INVESTIGATION IN CLOUD COMPUTING SERVICES ON TRUST MODELS

Ali Raza\textsuperscript{1}, Sidra Saleem\textsuperscript{2}, Maria Inayat\textsuperscript{3}, Maria Qadeer\textsuperscript{4}, Shagufta Anwar\textsuperscript{5}, Isma Jabeen\textsuperscript{6}, Anum Safder\textsuperscript{7}, Faisal Iqbal Jafri\textsuperscript{8}

\textsuperscript{1,2,3,4,5,6,7}Department of Computer Science, Best College Kharian, Pakistan.
\textsuperscript{8}Department of Botany, University of Gujrat, Gujrat, Pakistan.

Email: aliraza6136@gmail.com\textsuperscript{1}, Faisal.bhs@gmail.com\textsuperscript{8}

Abstract — In Cloud services, trust establishment has become an integral and a critical trademark feature. Therefore, Cloud users should be endowed with a systematic approach that helps users of these services to find an unequivocal trust model that most suit their organization’s trust policy at all levels. Hence, this study reports the analysis of existing trust models in cloud services in a CloudSim environment. Simulation results obtained with several experimental scenarios depict their respective performances and the most secured trust model in cloud services. Consequently, cloud computing organizations and end-users can without difficulty select tools that best suited and adopt it to meeting their respective organizations’ incidents response vis-à-vis services.

Index Terms — cloud services, CloudSim, trust model

1 INTRODUCTION
The world is a connected world. Cloud Computing is an evolving technology that has been acceptable by users in the Information Technology community in similarity to the trend recorded with the emergence of the Internet, that is, the World Wide Web, client-server architecture and networks [1]. Cloud Computing, as defined by Zhiguo et al. [2] “is a set of principles, standards and policies” employed in system analysis by service providers; on the fundamental principles of “virtualization, distributed computing, utility computing and service-oriented architecture”. Cloud system is characterized with front end and back ends with the connection platform as the Internet. Client coupled with its associated tools and Cloud refer to the front and bank ends respectively. Consequently, the client and cloud are variants of cutting-edge techniques; these features of cloud computing components extend its heterogeneous capacity. The heterogeneity feature enables various services; an instance is Web-based e-mail programs leverage on existing Web browsers such as Google chrome, UC and so on. Internet Explorer or Firefox including robust clients accessing the network access. Back end instances among others are servers, data storage as well as other perimeter security tools form the computing services in the “cloud”.

According to Ravish et al. [3], usually, each application owns a dedicated server; however, a cloud computing system may perhaps comprise any computer program imaginable: data processing to video games or other programs. As stated by National Institute of Standards and Technology (NIST), a vital characteristics of cloud computing include on-demand self-service; which simply requires that the service must be always available and easily changed by the client without contacting the service provider. With the exciting returns of cloud services, it is worthy to note that trust remains the contest in cloud computing with the customer’s data and business logics residing in the remotely situated servers which could be far away from the end-users. Thus, with the aim of catering for these issues, different security policies, mechanisms, techniques and protocols generally called trust models were projected to assess the trust level invariably addressing the cloud security challenges. The agitation created by trust issues have propelled professionals and researchers, both from the industry and academia, to propose various trust establishment solutions ranging from simple mechanisms of SLAs to complex trust evaluation models. These trust models are supported by different features sets of secured data and quality of service (QoS). Nonetheless, the continuous rising attention in Cloud trust domain; and existing literature on trust models largely remains unstructured. Hence, it turns out to be difficult whenever cloud consumers have to opt for the most secured trust model from an extensive variety of alternatives. This is because the best of the trust models in terms of its security requirements is yet to be identified.

2 RELATED WORK
Trust is found to be one of the major challenges in the cloud computing concepts as distrust prevents the consumers from
its wide use and distrust due to the fact that most consumers do not have a direct control over their data lying on the cloud. The component of trust is a critical factor in the wide usage and deployment of cloud services. Trust is established between the two parties, that is, the trustor and trustee. Kavita and Sudesh [4] explains the trustor as a person or entity holding confidence, reliability, belief, integrity and ability, belonging to the third party or thing as trust object, that is, the trustee. To this end, a reliable services offer depends on trust as a critical factor in the cloud environment to its customers. It has enhanced services acceptance among cloud consumers. Therefore, trust should be established between cloud service provider and cloud consumer; and as stated in Priya and Jaisankar [5], trust management is widely deployed in online services, E-commerce and social network.

