META:Meta-heuristic Enhanced Trust Assessment for Cloud Infrastructure

MandeepKaur

Department of Computer Science

Punjabi University

Patiala-147002, India

mkw.mandeep@gmail.com

Gagandeep

Associate Professor (Department Of Computer Science)

Punjabi University

Patiala-147002, India

gdeep.pbi@gmail.com

***Abstract*-Now days, Cloud Computing is having enormous thrust areas in research and development despite lots of work in the stream. There are number of research issues in this segment including trust management, privacy, security, integrity and power aware data centres. A significant and lots of work is done under each domain still there is huge scope of research. Trust management is one of the generalized and key areas in which colossal work is going on. As per the reports and corporate whitepapers, trust refers to as: "Generally an entity can be said to 'trust' a second entity when the first entity makes the assumption that the second entity will behave exactly as the first entity expects. Trust is the establishment of confidence that something will or will not occur in a predictable or promised manner. The enabling of confidence is supported by identification, authentication, accountability, authorization, and availability." A number of algorithms and approaches are developed so far which are integrated in the trust architectures including cryptography, nature inspired approaches and many others. In this research work, the existing approach of gene based architecture for trust management in cloud is adopted in which number of chromosomes and gene based libraries are integrated. The classical work is effective but there was scope of improvements and further enhancement of results. For improvements in the classical work is enhanced using simulated annealing that is very effective and making use of metallurgy based implementations. In metallurgy, the temperature factor is taken for the forging and development of metal components. The freezing point is achieved in a loop of down level temperature. In this work, the simulated annealing based implementation is used with the integrated with dynamic security key for enhanced security trust architecture. The proposed META (Meta-heuristic Enhanced Trust Assessment) architecture is giving effective results in terms of turnaround time, security factor, cost, complexity and trust value.**

Keywords-Cloud Computing, Genetic Algorithm, META Approach, Security Concerns, Simulated Annealing, Trust Management.

I. INTRODUCTION

Cloud computing refers to pool of services which are offered to a consumer on pay per use basis. It helps IT companies to focus on their business or strategic projects rather than technical aspects. It elevates the need of buying costly servers. Users need not to bother about installation and software maintenance. Mainly three service model are offered by cloud which are Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a service (SaaS). At SaaS level applications are hosted by providers on network, these services are used by customers over internet on demand basis. A web browser is used to access different software's from the cloud providers. A user need not to install software on his machine, only an instance of software is needed. For example Google Apps, SQL Azure. In PaaS model as name implies it gives platform to build various applications. Various facilities offered by PaaS to deploy applications include application designing, development, testing and hosting [10]. Providers give servers and network for application deployment without buying actual hardware and software. The downfall of PaaS is portability problem. Users have to pay high cost if he wants to migrate from one provider to another. Iaas is model in which only hardware is used by services for their operation. Users need not to purchase costly servers; they can rent server and network space, memory, storage space etc. This reduces hardware maintenance at local level. Some of IaaS vendors are Amazon Simple Storage Service (S3) for database backup, Amazon Elastic Cloud Computing (EC2), Go Grid, VMWare etc.

A. Cloud Security

As companies are placing more information on cloud, threats are increasing about the safety of environment. Security and data protection are one of serious concern in cloud development and adoption.Restricted manipulation on

data can cause miscellaneous security problems which include data outflow, unprotected interface, resource sharing, data availability and inner attacks [9]. As all aware cloud is increasingly accepted, but still people have certain confusion in their mind that their data might not be secure at other end. Security in cloud computing is one of big matter because equipment used to deliver services does not own by users. The consumers have no authority, nor any knowledge of, what is happening with their data. Service Provider Layer have various security concerns some of them are Data transmission, Privacy, People and Identity, Audit and Compliance, integrity and Binding problems. Security difficulties faced by Virtual Machine Layer are VM Escape, VM Sprawl, Insecure VM migration, Malicious VM Creation, Cloud legal and Regularity complains Identity and Access management. Data Centre are vulnerable to different type of attack at Physical and Network level.

B. Overview of Trust

Trust is a social problem. There are lots of definitions of trust. Basically trust refers to confidence or belief of one entity on other. One cannot build trust in a day. It is normally based upon provider's position in market. As users are putting their resources on provider's datacentres so there is major concern about the trustworthiness of providers and services. Two parties are involved in any trusted relationship: one is trusting party (i.etrustor) and other party to be trusted (i.e trustee) [1]. Various risks are involved: location security risk, data disclosure problem, data misplacement issue, data investigation concern. In cloud environment hostile user can add malicious code and take CPU space, resources and time. To model attractive cloud computing, trust should be introduced and there should be some trustworthy regions where users can deploy their applications and use resources safely.

