGES AND DISADVANTAGES OF CLOUD COMPUTING

Advantages	Disadvantages
Lower IT infrastructure cost	Requires a constant Network connection
Increased computing power	Dependable of network bandwidth
Unlimited storage capacity	Features might be limited
Improved compatibility between operating Systems	Stored data might not be secure
Easier group collaboration	If the cloud loses your data, you will not have access to your information.
Universal access to documents	

B. Cloud Computing Architecture

Distributed computing design depends on layers. Every layer manages a specific part of making application assets accessible. Fundamentally there are two primary layers: a lower and a higher asset layer. The lower layer contains the physical base and is in charge of the virtualization of capacity and computational assets. The higher layer gives particular administrations. These layers may have their own particular administration and observing framework, autonomous of each other, in this manner enhancing adaptability, reuse and versatility. Figure 1 displays the distributed computing compositional layers [11].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

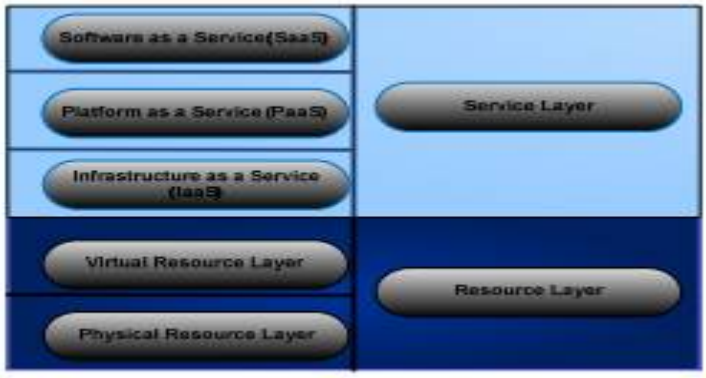

Figure 1. Cloud Computing Architecture [11]

C. Software as a Service

Programming as a Service (SaaS) gives every one of the elements of a customary application, yet gives access to particular applications through Internet. The SaaS model diminishes worries with application servers, working frameworks, stockpiling, application improvement, and so on. Subsequently, designers may concentrate on advancement, and not on framework, prompting quicker programming frameworks improvement. SaaS frameworks decrease costs subsequent to no product licenses are required to get to the applications. Rather, clients access administrations on interest. Since the product is generally Web based, SaaS permits better mix among the specialty units of a given association or even among various programming administrations. Case of SaaS incorporate [2]: Google Docs and Customer Relationship Management (CRM) administrations.

D. Stage as a Service

Stage as a Service (PaaS) is the center segment of the administration layer in the cloud. It offers clients programming and administrations that don't require downloads or establishments. PaaS furnishes a foundation with an abnormal state of combination keeping in mind the end goal to execute and test cloud applications. The client does not deal with the framework (counting system, servers, working frameworks and capacity), yet he controls sent applications and, perhaps, their arrangements [4]. PaaS gives a working framework, programming dialects and application programming situations. Hence, it empowers more proficient programming frameworks execution, as it incorporates instruments for improvement and coordinated effort among engineers. From a business outlook, PaaS permits clients to exploit outsider administrations, expanding the utilization of a bolster model in which clients subscribe to IT benefits or get issue determination guidelines through the Web. In such situations, the work and the obligations of organization IT groups can be better overseen. Case of SaaS [2] include: Azure Services Platform (Azure), Force.com, EngineYard and Google App Engine.

E. Framework as a Service

Framework as a Service (IaaS) is the part of the engineering in charge of giving the base important to PaaS and SaaS. Its principle goal is to make assets, for example, servers, system and capacity all the more promptly open by including applications and working frameworks. Along these lines, it offers essential base on-interest administrations. IaaS has a novel interface for framework administration, an Application Programming Interface (API) for connections with hosts, switches, and switches, and the capacity of including new gear in a basic and straightforward way. By and large the, client does not deal with the fundamental equipment in the cloud base, yet he controls the working frameworks, stockpiling and sent applications. Inevitably he can likewise choose system segments, for example, firewalls. The term IaaS alludes to a figuring framework, taking into account virtualization strategies that can scale powerfully, expanding or lessening assets as per the necessities of utilizations. The fundamental advantage gave by IaaS is the payper-use plan of action [4]. Case of IaaS [2] include: Amazon Elastic Cloud Computing (EC2) and Elastic Utility Computing Architecture Linking Your Programs To Useful Systems (Eucalyptus).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