Talal and Quan [6] presented the analysis of trust management perspectives and classify trust management techniques into four different categories. The work proposed a generic analytical framework sought to compare different trust management research prototypes using assessment criteria. overview and compares 30 representative research prototypes on trust management in cloud computing vis-à-vis the relevant research areas was carried out. A Trust Evaluation Model for QoS Guarantee in Cloud System was proposed by Hyukho et al. [7]. The work presented a trust model for efficient reconfiguration and allocation of computing resources satisfying various user requests. Probabilistic Latent Semantic Analysis (pLSA) methodology was employed to estimate the availability of each service/resource provision from the history of statistical usage data. Using pLSA, the system availability was estimated during specific periods and resources were allocated with a minimum failure rate and hence, it supports a more reliable cloud computing environment. A Trust model was developed which collects and analyses reliability based on historical information of servers in a Cloud data centre. Efficient utilization of the proposed trust model can be realized by cloud providers. In addition, provision of trusted resources and services to many users are s. Also, it increases the reliability of overall Cloud system by providing highly trustable computing resources. But the model only deals with reliability without considering other quality of service and trust issues.

Li et al., [8] proposed a trust model that enhances security and interoperability of cloud environment. The aim of the work is to develop a novel trust model which ensured the security of cloud entities both customers and providers in cross-clouds applications. Analysis of various trust models deployed in distributed environment was done. Thereafter, a novel cloud-based trust model that solves security issues in heterogenous environment coupled with incorporating customers’ choice enablement in services provision with resources availability in a given domain was developed. The model was domain-based, which divides one cloud provider’s resource nodes into the same domain and sets trust agent. Experimental result showed that the model can efficiently and safely construct trust relationship in cross-clouds environment and also establish trust relationship between customer and provider. The limitation of the work is that a cross-clouds security prototype system was not established. A Method for Trust Quantification in Cloud Computing Environments was done by Li et al. [9]. The aim was to propose a method for trust quantification based on fuzzy comprehensive evaluation theory for cloud computing to protect user data through trust quantification of cloud services. Fuzzy comprehensive evaluation method and information entropy theory were applied to determine the best combination of weights of various factors in the design of a preference trust quantification algorithm. Trust ontology and user preference definition of trust values were introduced for clouds services. Thus, by enhancing the existing trust concepts, based on dynamic requirements, some cloud service attributes layered service representation for trust preference was introduced and then the fuzzy comprehensive evaluation theory to perform trust quantification was applied. In addition, simulation experiment to demonstrate that the proposed approach can help users achieve more benefits and protect privacy. The proposed work was opined to be deployed to protect cloud users’ data and contain services providers’ malicious behavior.

3 METHODOLOGY

This study employed Simulation method of performance evaluation with the existing trust models using Java NetBeans integrated development environment (IDE) and evaluating their performances, the work involves 2 steps: algorithm description and trust evaluation. The simulation results were obtained using several experimental scenarios, exported in a csv file and imported into a R Environment where the results are presented. Experiments are needed to be performed on a repeatable, dependable, and scalable environment, which is not possible in the already existing world cloud because of the differences in the trust models being evaluated. So, to obtain a holistic platform used in software for modelling environment in cloud computing and perform testing, a simulator called CloudSim is used. By using CloudSim, specific system design issues were focused on that was used in investigating, without being bothered with details as relating to low level-based infrastructures and services in cloud.
3.1. Datacentre: The core infrastructure level services were modelled by (hardware, software) which is being offered in Cloud by resource providers. A set of compute hosts which could be either homogeneous or heterogeneous are covered regarding with their configurations of resource (capacity, memory and storage). Furthermore, every Data centre has a component where a generalized resource provisioning component were instantiated in order to implement set of policies that allocates bandwidth, memory, and storage devices.

