2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks
(ICRCICN)

# *Implementation of Trust Model on CloudSim based on Service Parametric Model*

Samarth Sharma
M.Tech Scholar
Department of Computer Science and Engineering
SKIT, RTU
Jaipur, India

Mr Mehul Mahrishi
Senior Lecturer
Department of Computer Science and Engineering
SKIT, RTU
Jaipur, India

***Abstract*— Cloud Computing has a lot of research emphasis in recent years and it offers a virtual agenda of resource allocation of. In such a purely dispersed environment, an entity has freedom to use pool of resources. Due to compassion and vivacity of data or facts, such objects wish to access their specific closed resources. The user/consumer assumes good quality of service from a reliable service provider. The service provider, on the other hand assumes the cloud resources to be safe and it permits them to be exploited by a reliable consumer. To accomplish this, it is essential to create trust between entities of cloud across the cloud.**

**Trust facilitates users to select the best available service in a diverse cloud infrastructure. A trust model is introduced based on past authorizations and present competences of a cloud service provider. Trust value is calculated using three parameters i.e. capability, behavior and feedback. A trust model is proposed to implement this trust value in cloud environment. The research work determines that our proposed model achieves better results than the existing trust models.**

***Keywords*— Agenda, dispersed, compassion, vivacity, credulity, competence, cloudlets, broker, threshold, success rate, throughput, rating.**

## I. INTRODUCTION

Cloud computing is a model that enables appropriate and on-demand network access to a common pool of computing resources that can be quickly configured, provisioned and released with minimal service provider's interaction [1].

A CloudSim is a new, widespread and extensible simulation toolkit and application that enables unified modeling, simulation and experimentation of developing cloud based computing systems, set-ups and presentation environments for individual and internetworked clouds.

Trust is related to an entity's confidence in morality, credulity, capability and dependability of another entity [2]. Trust is a built-in component of money-making phase of cloud. An important aim of trust in cloud computing is to establish belief and confidence on cloud entities in the internet based dispersed environments.

### *A) Motivation*

The motive behind why trust is an important idea for modern organizations is that the relocation from centralized information systems to cloud based applications will cause the transactions have to span a number of organizations and domains, all of which may or may not be trusted to the same level. Hence, there is the need for a general-purpose, flexible trust management system that can traverse these complex trust areas [3].

### *B) Background*

#### *1) Need of Cloud*

In the 1980s and 1990s, with the rise of PCs, client/server provided the ability to split the application tier away from server tier [4]. This was done to support distributed clients running richer user interfaces and also to reduce cost by offloading the user handling.

2000 onwards, as power and space became more expensive, concept of virtualization started to become established. Cloud computing takes these concepts further by allowing self-service, metered usage and more automated dynamic resource and workload management practices.

#### *2) Need of Trust in Cloud*

Trust and trustworthy domains are needed to make cloud computing smarter where resources can be used and services can be deployed safely by an entity. In such a situation the entities such as service provider and user/consumer can't control completely to each other. The user/consumer desires good quality of service from a reliable service provider. The service provider on the other hand desires the cloud resources to be secure and it allows them to be consumed by a reliable consumer. To accomplish this, it is essential to launch trust between the service provider and the user across the cloud.

## II. LITERATURE SURVEY

The literature focuses on identity and reputation as the bases of establishing trust between consumer and service provider.

Identity based model deals with authentication and authorization of an entity, but does not promise speed, consistency and excellence of service, results as loss to the users. Hence, this doesn't guarantee the quality of service for consumer [5].

On the other hand, reputation based trust management systems studied that have dealt primarily based on history of the knowledge from others [2].

*A. Definitions and Characteristics*

All definitions and characteristics are collected from the base research papers [2] and [5]. Before ongoing with the related work, all are significant to specify.

*1) Availability (AV)*

Availability is the grade to which a system or component is accessible and working when required for use.

*2) Reliability (RE)*

Reliability of a cloud resource is an amount of accepted jobs that are completed successfully by the cloud resource.