F. Parts in Cloud Computing

Parts characterize the obligations, get to and profile of various clients that are a piece of a distributed computing arrangement. Figure 2 displays these parts characterized in the three administration layers [3]. The supplier is in charge of overseeing, checking and ensuring the accessibility of the whole structure of the distributed computing arrangement. It liberates the designer and the last client from such obligations while giving administrations in the three layers of the engineering. Engineers utilize the assets gave by IaaS and PaaS to give programming administrations to conclusive clients. This multi-part association characterizes the performing artists (individuals who assume the parts) in distributed computing situations. Such performing artists may assume a few parts in the meantime as per need or intrigue. Just the supplier bolsters all the administration layers.

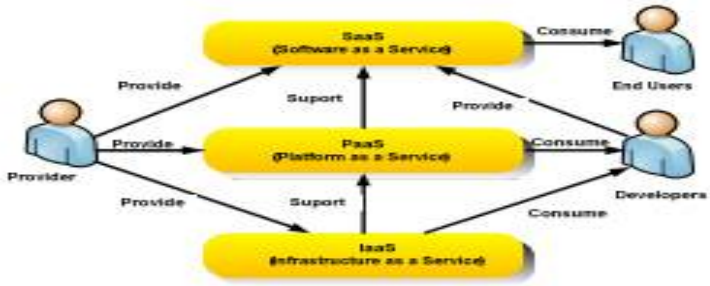

Figure 2.Roles in cloud computing .

G. Cloud Computing Deployment

According to the intended access methods and availability of cloud computing environments, there are different models of deployment [4]. Access restriction or permission depends on business processes, the type of information and characteristics of the organization. In some organizations, a more restrict environment may be necessary in order to ensure that only properly authorized users can access and use certain resources of the deployed cloud services. A few deployment models for cloud computing are discussed in this section. They include private cloud, public cloud, community cloud and hybrid cloud, which are briefly analyzed below.

TABLE II. MODELS OF DEPLOYMENT OF CLOUD SERVICES [4]

Cloud Model	Description
Private	In this model, the cloud infrastructure is exclusively used by a specific organization. The cloud may be local or remote, and managed by the company itself or by a third party. There are policies for accessing cloud services. The techniques employed to enforce such private model may be implemented by means of network management, service provider configuration, authorization and authentication technologies or a combination of these
Public	Infrastructure is made available to the public at large and can be accessed by any user that knows the service location. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used
Community	Several organizations may share the cloud services. These services are supported by a specific community with similar interests such as mission, security requirements and policies, or considerations about flexibility. A cloud environment operating according to this model may exist locally or remotely and is normally managed by a commission that represents the community or by a third party.
Hybrid	Involves the composition of two or more clouds. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds.

Private Cloud computing presents a few challenges related to protection, trust, privacy and security of user data.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

IV. CLOUD RELATED WORK ON SECURITY AND TRUST

This area audit some related work about security, document framework and trust in the cloud.

A. Security in the Cloud

Various advancements have been utilized with a specific end goal to give security to distributed computing situations. The creation and assurance of security testaments is typically insufficient to guarantee the essential security levels in the cloud. Cryptographic calculations utilized with cloud applications generally diminish execution and such decrease must be confined to adequate levels [21]. Distributed computing offers clients an advantageous method for sharing an expansive amount of appropriated assets having a place with various associations. Then again, the very way of the distributed computing worldview makes security angles entirely more intricate. Trust is the primary worry of purchasers and administration suppliers in a distributed computing environment [7]. The incorporation of very surprising nearby frameworks and clients of entirely differing situations conveys extraordinary difficulties to the security of distributed computing. On one hand, security components must offer clients a sufficiently high level of assurances. Then again, such component must not be so unpredictable as to make it troublesome for clients to utilize the framework. The openness and computational adaptability of well known industrially accessible working frameworks have been vital components to bolster the general selection of distributed computing. By the by, these same elements expand framework unpredictability, decrease the level of trust and acquaint openings that get to be dangers with security [7]. Huan et al. [22] explore the distinctive security helplessness evaluation strategies for cloud situations. Tests demonstrate that more vulnerabilities are identified if powerless apparatuses and servers are in the same LAN. In other word, the programmers can locate a less demanding approach to get the objective data in the event that it is on the same LAN of traded off frameworks. Trial results can be utilized to break down the danger in outsider process mists. Popovic et al. [23] examine security issues, necessities and difficulties that Cloud Service Providers (CSP) face amid cloud building. Prescribed security principles and administration models to address these are recommended both for the specialized and business group.

