International Journal of Cloud Computing and Database Management

E-ISSN: 2707-5915
P-ISSN: 2707-5907
IJCCDM 2020; 1(1): 37-42
Received: 19-11-2019
Accepted: 21-12-2019

Abbas Abazari
Department of Computer Science, Khoy Branch, Islamic Azad University, Khoy, Iran

Abdolreza Hatamlou
Department of Computer Science, Khoy Branch, Islamic Azad University, Khoy, Iran

Corresponding Author:
Abdolreza Hatamlou
Department of Computer Science, Khoy Branch, Islamic Azad University, Khoy, Iran

A new framework for security and trust in cloud computing

Abbas Abazari and Abdolreza Hatamlou

DOI: https://doi.org/10.33545/27075907.2020.v1.i1a.7

Abstract
Cloud computing is a new concept that refers to a pool of virtual computers resources. Dynamic and scalable internet-based development which is often presented as a service has turned it into a very interesting and significant topic. The service can be a physical machine, virtual machine, software and so on. This study has investigated the problem of building up confidence in cloud environments. To this end, it has designed a model which makes it possible for the users, based on their requirements, to compare a variety of cloud server providers and make their own choice of service provider. The proposed framework enjoys the features of continual availability of trust management service, allocating concessions to cloud service providers, of course, depending on the type of service rendered, utilizing filtering to stop improper storage of ideas, having access to continual service for storing service providers' information and of allowing transactions to unfamiliar service providers due to risk assessment, and finally storing users' data in the cloud based on user-defined encoded algorithm. The hopes are that the designed model owing to the above mentioned characteristics can succeed in building trust between users and cloud service providers.

Keywords: Cloud Computing, Service, Framework, Security, Trust

1. Introduction
Cloud computing is a computing model based on large computer networks such as internet and it is the new model for supply, delivery, consumption and IT services (including hardware, software, data and other shared computing resources) by using the internet networks. Applied software and data are stored on servers and are made available to the users based on their demands. Users do not need to know the details, nor do they need to have any specialization or exercise control over the technology of cloud hardware they are using. Cloud computing for rendering its information technology services suggests solutions very similar to those of general utilities (such as water, electricity, telephone, etc.). It means that access to the information technology resources at the time of need and based on their need quantity are flexibly made available to the users through internet. Just as a user pays the cost of his/her water and electricity consumption, the user of cloud computing just pays the costs of computing services. The services rendered by cloud computing model are very vast [1].
The service providers offer to the users various services with different qualities. The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).
a) Infrastructure as a Service (IaaS): Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power. They also allow varying degrees of financial and functional flexibility not found in internal data centers or with collocation services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data center or with a collocation service. IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but 'out of the box' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need

higher levels of security provided at the host [11].

b) Platform as a service (PaaS)

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the "view" of the developers. Platform as a service cloud layer works like IaaS but it provides an additional level of 'rented' functionality. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore, maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental [13].

c) Software as a Service

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is most often implemented to provide business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost. The architecture of SaaS-based applications is specifically designed to support many concurrent users (multi tenancy) at once. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet [2].

In addition to direct concerns, other security-related factors may need to be considered. For example, the degree of legal protection afforded to information in the cloud may be significantly lower if it is stored in a public cloud rather than on a local computer. In addition, information could potentially be stored on servers in countries other than that in which the customer resides, thereby potentially subjecting the information to different or even conflicting legal requirements for privacy. Due to several business benefits offered by Cloud computing, many organizations have started building applications on Cloud infrastructure and making their businesses agile by using flexible and elastic Cloud services. But moving applications and/or data into the Cloud is not straightforward. Numerous challenges exist to leverage the full potential that Cloud computing promises. These challenges are often related to the fact that existing applications have specific requirements and characteristics that need to be met by Cloud providers [3].