*3) Data Integrity (DI)*

Security is a key factor that requires special care in cloud. Data integrity is a general term that comprises accuracy, privacy and security of data.

*4) Turnaround Efficiency (TE)*

The exact time between a job submission by a user and executed job's delivery to the user is actual turnaround time..

*5) Cloud software package as a Service (SaaS)*

Software as a service (SaaS) is a software authorizing and distribution model in which software is authorized on a payment basis and is hosted centrally.

*6) Cloud Platform as a Service (PaaS)*

Platform as a service (PaaS) is a type of cloud computing service that offers a platform permitting customers to design, run and manage web applications without the complication of building and preserving the infrastructure usually linked with developing and launching an application.

*7) Cloud Infrastructure as a Service (IaaS)*

The aptitude provided to the consumer is to delivery of storage, processing, networks and other basic computing resources wherever the consumer is capable to organize and run variable software system, which may hold applications and system software.

*8) Service Level Agreement (SLA)*

A service-level agreement (SLA) is a part of a provision where a service is properly defined.

*B. Existing Trust Models*

We will mainly prefer research paper [5] "A trust model of cloud computing based on Quality of Service" for describing existing work. This model basically includes study of some other papers, hence we will also discuss them briefly.

Paul D Manuel [2] proposed a novel trust management system for cloud computing for IaaS Providers.

Grandison [6] has studied a number of trust models existed stating trust as the configuration of several attributes such as honesty, reliability, dependability, truthfulness, competence, security, timeliness, Return on Investment (ROI) and Quality of Service (QoS) in the framework of an environment.

Saurabh Ganeriwal [7] has developed the reputation based framework for high integrity sensor networks.

Alfarez Abdul-Rahman [8] has recommended the reputation is a belief about an agent behavior based on the information about or observations of its past behavior.

Josang and Claudia Keser [9] have proposed the various methods related to online activities where trust is appropriate and there is a requirement for trust management.

Nuno Santos [10] has proposed a strategy of trusted cloud computing platform (TCCP). This enables IaaS providers (e.g. Amazon EC2) to provide a closed box execution environment that promises sound execution of guest virtual machines.

Rochwerger [11] has proposed the reservoir model and architecture for Open Federated Cloud Computing.

Josang and Roslan Ismail [12] have proposed reputation is the belief about the persons or things character or standing

Matt blaze [13] has proposed decentralized trust management in which he described the parts of trust management problem as framing security policies.

Nitin P. Doiphode [14] has proposed data usage accountability in cloud computing for trust measurement.

## III. RESEARCH GAP AND PROPOSED WORK

*A. Research Gap*

- The trust value is calculated on client side i.e. there is not much role of broker in selection of service provider.
- Trust value is not much efficient as it is calculated on the basis of limited parameters and required values of these parameters are provided by inefficient/nontechnical user.
- It is desirable to refine trust using some additional parameters such as success rate, throughput and feedback.
- It is also desirable to introduce the role of broker (selection of service provider and submission of requirements in case of inefficient/nontechnical user) in trust management system.

*B. Proposed Trust Model*

The proposed cloud trust model is implemented on CloudSim. Hence, we have named this model as CloudSim trust model (CSTM). This model is integrated with the trust resource broker and trust estimator that computes the trust value of different cloud service providers (CSPs).

