Reviews on Security Issues and Challenges in Cloud Computing

Y Z An, Z F Zaaba & N F Samsudin

School of Computer Sciences, Universiti Sains Malaysia, 11800 Minden, Pulau Pinang, Malaysia

yzan.ucom14@student.usm.my,
zarulfitri@usm.my,
nfarhana.ucom12@student.usm.my,

Abstract. Cloud computing is an Internet-based computing service provided by the third party allowing share of resources and data among devices. It is widely used in many organizations nowadays and becoming more popular because it changes the way of how the Information Technology (IT) of an organization is organized and managed. It provides lots of benefits such as simplicity and lower costs, almost unlimited storage, least maintenance, easy utilization, backup and recovery, continuous availability, quality of service, automated software integration, scalability, flexibility and reliability, easy access to information, elasticity, quick deployment and lower barrier to entry. While there is increasing use of cloud computing service in this new era, the security issues of the cloud computing become a challenges. Cloud computing must be safe and secure enough to ensure the privacy of the users. This paper firstly lists out the architecture of the cloud computing, then discuss the most common security issues of using cloud and some solutions to the security issues since security is one of the most critical aspect in cloud computing due to the sensitivity of user's data.

1. Introduction

Cloud computing is a relatively new service that allow the users to store and access computing resources and data over Internet rather than from the local hard drive which might be costly. It help to increase the storage capacity because users can have more than one cloud service to stored their data and thus reduce the cost because there is no need to own an expensive computer with a larger memory. According to the US National Institute of Standards and Technology (NIST), cloud computing is a model enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. While the users are enjoying all the benefits that cloud computing could provide, many of the users did not realized that there are many threats that might cause a great loss them. Most of them did not even know how the cloud service provider manage their data and where exactly the data is stored. When choosing to use cloud computing service, the users are actually handling the confidential data to the third party who helps the users to keep and backup the data or resources. Based on that, there are some question that might be asked by the security professionals like "Do you really think that the data is safe and secure when it is managed by the third party?" and "Do you trust the cloud service that you

use?" Security issues and challenges are then arises since there is lack of awareness while the users are using the cloud service that provided by the cloud service provider [2].

This paper discusses the state of the art of cloud computing domain focuses on the issues and challenges and the current practices. This paper is organised as follows: Section 2 explores the related work; Section 3 describes the security issues and challenges of the current issues in cloud computing studies, Section 4 explains the solutions and practices utilise in overcoming the issues; and finally Section 5 presents the conclusion and future works of this study.

2. Related Works

The architecture of cloud composed of several service models and deployment models [1].

2.1. Service Model:

i. Software as a service (SaaS)
It is the top layer of cloud service model. The cloud service provider developed and hosts the software or application on the cloud infrastructure allowing the users to use it with various devices by using the thin client interface such as web browser. However the underlying cloud infrastructure, network, servers, operating systems or even individual application capabilities is not manageable by the users [3]. It helps the users to save cost because of licensing of the traditional packages is more expensive compared to the monthly fee for renting the application from cloud service.

ii. Platform as a service (PaaS)
A middle layer of cloud service model that provides a software environment or platform for the users to design, develop, deploy and test their application without worrying about the underlying of the cloud infrastructure using the virtual servers of the cloud service provided [1,3]. Therefore, the users can build their own applications which running on the provider's infrastructure and they have control over the deployed application they built.

Table 1. Comparisons of service model and examples [4].

	SaaS Consume	**PaaS** Build	**Iaas** Host
Consumer	End User	Application Owner	Application Owner
Type of Service Provided	Completed Applications	• RunTime scenario • Cloud storage • Integration, etc	• Cloud storage • Visual server
Coverage at Service Level	• Application uptime • Application performance	• Environment availability • Environment performance • No application coverage	• Virtual server availability • Time to provision • No platform or application coverage
Examples of Services Provided	• CRM • E-mails • Collaborative • ERP	• Application development • Decision support • Web • Streaming	• Caching • Security • Legacy • System management

iii. Infrastructure as a Service (IaaS)

The user allowed to rent the processing, storage and other fundamental computing resources to deploy and run arbitrary software which include operating system and applications and they have control over the operating system and network. It provides basic storage and computing capabilities. It also has a data centre space that can help to handle workload [1].