2. A review of related work

There are four types of cloud computing models listed by NIST (2009): private cloud, public cloud, hybrid cloud and community cloud:

a) **Public Cloud:** It is for the general public where resources, web applications, web services are provided over the internet and any user can get the services from the cloud. Public Organizations helps in providing the infrastructure to execute the public cloud [14].
b) **Private Cloud:** It is used by the organizations internally and is for a single organization, anyone within the organization can access the data, services and web applications but users outside the organizations cannot access the cloud. Infrastructure of private cloud is completely managed and corporate data are fully maintained by the organization itself [15].
c) **Hybrid Cloud:** The Cloud is a combination of two or more clouds (public, private and community). Basically it is an environment in which multiple internal or external suppliers of cloud services are used in various environments. It is being used by most of the organizations (IBM and Junipers Network, 2009).
d) **Community Cloud:** The cloud is basically the mixture of one or more public, private or hybrid clouds, which is shared by much organization for a single cause (mostly security). Infrastructure is to be shared by several organizations within specific community with common security, compliance objectives. It is managed by third party or managed internally. Its cost is less than public cloud but more than private cloud [4].

Because of the importance of security and trust in the cloud, many people worked on it. People Kuyoro SO, Ibikunle F. & Awodele O with an article titled "Cloud Computing Security Issues and Challenges", in International Journal of Computer Networks (IJCN), Volume 3, Number 5, 2011, issues of security and cloud computing challenges examined and concluded: Although Cloud computing can be seen as a new phenomenon which is set to revolutionist the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future [2].

In 1970, an economist named Akerl of published an article about the failure and collapse of the markets in which asymmetric information is warned. He raised the example of

the second hand car market in which buyers cannot be good or bad about the quality of the vehicle before purchasing comment. On the other hand, although vendor's quality vehicle sales to know are highly motivated by the opportunity to lack of buyers and used to raise the price of exaggerating the quality of your vehicle [5].

Garga S, (2013) propose a framework for measuring the quality of cloud services based on user requirements. A cloud services on the basis of the components of this framework are rated and on the basis of the process hierarchical analysis, the use of the Services, and quality needs are assessed [6].

Sadr-alsadaty, (1392), contends that cloud computing is a very promising technology for reducing operating costs and useful in increasing productivity of organizations. Though today we witness the cost use of cloud computing in different areas, we are still in initial state as far as the security category of cloud computing is concerned. Much work has to go into it. Among the new security challenges, cloud computing lays stress on three specific areas including the SLA (service level agreement), trustful sharing of data, and accountability of service providers users. Then, a solution method was proposed for creating a mutual for trust between the cloud service providers and organizations for the purpose of implementation and development of electronic government. This solution secures the safety and privacy of data as long as they are placed in the same general cloud, in the view of this interpretation, and the current state of country's new technologies and based on country's 21 year-old future outlook we are in dire need of making. National standards and laws in order to achieve our objective just like what is done by European countries and others [7].

Soon-Know Chong (2013) presented a model for dealing with security threats based on the feedback provided, in this trust model management system, to deal with threats, uses suspicious viewpoints with the aim of identifying and filtering out threats. The use the feedback report on the level of trust can minimize the impact of threats [8]. A comprehensive analysis of workflow scheduling in cloud computing and virtual machine placement schemes in cloud computing is given in [9-10].

Amol C. Adamuthe (2015), results show that increasing efforts are required to improve the business issues from different aspects such as service level agreement, licensing issues, adoption framework, pricing and billing issues etc. Cloud computing technology has received very good support from governments, giant software and hardware companies, researchers and customers. This analysis shows that cloud computing has upwards trend and it will influence enterprises in coming years. Cloud technology is changing rapidly due to market competition and in near future it shall metamorphosis into personal cloud cloud/client architecture, hybrid cloud computing and IT. We also envisage newer solutions will be emerging in securing information in cloud computing enabled Data Centre's through virtualization. Future work need to be investigating to identifying best fit of cloud computing technologies in E-governance and business sectors like, Energy, Education, Microfinance and Health care [11].

Hossein Mohammadi (2015), cloud computing is revolutionizing how information technology resources and services are used and managed, but the revolution always comes with new problem In the future, we will extend our research by providing implementations and producing results to justify our concepts of security for cloud computing [14].