*1) Architecture of Proposed Trust Model*

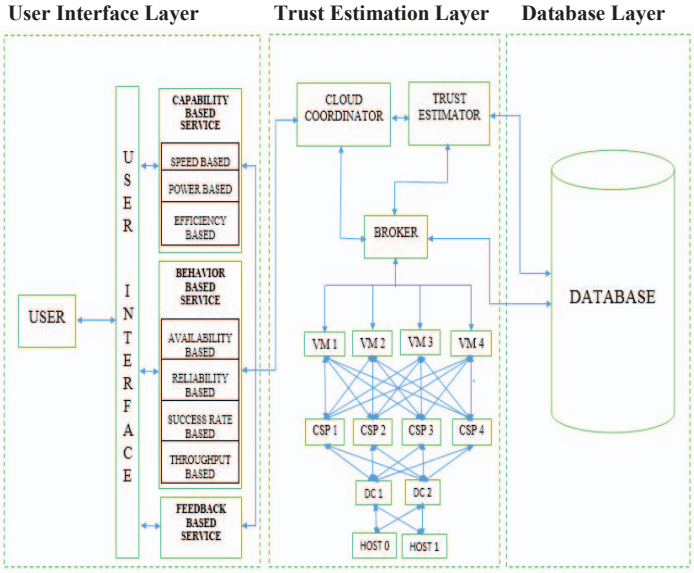


**Figure 3.1: Architecture of Proposed Trust Model**

*2) Algorithm of Proposed Trust Model*

**Input**

- Cloud user initially provides the list of CSTM requirements and parameters (capability based, behavior based and feedback based) with the weights for each type of requirement while submitting the job that he wants to execute. Let,

  $W_1$ = Capability based trust weight,
  $W_2$ = Behavior based trust weight and
  $W_3$ = Feedback based trust weight

  The values $W_1$, $W_2$ and $W_3$ are provided by user in such a way that
  $W_1 + W_2 + W_3 = 1$ and
  $W_1$, $W_2$ and $W_3 \leq 0.5$

**Method**

- Cloud coordinator collects these CSTM requirements with their weights, parameters, and incoming job and divides the job into N different cloudlets (each of equal size).
- Cloud coordinator forwards these CSTM requirements, weights, parameters and cloudlets to the trust estimator.
- User/broker provides the values of CSTM parameters (capability based and feedback based) to trust estimator. Broker forwards the values of CSTM parameters (capability based and behavior based) provided by all CSPs, to the trust estimator.
- Trust estimator calculates all the three types of trust values (capability based, behavior based and feedback based) and the averages of above three trust values for each CSP and returns these values to broker.

  **(i) Capability based trust value ($T_C$) = $T_S$ * $T_P$ * $T_E$**

  Where $T_S$ = Speed based trust value,
  $T_P$ = Power based trust value and
  $T_E$ = Efficiency based trust value

  **(ii) Behavior based trust value ($T_B$) = $T_A$ * $T_R$ * $T_{SR}$ * $T_T$**

  Where $T_A$ = Availability based trust value,
  $T_R$ = Reliability based trust value,
  $T_{SR}$ = Success Rate based trust value and
  $T_T$ = Throughput based trust value

  **(iii) Feedback based trust value ($T_F$) = R ÷ $t_h$**

  Where R = Average rating of given feedback ratings given by user and broker to CSP

  And $t_h$ = Threshold value

- Broker selects the CSP that contains maximum average trust value among given average trust values of all CSPs and returns that CSP to the trust estimator.

**Output**

- Trust estimator calculates the resultant trust value of the selected CSP.

  **Resultant trust value (T) = $W_1$*$T_C$ + $W_2$*$T_B$ + $W_3$*$T_F$**

- Trust estimator returns the resultant trust value to the user through cloud coordinator and updates the existing trust value in database as stores the resultant trust value.

*3) Cloud Trust Estimation*

The resultant trust value for proposed trust model can be calculated using following key components:

*a) Capability Based Trust Estimation (CBTE)*

The capability based trust value can be calculated using speed based parameters (processor and ram speed), power based parameters (bandwidth and latency) and efficiency based parameters (turnaround time).

Capability Based Trust value **($T_C$) = $T_S$ * $T_P$ * $T_E$**

Here, (i) **$T_S$ = (2*P + R) $_{Actual}$ ÷ (2*P + R) $_{User\ Required}$**,
(ii) **$T_P$ = (BW ÷ L) $_{Actual}$ ÷ (BW ÷ L) $_{User\ Required}$** and
(iii) **$T_E$ = TURNAROUND TIME $_{User\ Required}$ ÷ $_{Actual}$**

Where P, R, BW and L are defined and explained in table.