2.2. Deployment model:

i. Public cloud
The entire infrastructure of this cloud model is located on the premises of the cloud service provider. The users normally share the same infrastructure pool with limited configuration. It is accessible by any user and any user can store their data in the same cloud provided by the cloud service provider. It provides scalable, dynamically provisioned and virtualized resources available over the Internet.

ii. Private cloud
The cloud infrastructure is owned by only one user and it is not shared with the others. The user has physical control over the cloud infrastructure and it is more secure compared to the public cloud where everyone share a same cloud infrastructure. It provides host services on private network that helps most corporate network and data administrators to become in-house service provider efficiently. Studies by [5] provides an insights of a private cloud that addresses the requirements and needs of e-learning and collaboration in university.

iii. Hybrid cloud
Combination of the public, the private or even the community cloud infrastructure which allowed the transitive information exchange. It increased the flexibility of the cloud infrastructure where the users can implement the private cloud using the public cloud resources.

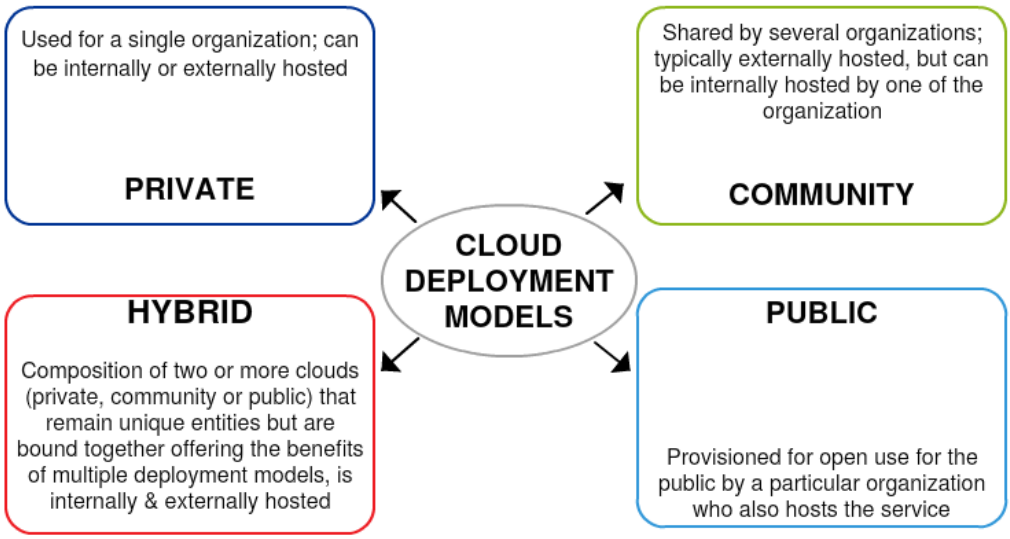

Figure 1: Types of cloud deployment models [6].

iv. Community cloud
The cloud infrastructure is shared among organizations that share the same concerns such as the mission, security requirement and policy. It may owned by more organization and it can exist on premises or even off-premises.

Each type of cloud model provides different level of control, flexibility and management. The users should choose the most suitable type of cloud computing model based on their own situation and their unique needs. This is very important since using unsuitable cloud model might cause the users to

suffer for a great loss such as reduced organization efficiency and might as well more serious like data breaches, data loss and corrupted. The summary of cloud development models are depicted in figure 1.