3.2. Datacentre Broker: A broker is being modeled by this class, which mediates between service providers and users which depends on users’ QoS requirements and deploying tasks used in services operated across Clouds. The way VM provisioning requests are submitted to datacenters and the way cloudlets are submitted was modified and it was enhanced by adding the Service Dir Trust simulation entity class were performed thereby allowing us to define cloud users, configure their trust values, specify trust weights and other essential trust parameters.

3.3. SAN Storage: A storage area network is being modeled by this class which is available to Cloud-based datacenters in clouds large portions of data are stored. In SANS storage, a simple interface is implemented that could be used to simulate storage and retrieval of data regarding of the amount, which is subjected at any time to network bandwidth is available. Accessing files used by SAN during processes for task unit execution incur delay which be additional., due to time elapsed for transferring the required data files through the datacenter internal network.

3.4. Cloud Coordinator: This abstract class monitoring the internal state of a data centre occurs periodically in terms of simulation time. The specific event that triggers the competing VMs deployed across the datacenter.

3.6. Memory Provisioner: This component models policies for allocating physical memory spaces to the competing VMs.

3.7. VM Provisioner: This abstract class represents the provisioning policy that a VM Monitor uses for allocating VMs to Hosts in a datacenter meets the memory, storage, and availability requirement for a VM deployment. The default strategy is to allocate the host with less running VMs receives the next VM. To change this behavior, extend VM Allocation Policy implementing optimize Allocation method in order to allow VM allocation to the first available host that meets the aforementioned requirements for achieving optimized allocations.

3.8. VM Scheduler: Vm Scheduler Time Shared was used as the scheduling policy which means that the fraction of processor elements is shared among the VMs and the VMs run simultaneously.

3 Simulation Entities Relationship

The Data center Broker is responsible for mediating between users and service providers depending on the users’ requirements in the cloud. D2atacenter are resource providers; it is composed of a set of hosts which is responsible for managing VMs during their lifecycles. Host is associated to a data centre, it executes actions related to management of Virtual machine like creation and destruction of VMs, it has defined policy for providing memory and bandwidth. VM runs inside a Host sharing the Hostlist with other VMs. Processing of task units (Cloudlets) is handled by the respective VMs, each VM has a host which can submit cloudlets to the VM to be executed. cloud; the allocation of VMs for specific applications to of Provisioner.

4 Enemies Communication in The Simulator

The Figure 2 depicts communication flow between core CloudSim entities. At the beginning of a simulation, each Datacentre entity registers with the Cloud Information Service (CIS), the CIS is an entity that provides resource registration and indexing which allows entities to register themselves with the CIS.
Next, the Datacenter broker acts on behalf of the users to identify suitable Cloud service providers through the CIS and negotiates with them for the allocation of resources that the application’s hardware and software requires. The CIS selects the available Host in a Datacenter that meets the application’s requirements, the Broker then access a component in the data centre that stores characteristics that is used by the Virtual datacentre that stores characteristics that is used by the Virtual Machine (VM) such as storage capacity and memory capabilities. The Host component is responsible for the instantiation of a VM and the set of Hosts are housed in a Datacenter, the Broker request for creation of VM from the Host component in a Datacenter. A method then is called that request that the VMs return the least completion time of the task units they are currently managing to the datacentre entity and the completed tasks are directly returned to the CloudBroker. Then, the CloudBroker requests that the datacentre destroy the VM. The data communication flow among entities during the simulation.

5 Algorithm Description

The adopted algorithm is:
Step 1: Input to the algorithm is a set W, which includes the weights of trust metrics. These weights are assigned by the Cloud consumer according to the level of impact specified.
Set W = {0.8, 0.4, 0.1, 0.6}
Set P = {C, PC, D, A}
where W is weight of parameters according their impact level, P is the parameters namely data confidentiality, process execution control, detection of malicious behavior and data availability respectively.