II. RELATED RESEARCH

Trust is a burning issue these days. Lots of researchers have worked on trust issues. Various trust management model have been used to assessfaithfulness of cloud service providers. The work of various researchers is listed below.

A. Literature Survey

DimitriosZissis et al. (2010) introduced a Trusted Third Party, that gurantees certain security attributes inside a cloud environment. A mixture of PKI (Public Key Infrastructure), SSO and LDAP can help to identify risks in cloud framework that deals with confidentiality, integrity, availability, authenticity. JiuyunXu et al.(2010) proposed a trust management scheme that distinguishes reputation of various user categories which is termed as local reputation.

Paul D Manuel et al.(2011) illustrated a novel trust model in which Trust Resource Broker is used to assess the cloud services of IaaS providers. The Broker is executed with the help of PERMIS authorization and Kerberos authentication. In this model trust value is evaluated depending upon the identity and behaviour of user. It applies the QoS metrics suitable for cloud resources.

Prajapati Kumar Somesh et al.(2013) introduced a trust management model to control trust at SaaS level. It also studied various kinds of trust like recommendation, direct and reputation trust.Xiaoyong Li et al. (2015) presented a T-broker scheme for effective matching of services to meet several user requests. A data brokering architecture which is built on trusted third party is implemented for numerous cloud environments, in given model T-broker behaves like aintimidator between service matching and trust management. Adaptive and hybrid trust model along with lightweight feedback is used to compute the final trust degree.

RathiKavita et al.(2015) discussed various trust issues along with the trust elements. It addresses the existing trust models for trust establishment among the cloud user and the cloud service provider. It concludes that most of the models lack transparency as their element for establishment of trust.

Talal H. Noor et al. (2015) designed a trust management architecture named "CloudArmor" that is based on reputation; it delivers a bundle of functionalities that present Trust as a Service (TaaS).A novel protocol is proposed to check the reliability of trust feedbacks. A novel protocol is proposed to check the reliability of trust feedbacks. It consists of credibility and availability model which are used to protect feedback from hostile users and to handle availability of trust management service.

Banerjee Soumya et al. (2015) proposed a rudimentary security model based on fuzzy logic, it is designed for middleware architecture of the cloud system to identify the anomalies.Christina Terese Joseph et al. (2015) presented a Novel family genetic algorithm for allocation of virtual machine. It presented a novel technique that uses family gene approach to allocate virtual machines.

BrototiMondal et al. (2015) presented a load balancing technique that is based on Simulated Annealing. It discussed comparative analysis between various algorithms like First come first serve(FCFS) , Round Robin(RR) and Stochastic Hill Climbing (SHC).

Gupta Sachin et al. (2015) discussed a Hash Key Based Effective Algorithm for Security in Cloud. In proposed work dynamic key is implemented at every step of data channel. It underlines implementation of secured dynamic key based algorithm. Syed Hamid HussainMadni et al. (2016) investigated various Meta-Heuristic techniques to allocate resources in IaaS clouds. It addresses various issues related to

VM allocation, Optimal Resource allocation and QOS aware resources allocation.

Talal H. Noor et al. (2016) proposed a trust a management framework that helps to address various challenges like personalization, identification, security privacy, scalability and integration. It consists of two sub components known as trust assessment and trust feedback.KanagasabapathyJayalakshmi et al. (2016) proposeda broker coordinator and two segmentation schemes named automaton segmentation scheme and query segment encryption scheme. These schemes are implemented to share routing function safely among brokering servers.G. JeevaRathanam et al. (2016) proposed a (TMWS) trust based Meta heuristic workflow scheduling. It implemented various trust strategies in workflow scheduling and trust policieswith meta-heuristic techniques are considered to overcome application threats.

III. PROBLEM FORMULATION

Maintaining consumers' secrecy is a difficult task because of the sensitive data present in communication between trust management service and consumers. To model attractive cloud computing, trust should be introduced and there should be some trustworthy regions where users can deploy their applications and use resources safely. The consumer always expects better Quality of Service from a service provider and the provider expects the cloud resources to be utilized by a trustworthy consumer. Trust Management and Security Enhancement is one of the prominent domain of research in cloud computing. A number of algorithms and multi-layered architectures are developed so far and still this area is under research.