B. Record framework Security

As the quantity of gadgets oversaw by clients is constantly expanding, there is a developing need of synchronizing a few progressively appropriated record frameworks utilizing impromptu network. Uppoor et al. [6] present another methodology for synchronizing of progressively conveyed record frameworks. Their methodology looks like the upsides of peerto-companion synchronization, putting away online expert reproductions of the mutual records. The proposed plan gives information synchronization in a distributed system, wiping out the expenses and transfer speed necessities generally exhibit in distributed computing expert copy approaches. The work in [9] presents CDRM, a plan for element circulation of record imitations in a distributed storage group. This plan occasionally overhauls the number and area of document square imitations in the bunch. The quantity of copies is redesigned by genuine accessibility of group hubs and the normal record accessibility. The dynamic dissemination calculation for imitation arrangement considers the capacity and computational limit of the bunch hubs, and also the data transfer capacity of the correspondence system. A usage of the proposed plan utilizing an open source dispersed document framework named HDFS (Hadoop Distributed File System) is talked about. Exploratory estimations call attention to that the dynamic plan beats existing static document appropriation calculations.

C. Trust in the Cloud

Trust and security have ended up essential to ensure the solid improvement of cloud stages, giving answers for concerns, for example, the absence of protection and assurance, the surety of security and creator rights. Protection and security have been appeared to be two essential snags concerning the general reception of the distributed computing worldview. With a specific end goal to take care of these issues in the IaaS administration layer, a model of dependable distributed computing which gives a shut execution environment to the secret execution of virtual machines was proposed [5]. This work has demonstrated how the issue can be tackled utilizing a Trusted Platform Module. The proposed model, called Trusted Cloud Computing Platform (TCCP), should give larger amounts of unwavering quality, accessibility and security. In this arrangement, there is a bunch hub that goes about as a Trusted Coordinator (TC). Different hubs in the bunch must enroll with the TC so as to ensure and confirm its key and estimation list. The TC keeps a rundown of trusted hubs. At the point when a virtual machine is begun or a relocation happens, the TC confirms whether the hub is reliable so that the client of the virtual machine might make sure that the stage stays