TABLE I: Capability Based Service required by User and provided by CSPs

| **CSTM PARAMETERS (Capability based)** | **By User/ Broker** | **By CSP1** | **By CSP2** | **By CSP3** | **By CSP4** |
|---|---|---|---|---|---|
| **1) SPEED BASED** | | | | | |
| **(i) PROCESSOR SPEED (P) (GHz)** | | | | | |
| (a) Clock speed | 3.07 | 3.01 | 3.02 | 3.03 | 3.04 |
| (b) Cache speed | 1.23 | 1.204 | 1.208 | 1.212 | 1.216 |
| (c) Bus speed | 0.533 | 0.430 | 0.480 | 0.500 | 0.520 |
| **TOTAL PROCESSOR SPEED (P)** = Clock + Cache + Bus speed | **4.833** | **4.644** | **4.708** | **4.742** | **4.776** |
| **(ii) RAM SPEED (R) (GHz)** | | | | | |
| (a) Onboard RAM speed | 0.307 | 0.301 | 0.302 | 0.303 | 0.304 |
| (b) Bus speed | 0.533 | 0.430 | 0.480 | 0.500 | 0.520 |
| (c) SRAM speed | 0.1535 | 0.1505 | 0.1510 | 0.1515 | 0.1520 |
| (d) DRAM speed | 0.0307 | 0.0301 | 0.0302 | 0.0303 | 0.0304 |
| **TOTAL RAM SPEED (R)** = Onboard RAM + Bus + SRAM + DRAM speed | **1.0242** | **0.9116** | **0.9632** | **0.9848** | **1.0064** |
| **2) POWER BASED** | | | | | |
| **(i) BANDWIDTH** | | | | | |
| (a) Write | 9519 | 9500 | 9505 | 9510 | 9515 |
| (b) Read | 7182 | 7100 | 7110 | 7120 | 7130 |
| **NET(AVERAGE) BANDWIDTH(BW) (Mbps)** | **8350.5** | **8300** | **8307.5** | **8315** | **8322.5** |
| **(ii) LATENCY(L) (Nano Second)** | **90.7** | **98** | **96** | **94** | **92** |
| **3) EFFICIENCY BASED** | | | | | |
| **TURNAROUND TIME (Minute)** | **100** | **108** | **106** | **104** | **102** |

Hence,

(i) Capability Based Trust value for **CSP1 ($T_{C1}$)** = 0.9541* 0.9199 * 0.9259 = **0.8605**

(ii) Capability Based Trust value for **CSP2 ($T_{C2}$)** = 0.9709 * 0.9399 * 0.9434 = **0.8609**

(iii) Capability Based Trust value for **CSP 3 ($T_{C3}$)** = 0.9752 * 0.9608 * 0.9615 = **0.9009**

(iv) Capability Based Trust value for **CSP 4 ($T_{C4}$)** = 0.9877 * 0.9825 * 0.9804 = **0.9514**

*b) Behavior Based Trust Estimation (BBTE)*

Behavior based trust value can be calculated using parameters such as availability, reliability, success rate and throughput for each CSP [15].

Here incoming job is divided into N number of equal sized cloudlets. Then cloud coordinator forwards the cloudlets.

Given,

(i) Total number of cloudlets submitted (N) = 20
(ii) Number of VMs (Virtual machines) = 4
(iii) Number of CSPs (Cloud service providers) = 4
(iv) Number of DCs (Data centers) = 2
(v) Number of Hosts = 2

- Cloudlets 0-6 sent to VM 1
- Cloudlets 7-11 sent to VM 2
- Cloudlets 12-16 sent to VM 3
- Cloudlets 17-19 sent to VM 4

Behavior based Trust value **($T_B$) = $T_A$ * $T_R$ * $T_{SR}$ * $T_T$**

Here, **$T_A$ = A ÷ N,**

**$T_R$ = B ÷ A,**

**$T_{SR}$ = C ÷ B and**

**$T_T$ = C ÷ t**

Where **N = Total number of cloudlets submitted to VMs**

**A = Total number of cloudlets accepted by VMs**

**B = Total number of cloudlets accepted by CSPs**

**C = Total number of cloudlets accepted by DCs**

**t = Total time to execute finally accepted cloudlets**

The values of A, B, C and t for each CSP are shown in table.