IV.RESEARCH GAPS

In the classical approach, there is gene based architecture and flow for the optimization of results.
The classical trust management techniques are having number of pitfalls that takes more execution time and higher complexity with vulnerability factor that is the violation of trust managementThe basic solution obtained without further and effective meta-heuristic approach is not efficient in terms of the turnaround time and optimal resultsThe classical results are not effective in terms of multiple parameters including

a. Time Factor
b. Algorithmic Complexity
c. Turnaround Time
d. Overall Throughput
e. Cost Parameter
f. Performance

V. PROPOSED METHODOLOGY – META FRAMEWORK

Trust Management is directly associated with CTP that is cloud trust protocol which was created in 2010 by the late Ron Knode of CSC and licensed for use by the Cloud Security Alliance (CSA) in 2011, itconsists of 23 criteria for cloud transparency. The Cloud Trust Protocol is planned to establish digital trust between a cloud computing customer and provider and create transparency about the provider's vulnerabilities, configurations, accountability, access,policy, authorization, anchoring and operating status conditions. In trust management and parameter optimization can be achieved using assorted approaches including heuristics and meta-heuristics. In case of heuristics, there are fixed mathematical formulations and there is very less scope of optimization because of local optima.

A. Trust Evaluation Criteria and Associated Components

*Trust Initialization:*Trust is the key parameter and aspect in the proposed methodology for security and integrity in the cloud infrastructure. In the base work, there are specific formulations for trust evaluation and measurement based on the allocation of resource to the cloud users.

In META model for trust and related integrity, a specific set of formulations are used which are directly associated with the dynamic security key and integration of allocated virtual machine to the cloud users.

In this case, the trust value is binary in nature which accepts true or false based trust allocation and this is effective because binary trust value ensures whether there is any inclusion of trust or not. Using different formulations as in the base work can create the fix and biasing can be done. This framework is not biased because it is directly dependent on the allocation of resources along with the security key. If security key is empty, the trust value is discarded and overall integrity is compromised.

B. Flow for Evaluation and Allocation of Trust in the Overall Architecture

1. Application Activation with Cloud Components and Initialization Factors
2. Initialize Trust Value as 0 with possible combinations (binary trust in this case)
3. Cloud Data Centre and Running Environment Setup
4. Random Hash Key Process
    a. Generate new random number
    b. Max. threshold setup and initialization
    c. Dataset with empty value for further storage from hash values
    d. Generation of ASCII code and dataset with encrypted string

   e. Unification / Fusion of strings to strengthen key
   f. Final generation of security and unified message digest with hash key
   g. Byte to Hex Conversion to transmission via cloud channels
   h. String buffers activation and append to the cloudlet for security and integrity for overall trust
5. Trust Value Migration initiates and moves with the cloud service to user end
6. Cloud user panel
   a. Fetching of cloud services
      i. Cloudlets
      ii. bandwidth
      iii. migration values
      iv. trust
   b. if (trustvalue) != (notNull) or ((trustvalue) != (earliertransmitted))
      i. goto step 1
      ii. else
      iii. stop and terminate with success
7. Record logs and trust factors with cumulative score
8. Investigate the visibility score and trust parameters for the dynamic components at each phase

C. Evaluation of Metrics for Performance and Related Parameters

1. Initialize and activate the evaluation parameters
   a. Cost
   b. Complexity
   c. Efficiency
   d. Waiting Time
   e. Execution Time (ext)
2. ext=0, wt=0;
3. timer1=millitime;
4. Initialization of objects and components for Cloud Trust Evaluation
   a. Internet Boundaries and Characteristics
   b. Bandwidth Configuration Panel
   c. Dimension and Aspects of Cloud with Speed Matrix
   d. Cloud Controller for CardLayout screen
5. Activation of new Cloud and Data Center
   a. Mapping of HashMap
      i. Dynamic View of Global Delivery of Cloud Components
   b. Mapping of screenController with CloudCardLayout
6. Setting Up the Dimensions for Size of VM, Boundaries and Security
7. Initialize the Module to activate, log and monitor the Internet Behavior
8. Logging and Fetching of Results
9. Timer2=millitime;
10. Evaluate ext=timer2-timer1
11. Log and View simulation in a new thread, because this is the Event-dispatch thread
12. Analyze results
13. If (results == successful), stop and terminate
14. else goto step 4

D. Apply Simulated Annealing Algorithm to Select Optimal Result

The work is based on simulated annealing. Simulated annealing is the automated version of annealing process in metallurgy in which the development and formation of metal components are done from melting to freezing point so that higher accuracy and less fragility can be achieved. Each step in the SA algorithm substitutes the current result by an random "nearby" solution, selected with a possibility which depends on the variance between the corresponding function values and on a global parameter T (called the temperature), that is steadily decreased throughout the process. The dependency is such that the current solution changes almost randomly when T is large, but increasingly "downhill" as T goes to zero.