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

dependable. A key and a mark are utilized for recognizing the hub. In the TCCP model, the private accreditation power is included in every exchange together with the TC [5]. Shen et al. [7] introduced a strategy for building a reliable distributed computing environment by incorporating a Trusted Computing Platform (TCP) to the distributed computing framework. The TCP is utilized to give verification, classification and uprightness [7]. This plan showed positive results for verification, guideline based access and information insurance in the distributed computing environment. Cloud administration suppliers (CSP) ought to ensure the administrations they offer, without abusing clients' security and classification rights. Li et al. [8] presented a multitenancy trusted registering environment model (MTCEM). This model was intended for the IaaS layer with the objective of guaranteeing a dependable distributed computing environment to clients. MTCEM has two progressive levels in the transitive trust display that backings partition of worries amongst usefulness and security. It has 3 personality streams: a) the customers, who procure the CSP distributed computing administrations; b) the CSP, that gives the IaaS administrations; c) the reviewer (discretionary, yet prescribed), who is in charge of confirming whether the framework gave by the CSP is reliable in the interest of clients. In MTCEM, the CSP and the clients team up with each other to manufacture and keep up a dependable distributed computing environment. Zhimin et al. [12] propose a community oriented trust model for firewalls in distributed computing. The model has three focal points: an) it utilizes diverse security arrangements for various areas; b) it considers the exchange connections, noteworthy information of substances and their impact in the dynamic estimation of the trust worth; and c) the trust model is good with the firewall and does not break its neighborhood control strategies. A model of area trust is utilized. Trust is measured by a trust esteem that relies on upon the substance's setting and chronicled conduct, and is not altered. The cloud is isolated in various self-ruling spaces and the trust relations among the hubs is partitioned in intra and interdomain trust relations. The intra-area trust relations depend on exchanges worked inside the space. Every hub keeps two tables: an immediate trust table and a proposal list. On the off chance that a hub needs to compute the trust estimation of another hub, it first checks the immediate trust table and uses that worth if the quality comparing to the coveted hub is as of now accessible. Something else, in the event that this quality is not locally accessible, the asking for hub checks the proposal list keeping in mind the end goal to decide a hub that has an immediate trust table that incorporates the fancied hub. At that point it checks the immediate trust table of the suggested hub for the trust estimation of the sought hub. The procedure proceeds until a trust esteem for the wanted hub is found in an immediate trust table of some hub. The interdomain trust qualities are figured in light of the exchanges among the between space hubs. The between area trust worth is a worldwide estimation of the hubs direct trust values and the suggested trust esteem from different spaces. Two tables are kept up in the Trust Agents sent in every space: type of Inter-area trust connections and the weight esteem table of this space hub. In [17] a trusted distributed computing stage (TCCP) which empowers IaaS suppliers to offer a shut box execution environment that certifications private execution of visitor virtual machines (VMs) is proposed. This framework permits a client to confirm whether its calculation will run safely, before asking for the administration to dispatch a VM. TCCP accept that there is a trusted facilitator facilitated in a dependable outer substance. The TCCP ensures the privacy and the respectability of a client's VM, and permits a client to decide in advance regardless of whether the IaaS upholds these properties. The work [18] assesses various trust models for dispersed cloud frameworks and P2P systems. It additionally proposes a reliable cloud engineering (counting trust appointment and notoriety frameworks for cloud asset destinations and datacenters) with ensured assets including datasets for on-interest administrations.

VI. SIMULATION RESULTS

we evaluate whether our proposed ATRCM system can fulfill the predetermined functions: 1) authenticating CSP and SNP to avoid malicious impersonation attacks; 2) calculating and managing trust and reputation regarding the service of CSP and SNP; 3) helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP, based on (i) the authenticity of CSP and SNP; (ii) the attribute requirement of CSU and CSP as well as (iii) the cost, trust and reputation of the service of CSP and SNP.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

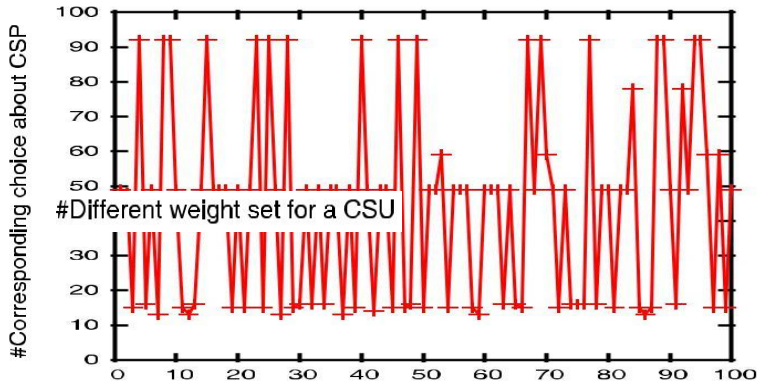

Fig. 3. Different weight set for a CSU and Corresponding Choice About CSP

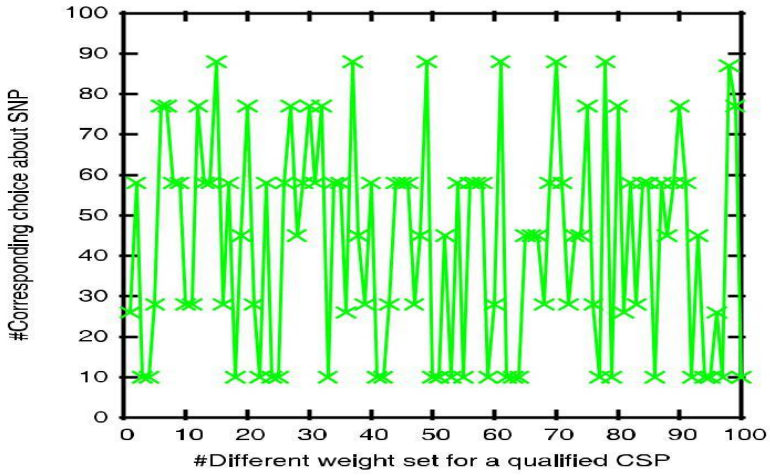

Fig.4. Different weight set for a qualified CSP and corresponding choice about SNP.