TABLE II: Behavior Based Service provided by CSPs

| **CSTM PARAMETERS (BEHAVIOR BASED)** | **CSP1** | **CSP2** | **CSP3** | **CSP4** |
|---|---|---|---|---|
| **AVAILABILITY based:** | | | | |
| N | 20 | 20 | 20 | 20 |
| A | 14 | 12 | 13 | 14 |
| **RELIABILITY based:** | | | | |
| A | 14 | 12 | 13 | 14 |
| B | 10 | 10 | 09 | 12 |
| **SUCCESS RATE based:** | | | | |
| B | 10 | 10 | 09 | 12 |
| C | 06 | 07 | 08 | 09 |
| **THROUGHPUT based:** | | | | |
| C | 06 | 07 | 08 | 09 |
| t (Second) | 09 | 09 | 09 | 09 |

Hence,

Behavior based Trust value for **CSP1 ($T_{B1}$)** = 0.7000 * 0.7143 * 0.6000 * 0.6667 = **0.2000**

Behavior based Trust value for **CSP2 ($T_{B2}$)** = 0.6000 * 0.8333 * 0.7000 * 0.7778 = **0.2722**

Behavior based Trust value for **CSP3 ($T_{B3}$)** = 0.6500* 0.6923 * 0.8889 * 0.8889 = **0.3556**

Behavior based Trust value for **CSP4 ($T_{B4}$)** = 0.7000 * 0.8571 * 0.7500 * 1.000 = **0.4500**

*c) Feedback Based Trust Estimation (FBTE)*

Feedback based trust value ($T_F$) is calculated by dividing the average value of ratings given by customer and broker to CSP with the threshold value received by broker from database. We can understand it by giving the example using table.

TABLE III: Feedback Based Ratings provided by User and Broker to CSPs

| CSTM PARAMETERS (Feedback based) | CSP1 | CSP2 | CSP3 | CSP4 |
|---|---|---|---|---|
| User Rating ($R_U$) | 7 | 7 | 9 | 8 |
| Broker Rating ($R_B$) | 3 | 5 | 7 | 6 |
| Average Rating (R) = ($R_U + R_B$) ÷ 2 | 5 | 6 | 8 | 7 |
| Threshold value ($t_h$) | 8 | 8 | 8 | 8 |

**Feedback based Trust value ($T_F$) = R ÷ $t_h$**

- **For CSP 1: $T_{F1}$ = 5 ÷ 8 = 0.6250**
- **For CSP 2: $T_{F2}$ = 6 ÷ 8 = 0.7500**
- **For CSP 3: $T_{F3}$ = 8 ÷ 8 = 1.0000**
- **For CSP 4: $T_{F4}$ = 7 ÷ 8 = 0.8750**

*d) Resultant Trust Estimation (RTE)*

We summarize all three types of trust values for all CSPs into a table.

TABLE IV: All trust values for all CSPs:

| Trust value | CSP1 | CSP2 | CSP3 | CSP4 |
|---|---|---|---|---|
| Capability based ($T_C$) | 0.8605 | 0.8609 | 0.9009 | 0.9514 |
| Behavior based ($T_B$) | 0.2000 | 0.2722 | 0.3556 | 0.4500 |
| Feedback based ($T_F$) | 0.6250 | 0.7500 | 1.0000 | 0.8750 |
| **Average ($T_{AV}$)** | **0.5618** | **0.6277** | **0.7521** | **0.7588** |

- Here, we can observe that average trust value ($T_{AV}$) is maximum for **CSP4** among all CSPs.
- Hence, user will select **CSP4** as required **CSP.**
- Now, we calculate the CloudSim trust value (CST) as trust value for CSP4
  - **$T_C = T_{C4} = 0.9514$**
  - **$T_B = T_{B4} = 0.4500$**
  - **$T_F = T_{F4} = 0.8750$**

**CloudSim trust value (CST) = $W_1$*$T_C$ + $W_2$*$T_B$ + $W_3$*$T_F$**
Here, **$W_1$ = 0.5, $W_2$ = 0.2 and $W_3$ = 0.3**
Hence, trust value for CloudSim trust model is:
**CST** = 0.5*0.9514 + 0.2*0.4500 + 0.3*0.8750
= **0.8282**
The trust value (CST) is returned by trust estimator to cloud user through cloud coordinator. Trust estimator also updates the existing trust value in database as it stores CloudSim trust value**.**

## IV. RESULTS AND COMPARISONS

We compare our proposed trust model with the existing trust models such as FIFO model, QoS trust model [5] and combined trust model [2] on the basis of trust value.