D Pharkkavi (2016), cloud computing are many as compared to the traditional computing but the cost of implementation of various technologies to safeguard the cloud play a vital role in selecting the right service providers. In order to keep the cloud secure, these security threats need to be controlled. In this paper, we discussed so far many issues and attacks faced in fundamental level of cloud computing, security issues for various layer levels, data related and also service models [17].

Atoosa Gholami (2015), Cloud computing is a very broad term is used for recent development Internet-based computing. General characteristics and reliable security of cloud computing helps development and adoption of this growing technology. Creating Confidence to suppliers of cloud services is a challenging issue, so that many large companies are hesitant to transfer their business to cloud data centers. Currently, many cloud providers that offer cloud services, their service quality and service level agreements are different. One of the challenges being faced by the cloud client is that how to find cloud service that can satisfy them based on the requirements of quality of service with regard to parameters. Now, there is nothing that could help large companies choose a model of trust in accordance with the appropriate security features and data control. In this paper, we presented a trust model to choose the best source. The proposed model, in addition to taking into account criteria of quality of service such as cost, response time, bandwidth, and processor speed, and so on it considers the speed of implementation of works. The proposed model (trust Model Turnaround Trust) has better performance compared to the trust model of the first input, the first output (FIFO) and trust model of quality of service (QOS Trust) and similar models. The proposed model, in addition to taking into account the measures of quality of service, selects the most reliable source in the cloud environment by taking into account the speed of things. Using rating mechanism by using the analytic hierarchy process model to select the best cloud source and the development of trust model based on cost efficient algorithm are among the things that can be done in the continuation of this study [18].

Jingwei Huang (2016), Trust is a critical aspect of cloud computing. We examined and categorized existing research and practice of trust mechanisms for cloud computing in five categories – reputation based, SLA verification based, transparency mechanisms (self-assessment and information revealing), trust as a service, and formal accreditation, audit, and standards. Most current work on trust in the cloud a focus narrowly on certain aspects of trust; our thesis is that this is insufficient. Trust is a complex social phenomenon, and a systemic view of trust mechanism analysis is necessary. In this paper we take a broad view of trust mechanism analysis in cloud computing and develop a somewhat informal and abstract framework as a route map for analyzing trust in the clouds. In particular, we suggest: (1) a policy-based approach of trust judgment, by which the trust placed on a cloud service or a cloud entity is derived from a "formal" audit proving that the cloud entity conforms to some trusted policies; (2) a "formal" attribute based approach of trust judgment, by which particular attributes of a cloud service or attributes of a service provider are used as evidence for trust judgment, and the belief in those

attributes is based on formal certification and chains of trust for validation. To support this mechanism, we propose a general structure of evidence based trust judgment, which provides a basis to infer the trust in a cloud entity from the belief in the attributes that entity has, and in which, based on the semantics of trust, we define the attributes to be examined are in a space of two-dimensions – domain of expectancy and source of trust including competency, integrity, and goodwill. Future research will focus on mathematically formal frameworks for reasoning about trust, including model [19].

3. The proposed framework

The flowchart of the proposed model is presented in Figure 1. This model consists of two levels of communications:

a) **The first level communication:** This level is composed of several main layers which are trust management layer, data trust storage layer, and management membership layer respective, which will be expounded layer on.
b) **The second level communication:** the second communication concerns access to the user's data which will be described as the paper enfolds.