Studies by [7] discussed the security issues for the cloud includes storage security, middleware security, data security, network security and application security. They also conducted a study approach where they solve small problems in cloud security hoping to solve the larger problems later. They discuss three issues which are:

i. How to secure documents published in third party environment.
ii. How secure co-processors may be used to enhance security.
iii. How XACML (eXtensible Access Control Markup Language) may be implemented in Hadoop environment

They claimed that major aspects in secured cloud computing would be building trusted applications from untrusted components. The extensive security issues and challenges will be discussed further in the next section.

3. Security Issues and Challenges

There are numerous security issues and challenges in cloud computing because it encompasses many technologies such as networks, databases, operating system, virtualization, resource scheduling, transaction management, concurrent control and memory management [8]. This is very important because the cloud service provider must ensure that the users is not facing any serious problem like data loss and data theft which may cause a great loss depending on the sensitivity of the data stored in cloud. A malicious user may pretend to be the legitimate users and infecting the cloud.

There are a lot of security issues to be discussed:

3.1. Security issues

Data at rest is the major issues in cloud computing because users may store all their common, private, or even sensitive data in the cloud which can be accessed by anyone anywhere. Data theft is a very common issues that are facing by the cloud service providers nowadays. Besides, some cloud service providers even don't provide their own server because of the cost effectiveness and flexibility. There are also incidents like data loss which might be also a serious problem for the users. For example, the server is suddenly shut down and causes data loss of the users. Furthermore, natural disaster might also cause data to be damaged or corrupted. Therefore, physical data location can be considered one of the security issues in cloud computing.

3.2. Privacy issues

The cloud computing service provider must enforce their own policies to ensure the safety of the data users stored in their cloud model. They must make sure that they realize who is actually accessing the data stored in the cloud and only the authorized person can maintain the cloud service model [9]. The security of cloud computing should be done on the provider side and also the user side. Cloud service provider should provide a good layer of security protection for the users while the users should not tampered with the other user's data. The cloud computing is a good way to reduce the cost and provide more storage if and only if the security is done by both provider and user. [10] claimed that regulatory reform is essential to protect sensitive data in the cloud since one of the most challenging aspect in cloud computing is to ensures that the consumer have trust in privacy and security of their data.

3.3. Application issues

Monitoring and maintenance should be done by the cloud service provider frequently to ensure that the cloud is secure and not infected by the malicious code that have been uploaded to the cloud by the hackers or attackers with the purpose of stealing sensitive information or even damaging the information of certain users.

3.4. Threats issues

There are lots of security issues regarding the cloud computing that have been widely used nowadays. There are top nine threat that pose severe danger to the cloud computing in year 2013 according to "The Notorious Nine: Cloud Computing Top Threat" by the Cloud Security Alliance (CSA) [11]. The top nine threat that have been mentioned in the white paper are:

i. Data Breaches
Data that stored to the cloud by the users might be important and sensitive. The data store in cloud might be stole by the unauthorized users and that might poses some level of danger to the users under attack. It is the top threat to threat to the cloud computing because hackers or attackers can easily access to the data of the users which store in the cloud. The cloud stored a pool of confidential information of many users. The cloud service users should also ensure the quality, reliability and performance of the cloud service providers through Service Level Agreements (SLAs) negotiated between providers and users [12]. Therefore, data breaches are the worst problem that the cloud computing service faces.

ii. Data Loss
Data stored in cloud might be damaged or corrupted due to some reasons such as shut down of server because of financial or legal problem, natural disaster like earthquakes and fire [13]. Data might not be able to recover because back up is not done well and the data of the users will be lost forever if there are no extra copies of that information.

iii. Account Hijacking
The user's account is stolen or hijacked and the hackers might impersonate he user to perform malicious and unauthorized activities which might also harm the user [14]. For example, the hackers might manipulate the data, provide false information and eavesdropping on transactions using the stolen account. In addition, no native APIs are used for login and anyone can register as a cloud service user hence the chances of the account being hijacked is high [15].