<table>
<thead>
<tr>
<th>Level for trust features</th>
<th>Range for specific impact level</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>0.7 &lt; value 1.0</td>
</tr>
<tr>
<td>Medium</td>
<td>Value</td>
</tr>
</tbody>
</table>

The essential trust requirements, the required trust levels and their corresponding desired weights are set. The four main levels for these requirements which are „High”, „Medium”, „Low” and „Very Low” are defined and any of the four options against each trust requirements are selected. The ‘High’ level corresponds to the specific range of values that lie between 0.7 and 1, which means if the Cloud consumer has very high priority for a trust requirement, the cloud user will select the ‘High’ level and assign a weight to this feature between 0.7 and 1. Similarly, ‘Medium’ level lies between 0.4 and 0.7, ‘Low’ level has the range from 0.1 to 0.4 and the ‘Very Low’ level corresponds to the values between 0 and 0.1.

Step 2: The second step calculates the trust features supported by all the trust models.

These features calculated for each trust model separately.
Step 3: A cumulative value is calculated for all the trust models.

Step 4: After this, by comparing the calculated Cumvalue of all the trust models, the largest cumulative value is found. This particular trust model will be selected as the most suitable model according to the level of trust features which is deduced by its cumulative trust value and weight.

Step 5: The one with the highest weight and having the largest numbers of elements is selected as the most secured trust model for cloud services.

The proposed algorithm comparing these models for trust would be simulated on the java version of CloudSim v4.0.0, using NetBeans IDE.

6 System Implementation And Results

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>ENTITIES</th>
<th>ENTITIES</th>
<th>VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Users</td>
<td>No of Users</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Cloudlets</td>
<td>No of Cloudlets</td>
<td>100-1000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Length</td>
<td>2000</td>
</tr>
<tr>
<td>3</td>
<td>Host</td>
<td>No of Hosts</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ram</td>
<td>512MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Storage</td>
<td>500GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bandwidth</td>
<td>10000</td>
</tr>
<tr>
<td>4</td>
<td>Virtual Machine</td>
<td>No of VMs</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type of Policy</td>
<td>Time Shared</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ram</td>
<td>512</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bandwidth</td>
<td>1000</td>
</tr>
</tbody>
</table>
Tests and evaluation undertook are presented in order to select the most secured trust model for cloud services. The tests were conducted on an Intel system having configuration: 1.60GHz with 1 GB of RAM running a java version 8.0.2 and JDK 1.8.

Trust evaluation was achieved with a simulated Cloud computing environment consisting of two data centers, a broker and a user, with series of experiments performed. The number of hosts in the data center in each experiment was varied from 100 to 1000 where each host was modelled to have a single CPU core (1000MIPS), 512MB of RAM memory and 1GB of storage. Scheduling policy for VMs was Time-shared, which meant all VMs were allowed to be hosted in a host simultaneously at a given instance of time. Users were modelled (through the DatacenterBroker) to request creation of 5 VMs, the VMs have the following constraints: 512MB of physical memory, 1 CPU core and 1GB of storage. The application unit was modelled to consist of 5 task units, with each task unit requiring 1000million instruction per second. As the goal of these tests were to evaluate the trust requirements directly in the trust models, no attention was given to the user workload.

The total delay in instantiating the simulation environment is the time difference between the following events: (i) the time at which the runtime environment (java virtual machine) is directed to load the CloudSim program; and (ii) the instance at which CloudSim’s entities and components are fully initialized and are ready to process events.
Feedback based trust models give good results. These models were compared with other based on four trustworthiness parameters which are data confidentiality, detection of malicious behaviour, data availability and process execution control. The trust models evaluated in this work, overall Certificate based trust models performs better than other trust models, while Agreement based and Feedback based trust models give good results. These analyses will help the Cloud consumers and the IT professionals in selection of an appropriate trust model in their trust evaluation requirements. The limitation is that this work did not feature all the security and trust issues in cloud services as it was too much to cover but the important ones with high severity were covered. It is recommended that Cloud computing should be fully embraced despite its security and privacy breaches.

8 CONCLUSIONS

The important trust features of the Cloud-based trust models were identified and presented. These features helped in identifying a reliable and secure trust model for the Cloud environment that completely met all the important trust requirements. In conclusion, the comparison of trust models in cloud computing services executed with the help of CloudSim simulator without the user workload traces was presented.

These models were compared with each other based on four trustworthiness parameters which are data confidentiality, detection of malicious behaviour, data availability and process execution control. The trust models evaluated in this work, overall Certificate based trust models performs better than other trust models, while Agreement based and Feedback based trust models give good results. These