1. Activate Cloud Objects at server and User End Cloud Components
   a. Allocation Matrix
   b. Bandwidth Matrix
   c. Initial Trust Factor
   d. Data Centers
   e. VM
   f. Cloudlets
   g. Users
2. Amalgamation of security keys for Security and Integrity to improve the Trust Model and transmission initiates
3. Collection and Initialization of Training DataSets with dynamic initialization of the cloud elements for deep investigation and research
   a. Solution space (All Trust Values and individual score)s
   b. Cost function (Directly proportional to the execution time and performance parameters $c = 1/(r * (p + e)) * 100$)
      i. Analysis of the acceptance value for the cost function
   c. Perturbation rules for Transforming a solution to a new one
      i. Solutions from one phase to other for higher degree of accuracy and integrtiy
   d. Simulated Annealing engine
      i. Activation of variable T (Temperature)
      ii. An initial temperature T_0 (T_0 =

50,000)

iii. A freezing temperature $T_{freezing}$ ($T_{freezing}$= 0.1)

iv. thre=(0.05) 5% Rejection rate

4. A cooling schedule (T = 0.95 * T)
5. SA evaluation module for trust value with binary permutations
6. Application of the META approach and model on cloud elements for effective results
7. Fetching of Results and storage in the file system
8. Data Cleaning, Analysis, Interpretation and Predictions

In the META (Meta-heuristic Enhanced Trust Assessment)of improved security and related dimensions using simulated annealing with the dynamic security for higher trust factors over the classical gene based approach. It proposed and actualized the measurements for the ideal use of the considerable number of processors in a cloud framework to actualize the Hybrid and in addition parallel methodologies of booking calculation and assesses the proposed cloud based virtualization which is taken from driving computational focuses. The significant key idea or thought of the proposed calculations is to execute employments ideally with the goal that there is the best mix of normal holding up, turnaround and effectiveness and expense. The classical virtualization techniques are having number of pitfalls that takes more execution time. The basic solution obtained without swarm intelligence is not efficient in terms of the turnaround time and optimal results.

VI. RESULTS AND DISCUSSION

For the implementation of classical and META approach, the results are fetched from cloudsim, cloudanalyst and gridsim with the integration of jcharts for plotting of results. The results from SA are better in terms of all the parameters including

- Waiting Time
- Cost Factor
- Turnaround Time
- Complexity
- Performance

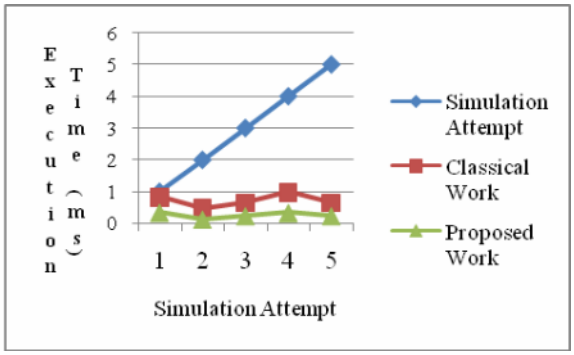

Figure 1 Line Graph Analysis of the Existing and META Approach

Figure 1 shows graphical results show the execution time and related parameter in the META approach that is very less when compared to the existing algorithmic approach. The execution time in the Existing work is taking higher units.

TABLE I COST COMAPRISION

Simulation Attempt	Existing Work (USD)	META Work(USD)
1	89	70
2	78	60
3	67	59
4	76	40
5	49	20

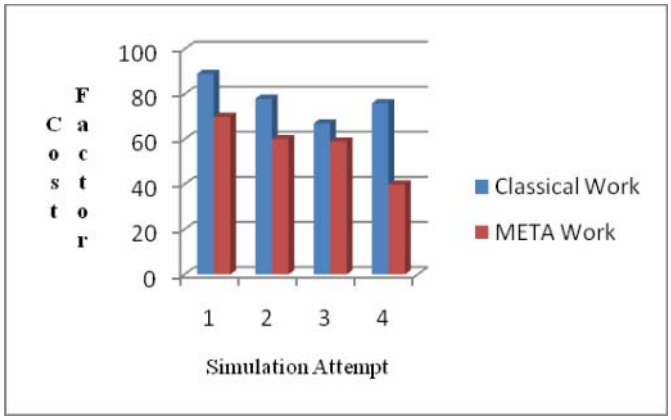

Figure 2 Cost Factor Graph Analysis of the Existing and METAApproach

Figure 2 depicts that the cost factor in the META approach that is very less when compared to the existing algorithmic approach.