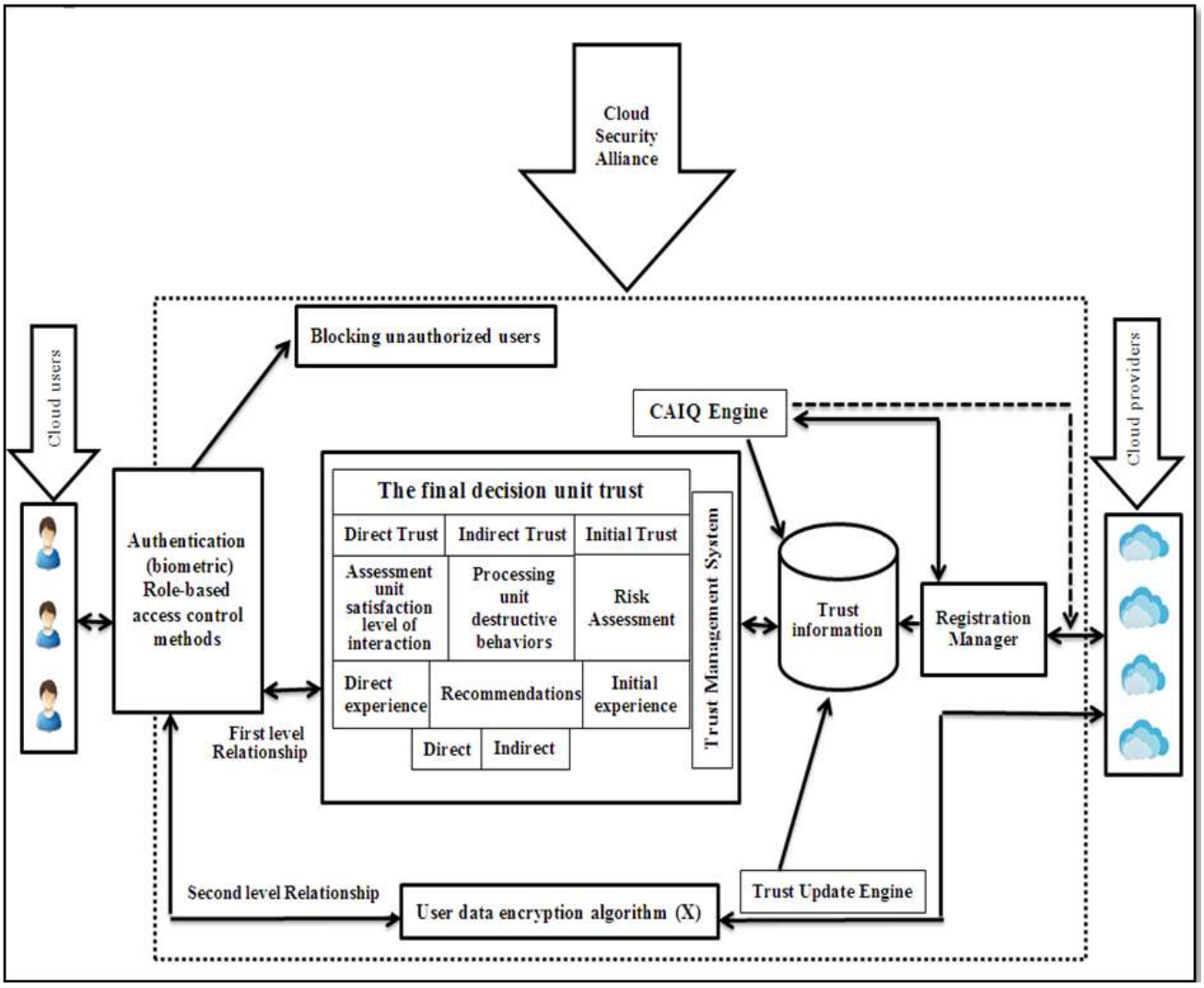

Fig 1: The proposed framework

3.1 First level relationship

3.1.1 Trust Management Layer

This unit is responsible for collecting and rating of trust. This unit measures the trust value of service providers and sends them to data trust storage layer for updating. The system's output is a list of ratings concerns the cloud service providers. The trust management layer allows users to have an access to cloud providers and to cloud trust ratings as well. This is a web-based service that makes it possible for users to determine their needs. This layer consists of several parts that will be dealt with in subsequent sections.

3.1.1.1 Direct experience

The trust value is assigned based on the satisfaction level of interaction between the two entities, the part of the trust is very important because it does not depend on the recommendations from other trusted trustees.