Trust value for FIFO and QOS model

**T= w1*AV+w2*RE+w3*DI+w4*TE**

Where, w1 = Availability based trust weight = 0.2,
w2 = Reliability based trust weight = 0.2,
w3 = Data integrity based trust weight = 0.5 and
w4 = Turnaround efficiency based trust weight = 0.1

- **For FIFO model**

Initial trust value **$FT_1$ = 0.46**
Final trust value **$FT_2$ = 0.32**
Average trust value **FT = 0.39**

- **For QoS trust model**

Initial trust value **$QT_1$ = 0.674**
Final trust value **$QT_2$ = 0.84**
Average trust value **QT = 0.757**

- **For combined trust model [2]**

Trust value using resource $R_1$: **$CT_1$ = 0.822**
Trust value using resource $R_2$: **$CT_2$ = 0.861**
Trust value using resource $R_3$: **$CT_3$ = 0.242**
Average trust value **CT = 0.642**

- **For Cloudsim trust model**

Resultant CloudSim trust value: **CST= 0.8282**

Now, we compare resultant trust value of proposed CloudSim trust model with the average trust values of existing trust models using column chart.

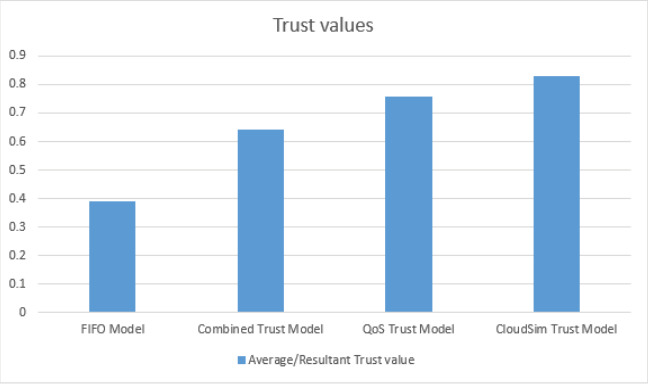


Fig. 1. Comparison of Trust Values of Existing and Proposed Trust Models

- From the given chart we can observe that FT<CT<QT<CST i.e. CSTM provides maximum trust value than existing models.

CSTM is more efficient than existing trust models on the basis following points also:

- CSTM is implemented on CloudSim. Hence, it is more widely adoptable than existing models.
- As the model is implemented on CloudSim. Hence, there is no need to introduce Integrity based trust parameters that are used by existing models.
- CSTM is purely mathematical. Hence, it is simpler than all existing models

## V. CONCLUSION AND FUTURE WORK

### *A. Conclusion*

- We have proposed CloudSim trust model (CSTM) implemented on CloudSim. The trust estimator estimates the value of trust of cloud resources delivered by the service providers and CSP selection based on the computed trust value improves the quality of cloud services.
- In capability based trust estimation, trust value of a CSP is estimated on the basis of parameters such as processor speed, RAM speed, bandwidth, latency and turnaround time.
- In behavior based trust estimation, trust value of a CSP is estimated on the basis of parameters such as availability, reliability, success rate and throughput.
- In feedback based trust estimation, trust value of a CSP is estimated on the basis of parameters such as user rating, broker rating given to a CSP and threshold value of feedback.
- Resultant trust estimator calculates the resultant trust value of CSP also known as CloudSim trust value (CST) by multiplying each type of trust value to corresponding weight assigned by user and finally by adding them.