TABLE II Effectiveness between Existing and Improved Approach

Existing Base Work (Overall Effectiveness)	META Approach (Overall Effectiveness)
49	59
50	87
68	88
49	68

Table II depicts the trust values of existing and META Approach. Overall Effectiveness in terms of trust value is

higher in case of META Technique when taking DataCentres -2 and Cloudlets- 20 in each module.

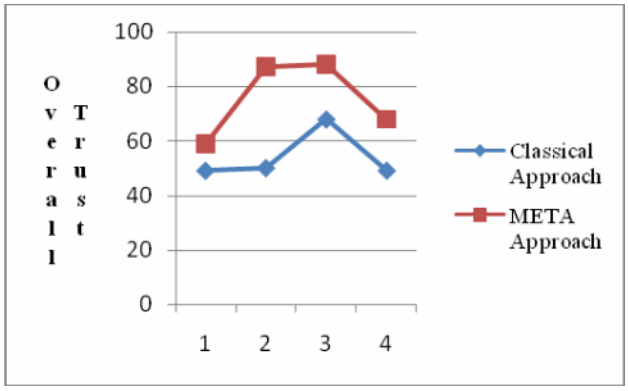

Figure 3 Comparison of Trust Values in Existing and META Approach

TABLE III Waiting Time

Existing Base Work	Proposed Approach
90	59

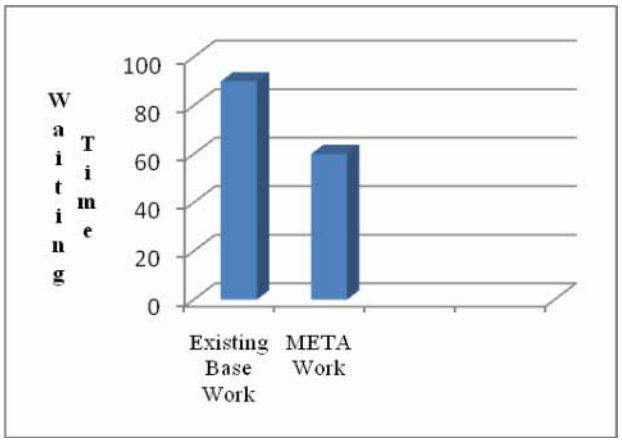

Figure 4 Comparison in terms of Waiting Time

From the simulation results, it is found that the proposed SA is better than GA based approach and giving better results in terms of less waiting time which is very important aspect in cloud infrastructure to perform effectively.

VII. CONCLUSION

In cloud environment, there are various paradigms and research issues but the trust management is one of the most touched area which is directly associated with security, integrity and privacy. Trust management has been recognised as imperative element for creating and preserving successful relational interactions between e-commerce dealing partners in cloud atmosphere.

In the highly competitive and disseminated environment, the promises are scarce for the users to find the dependable and reliable Cloud providers. Due to these limitations, potential customers are not sure whether they can trust the Cloud providers in offering dependable services. In this work, multi-faceted trust management architecture with the integration of meta-heuristic approach simulated annealing is implemented for cloud marketplaces, to support customers in detecting trustworthy resource providers. In this research work, a unique and effective approach simulated annealing is used with the integration of dynamic hash key so that the overall security and trust can be maintained as well as improved.

ACKNOWLEDGEMENT

The author appreciates the help of Dr. Gagandeep an associate professor at Punjabi University Patiala, who helped and guided for this work. Her encouraging remarks from time to time greatly helped in completing this work