3.1.1.2 Assessment unit of satisfaction level of direct interaction

This unit is used to evaluate the satisfaction level of direct interaction based on service priorities. Since the data concerning the direct transactions are used as recommendations in subsequent interactions.

3.1.1.3 Recommendations

Amount of this trust about a particular service provider is gathered by other trused group. This amount includes both direct and indirect recommendations.

3.1.1.4 Processing unit destructive behaviors
Effective protection against inappropriate necessary rating on a system of trust management and part of it is interminable; therefore, it is essential to recognize the validity of the proposed model is the feedback filter.

3.1.1.5 Initial experience
Initial trust concerns when provide is totally unknown.

3.1.1.6 Risk Assessment
Lack of information on cloud computing is a common phenomenon. Even in the absence of information, we need to contact with the server provider, therefore, the risk assessment model is meat to solve this problem. In the proposed model service are classified on the basis of their safety needs, this follows that each service provider has a table of different services with different security levels to which are classified based on operational and non-operational needs.

3.1.1.7 The final trust decision-making unit
In this model, first proposed parameters are combined, then, a final classified of rates of cloud service providers, based on user's needs, are presented.

3.1.2 Trust information storage layer
This layer composed of several parts. The main part this information storage layer is storing and protecting of trust information. This information is continually updated. In the sections that follow, we will deal with in greater details with the description and updating of trust information.

3.1.2.1 Trust information storage location
User's records and the rates of cloud service providers are stored in this section. This information is continually updated by trust updating engine, CAIQ, etc.

3.1.2.2 Trust updating engine
The TUE allows collecting opinions from various sources and roots about the trustworthiness of cloud providers. The opinions collected here should be filtered in such a way so that the users may use the valid opinions according to their requirements. For example, spam and information filtering should be used to eliminate junk or useless information to be stored in the TI repository. The filtered opinions are then taken into account when updating the trust value of cloud providers.

3.1.2.3 Consensus assessments initiative questionnaire (CAIQ) engine
The CAIQ engine allows cloud providers to fill in the CAI questionnaire by providing an intuitive graphical interface through the Registration Manager. The questionnaire helps cloud providers to represent their competencies to the potential users with respect to different attributes. The questions are designed to be answered in 'yes' or 'no'. All the answers are stored in the TI for further processing.

3.1.2.4 Registration manager layer (RML)
Cloud providers register through the RML to be able to act as sellers in a cloud marketplace. They have to provide system/service specifications related to the service delivery models (e.g., SaaS, PaaS, IaaS) they offer and fill in the CAI questionnaire as a part of cloud marketplace policy. The RM forwards the answers of the questionnaire and system/service description to the CAIQ engine and TI (Trust Information) respectively for further processing.

3.2 Second level relationship
The fundamental problem in the cloud computing, the lack of mutual trust between cloud providers and users of cloud services, to solve this problem, in this study we have tried to escape user data from the cloud provider the information to be decoded. Select the encryption algorithm to the data stored in the user's own cloud.
The proposed model provided user communication through multi-layered system of trust, also in this system user evaluation done entirely according to their behavior and because of the possible influence of biometric authentication is very low. Since they of destructive authorized users requirements are fully documented and based on user behavior will be dealt with after the proposed framework can be a trusted cloud environment created for users. Despite the second level of relation in the framework of the cloud users the possibility provides for the security of information stored in cloud anyway provides. Finally the characteristics of the framework can be expressed in this way: The other model and the traditional model trust management is offered as a service. Because there is no service but the dynamic the proposed model is required and is always available. The other features of the proposed model, assign rate based on the type of service providers, direct assessment service providers, filter out inappropriate comments to reuse the trust recommended, there is a permanent service providers to store data in the absence of timely information, to interact with service providers unfamiliar with the use of risk assessment stated, This model for comprehensive vision to providers and cloud users with the other models are quite distinct. This feature is one of superiority of the proposed model is compared with other models.