### *B. Future Work*

- We can improve the work by adding several other trust parameters to calculate trust value of model.
- Interactive user interface can be prepare for both CSP and user to enhance transparency in the system and ease for cloud users.
- This model can also be extended to deal with various fault-tolerance techniques and both research institutes and companies can follow the approach to implement trust.

## ACKNOWLEDGEMENT

The authors would like to thank Dr. Siddhartha Bhattacharyya General Chair (ICRCICN-2015), RCC Institute of Information Technology, Kolkata, India, for providing the necessary support for this publication.

## REFERENCES

[1] Ian Foster, "Cloud Computing and Grid Computing 360-Degree Compared", Department of Computer Science, University of Chicago, Chicago, IL, USA

[2] Paul D Manuel, "A Novel Trust Management System for Cloud Computing - IaaS Providers", Department of Information Science, College for Women, Kuwait University, Kuwait

[3] Tyrone Grandison, "A Survey of Trust in Internet Applications", Imperial College, Department of Computing, 180, Queen's Gate, London SW7 2BZ, UK

[4] Aradhana, "Trust based Identity provisioning for cloud computing", computer science and engineering department, Thapar University, Patiala-147004, June 2011

[5] Paul Manuel, "A trust model of cloud computing based on Quality of Service", Department of Information Science, Kuwait University, Kuwait

[6] T. Grandison, "A Survey of Trust in Internet Applications", Imperial College, Department of Computing, 180 Queen's Gate, London SW7 2BZ, UK

[7] S. Ganeriwal, "Reputation-Based Framework for High Integrity Sensor Networks", Networked and Embedded Systems lab, 56-125B, EE-IV, University of California, Los Angeles

[8] Alfarez Abdul-Rahman, "Supporting Trust in Virtual Communities", Department of Computer Science, University College London, Gower Street, London WC1E 6BT, United Kingdom

[9] Audun Josang, "Can We Manage Trust?" DSTC UQ Qld 4072, Australia

[10] Nuno Santos, "Towards Trusted Cloud Computing" Proceedings of the Workshop on Hot Topics in Cloud Computing (HotCloud), San Diego, CA, June 2009

[11] B. Rochwerger, "The Reservoir model and architecture for open federated cloud computing" IBM Journal of Research and Development, Monday, 6 April 2009, Allen Press, Inc. ibmr-53-04-04

[12] Audun Josang and Roslan Ismail, "A Survey of Trust and Reputation Systems for Online Service Provision", Distributed Systems Technology Centre University of Queensland UQ Qld 4072, Australia

[13] Matt Blaze, "Decentralized Trust Management", Proceedings of IEEE Conference on Security and Privacy, IEEE Computer Society. Oakland, CA, USA, pages 164-173, May 1996

[14] Nitin P. Doiphode "A Survey on Accountability of Data usage in Cloud Computing", International Journal of Science, Engineering and Technology Research (IJSETR) Volume 4, Issue 3, March 2015

[15] Abdallah M'Hamed, "Towards a Context Aware Modeling of Trust and Access Control Based on the User Behavior and Capabilities", ICOST 2013, Jun 2013, Singapore

**Samarth Sharma** received the B.Tech degree in Computer Science and Engineering from PCE (RTU), Jaipur, Rajasthan, India, in 2013.
He has completed the degree of M.Tech degree in Computer Science and Engineering from SKIT (RTU), Jaipur, Rajasthan, India, in 2015.
His research interest is cloud computing.

**Mehul Mahrishi** is currently working as an Assistant Professor in the department of computer Science at the SKIT (RTU), Jaipur, Rajasthan, India.
Prior to this he has also served as an Assistant Professor at Central University of Rajasthan, Ajmer, Rajasthan.
He has received his B.Tech degree in Computer Engineering from the State University of Rajasthan and M.Tech degree in Information Communication from Gyan Vihar University, Jaipur.
He also published a number of papers in national and international Journals, conferences including 3rd International Conference on Machine Learning and Computing (ICMLC 2011), 3rd IACC 2013 and chapters in books, and participated in a range of forums by Infosys, TCS, and WIPRO-Mission 10X, IBM etc.