REFERENCES

[1] Ye Diana Wang, Henry H. Emurian “An Overview of Online Trust : Concepts, elements and implications”, ELSEVIER journal, 2005
[2] S. Subashini,V.Kavitha “A Survey on Security in Service delivery models of cloud computing” ELSEVIER journal of network and computer applications,July 2010
[3] ZhidongShen and Qiang “The Security of Cloud Computing System enabled by Trusted Computing Technology” IEEE Conference on Signal Processing Systems,2010
[4] DimitriosZissis ,DimitriosLekkas, “Addressing cloud computing security issues” ELSEVIER journal of network and computer appliations, December 2010.
[5] S. Pearson and A. Benameur, “Privacy, Security and Trust Issues Arising from Cloud Computing,” IEEE 2nd Conference on Cloud Computing ,2010
[6] Ramgovind S, Eloff MM, Smith E “The Management of Security in Cloud Computing” IEEE conference,2010.
[7] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee “TrustCloud: A Framework for Accountability and Trust in Cloud Computing” March 2011
[8] Paul D Manuel1, S. Thamarai Selvi2 and Mostafa Ibrahim Abd-El Barr “A Novel Trust Management System for Cloud Computing - IaaS Providers” article in journal of combinatorial mathematics and combinatorial computing, November 2011
[9] Rabi Prasad Padhy, ManasRanjanPatra IRACST “Cloud Computing: Security Issues and Research Challenges”IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS),Vol 3, No. 2,December 2011
[10] Reddy G.Harish, Reddy K. Venkat, Raj S.Uttam, K.JeevanaJyothi “Security Issues in Cloud Computing Services”, (IIJCSE) International journal of Advanced Research in Computer Science and Software Engineering,Vol 3, Issue 6, June 2013
[11] Ayesha Kanwal, RahatMasood, Um E Ghazia, Muhammad AwaisShibli and Abdul GhafoorAbbasi, “Assessment Criteria for Trust Models in Cloud Computing”, IEEE International Conference on Green Computing, 2013
[12] YashashreeBendale and Seema Shah “User Level Trust Evaluation in Cloud Computing” , International Journal of Computer Applications,Vol 69, No. 24, May 2013

[13] SomeshKumar Prajapati, SuvamoyChangder and AnirbanSarkar "Trust Management Model For Cloud Computing Environment", Proceedings of the International Conference on Computing. Communication and Advanced Network – ICCCAN, 2013
[14] Christina Terese Joseph, Chandrasekaran K,Robin Cyriac "A Novel Family Genetic Approach for Virtual Machine Allocation" ELSEVERE Conference on Information and Communication Technologies, 2015
[15] RathiKavita, SudeshKumari,"A Survey on Trust in Cloud Computing" (IJETMAS)International Journal of Engineering Technology, Management and Applied Sciences,Vol 3, Issue 1, January 2015
[16] Sachin Gupta, S.N Panda, Bharat Bhushan "Hash Key Based Effective Algorithm for Security in Cloud Infrastructure" International Journal of Computer Science and Technology,Vol 6, Issue 3, July 2015
[17] Xiaoyong Li, Huadong Ma, Feng Zhou, and Wenbin Yao "T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services"IEEE transactions on information forensics and security, Vol 10, No. 7, July 2015
[18] BrototiMondal, AvishekChoudhury "Simulated Annealing (SA) based Load Balancing Strategy for Cloud Computing" International Journal of Computer Science and Information Technologies,Vol 6, No. 4, 2015
[19] Talal H. Noor, Quan Z. Sheng, Lina Yao, SchahramDustdar, and Anne H.H. Ngu "CloudArmor: Supporting Reputation-based Trust Management for Cloud Services" IEEE transactions on parallel and distributed system, 2015
[20] ManashSarkar, Soumya Banerjee and Valentina E. "Configuring Trust Model for Cloud Computing: Decision Exploration Using Fuzzy Reasoning" IEEE 19th International Conference on Intelligent Engineering Systems, September 2015
[21] UshaDivakarla, K. Chandrasekaran "Secure Allocation of Resources in Cloud Using Trust" International journal on Computer Network and Information Security, January 2016
[22] Syed Hamid HussainMadni, Muhammad ShafieAbdLatiff, YahayaCoulibaly and Shafi'i Muhammad Abdulhamid "An Appraisal of Meta-Heuristic Resource Allocation Techniques for IaaS Cloud" Indian Journal of Science and Technology,Vol 9, No. 4, January 2016
[23] Talal H. Noor, Quan Z. Sheng, ZakariaMaamar, SheraliZeadally "Managing Trust in the Cloud: State of the Art and Research Challenges" IEEE journal, 2016
[24] JayalakshmiKanagasabapathy, C. Swaraj Paul "Secure and Trusted Information Brokering In Cloud Computing" International Journal of Scientific Research in Science and Technology, Vol 2, Issue 2, April 2016
[25] G. JeevaRathanam, A. Rajaram "Trust Based Meta-Heuristics Workflow Scheduling in Cloud Service Environment" Journal of Scientific Research, April 2016