4. Conclusion
Cloud computing business is rapidly growing. The new cloud providers are entering into the market while investing massively. Providers with the investment of millions of people in the new data centers are being set up. At present, it is difficult to state the difference between good and bad clouds or cloud quality to customers. In fact, the market clouds are lacking in appropriate platform or system that can distinguish cloud providers in terms of different characteristics. Therefore, we have proposed for the cloud market a framework of multi-dimensional trust management. The hopes are that we cloud offer an effective tool to order to differentiate a high quality cloud from a bad quality cloud beyond performance matters. The Purpose of the system is to give credits to cloud trust provider on the basis of reliable behavior of basic system and service providers respond to the questions of cloud Security Alliance and heuristic evaluation engine. As a suggestion for future works, we can refer to data user encryption algorithms to provide convenient and efficient algorithms for data encryption and data storage in the cloud, and complete the framework provided.

5. References
1. Rajesh Laxman Gaikwad, Prof. Dhananjay M Dakhane, Prof. Ravindra L Pardhi. Network security enhancement

in Hadoop Clusters, International Journal of Application or Innovation in engineering & management (IJAIEM). 2013; 2:3.
2. Kuyoro S.O, Ibikunle F, Awodele O. Cloud computing security issues and challenges, 2011.
3. Dan Jerker B Svantesson. Data protection in cloud computing The Swedish perspective, computer law & security review. 2012; 28:476- 480.
4. K Kavitha. Assistant Professor, Department of MCA, Adhiparasakthi engineering college, Melmaruvathur, Tamilnadu, India, Study on cloud computing model and its benefits, challenges, 2014.
5. Mell Peter, Grance Timoth. The NIST definition of cloud computing draft, 2011.
6. Garga S, Versteeg S, Buyya R. A framework for ranking of cloud computing services. Journal of future generation computer systems. 2013; 22:102–122.
7. Sadr Alsadati. Sayed Mohsen, Security challenges in cloud computing in order to improve security in the development of e-government services, The 8th symposium on advances in science and technology (8thSASTech), Mashhad, Iran, 8th SASTech.khi.ac.ir, 2013.
8. Soon-Keow Chong, Jemal Abawajy, Masitah Ahmad, Isredza Rahmi A. Hamid, Enhancing Trust Management in cloud environment, international conference on innovation, management and technology research, Malaysia, 2013, 22-23.
9. Masdari M, ValiKardan S, Shahi Z, Azar SI. Towards workflow scheduling in cloud computing: a comprehensive analysis, Journal of network and computer applications. 2016; 31:66:64-82.
10. Masdari M, Nabavi SS, Ahmadi V. An overview of virtual machine placement schemes in cloud computing, Journal of network and computer applications. 2016; 31(66):106-27.
11. Amol C. Adamuthe cloud computing – A market perspective and research directions, I.J Information technology and computer science, (http://www.mecs-press.org/), 2015, 42-53.
12. G. Arjunan. An survey on cloud computing process and its applications, international journal of research in computer applications and robotics. www.ijrcar.com 2015; 3:10.
13. European Academic Research. ISSN: 2286-4822, www.euacademic.org, 2016; 3:11.
14. Hossein Mohammadi. Considerations on models, algorithms and security challenges in cloud computing, IJISET - International journal of innovative science, engineering & technology. 2015; 3(6):2348-7968.
15. M. Chandni Jain. Cloud Computing: Network/security threats and counter measures, International journal of advanced research in computer and communication engineering. 2015; 4:8.
16. B.Fathima Mary. CRBS-An Architecture for Accessing Location Based Services (LBS) in Cloud, Intern J Fuzzy mathematical archive, (www.researchmathsci.org), 2015, 6.
17. D Pharkkavi. An comprehensive on study on security issues of cloud computing and its data, International journal of contemporary research in computer science and technology (IJCRCST). 2016; 2:2.
18. Atoosa Gholami. A trust model based on quality of service in cloud computing environment, International Journal of database theory and application, (http://dx.doi.org), 2015; 8:161-170.
19. Jingwei Huang. Trust mechanisms for cloud computing, Journal of cloud computing: advances, systems and applications (http://www.journalofcloudcomputing.com), 2013, 2.