V. CONCLUSION

We have introduced an outline of the distributed computing worldview, and in addition its principle components, structures and arrangement models. In addition, we distinguished the principle issues identified with trust and security in distributed computing situations. With a specific end goal to address these issues, we proposed a trust model to guarantee solid trade of records among cloud clients in broad daylight mists. In our model, the trust estimation of a given hub is acquired from a pool of straightforward parameters identified with its appropriateness for performing stockpiling operations. Hubs with more noteworthy trust qualities are thusly decided for further record stockpiling operations. As a future work, we plan to execute the proposed trust show and investigate hub conduct after the positioning of reliable hubs is built up.

REFERENCES

[1] Chen Kang and Zen WeiMing, "Cloud computing: system instance and current research," Journal of Software, pp. 20(5):1337-1347. 2009.
[2] Minqi Zhou, Rong Zhang, DadanZeng, and WeiningQian, "Services in the cloud computing era: a survey," Software Engineering Institute. Universal Communication.Symposium (IUCS), 4th International. IEEE Shanghai, pp. 40-46. China. 978-1-4244-7821-7 (2010).
[3] A. Marinos and G. Briscoe, "Community cloud computing," in First International Conference Cloud Computing, CloudCom, volume 5931 of Lecture Notes in Computer Science, pp. 472–484. Springer (2009).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

[4] Zhao-xiong Zhou, He Xu, and Suo-ping Wang, "A Novel Weighted Trust Model based on Cloud," AISS: Advances in Information Science and Service Sciences, Vol. 3, No. 3, pp. 115- 124, April 2011.
[5] Wang Han-zhang and Huang Liu-sheng, "An improved trusted cloud computing platform model based on DAA and Privacy CA scheme," IEEE International Conference on Computer Application and System Modeling (ICCASM 2010).978-1-4244-7235-2. 2010.
[6] S. Uppoor, M. Flouris, and A. Bilas, "Cloud-based synchronization of distributed file system hierarchies," Cluster Computing Workshops and Posters (CLUSTER WORKSHOPS), IEEE International Conference, pp. 1-4. 2010.
[7] ZhidongShen, Li Li, Fei Yan, and Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform," Intelligent Computation Technology and Automation (ICICTA), IEEE International Conference on Volume: 1, pp. 942-945. China. 2010.
[8] Xiao-Yong Li, Li-Tao Zhou, Yong Shi, and Yu Guo, "A Trusted Computing Environment Model in Cloud Architecture," Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, 978-1- 4244-6526-2. Qingdao, pp. 11-14. China. July 2010.
[9] Qingsong Wei, BharadwajVeeravalli, Bozhao Gong, LingfangZeng, and Dan Feng, "CDRM: A Cost-Effective Dynamic Replication Management Scheme for Cloud Storage Cluster," 2009 IEEE International Conference on Cluster Computing (CLUSTER), pp. 188-196, 2010.
[10] Kai Hwang, Sameer Kulkareni, and Yue Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Mangement," 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC '09), pp. 717-722, 2009.

BIOGRAPHY

1.Jangam Bhargavi is an Assitant Professor in the Computer Science & Engineering Department, Anurag College of Engineering, JNTUH. I received Master of Technology (M.Tech) degree in 2013 from Nishita College of Engineering, Ranga Reddy, Telangana, India. My research interests are Computer Networks (wireless Networks), Cloud Computing, etc

2.Ambica Venna is an Assistant Professor in the Information Technology Department, Vignana Bharathi Institute of Technology, JNTUH. I received Master of Technology (M.Tech) degree in 2013 from Tirumala Engineering College, Ranga Reddy, India. My research interests are Internet of Things ,Cloud computing,Computer Networks,Web Technologies etc.