iv. Insecure APIs
Software Interface for the users to interact with the cloud services is also crucial to ensure the security of the cloud model. The API from the authentication and access control to the encryption and activity monitoring should be well implemented to protect against both accidental and malicious attack. For example, [16] propose two stage access control mechanism using the Role Based Access Control Model (RBAC) in order to provide a strong API mechanism.

v. Denial of Service
Hacker use this type of attack to flood the machine or network resources of the cloud service provider which interrupt the users and prevent the users from connecting to the network access [11,17]. This is also a security issues that might harm the user because cloud service becomes unavailable to users and they might not get what they need in time.

vi. Malicious Insiders
Employee of the company might also be a big threat. They might be the attacker themselves or a partner of the hacker who have the better chances of stealing or tampering the data of the cloud model with intention. These activities cause the sensitive or confidential data of the users leak to the others which might harm the targeted users. Studies by [18] reveals that password and other confidential data can be easily obtained by malicious insiders of cloud service providers. Studies by [19] addresses the problems of malicious insiders where they claimed that it should be studied in two context which are insider threat in cloud provider (i.e. insider is malicious employee working for cloud provider) and insider threat in cloud outsourcer (i.e. employee of an organization which sourced its infrastructure to the cloud).

vii. Abuse of Cloud Service
Most of the cloud computing systems have weak registration system. For example, anyone with a valid credit card may register and start using the cloud service immediately. Thus, attackers often conduct the malicious activities by abusing the relative anonymity of the

registration of the cloud computing services. Future areas of concern include password and key cracking, DDOS attack, launching dynamic attack points and hosting malicious data.

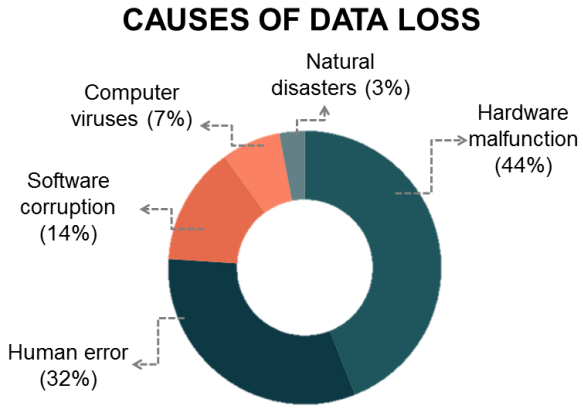

Figure 2: Analysis of causes of data loss.

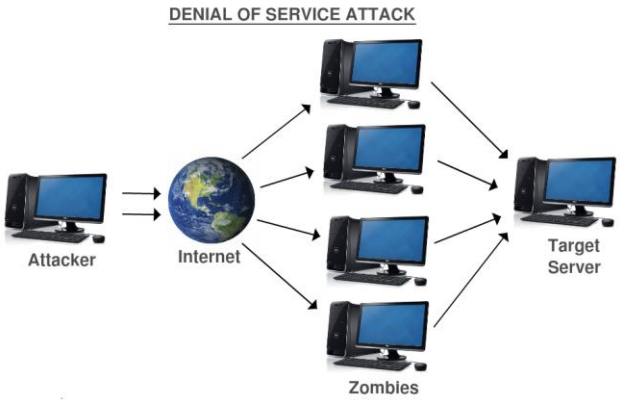

Figure 3: How Denial Of Service (DOS) attack works.

viii. Insufficient Due Diligence
Many users undertake little due diligence about their cloud service providers (CSPs). They did not even consider basic due diligence, such as assessing the financial health of the CSP or determining how long the CSP has been in business [20]. The due diligent should not be ignored because the cloud service provider might not secure enough and they did not take responsible to the data stolen from the cloud by some hackers.

ix. Shared Technologies Issue
IaaS vendors deliver their services in a scalable way by sharing infrastructure. It is not designed to offer strong isolation properties for a multi-tenant architecture.

4. Solution and Practices for Cloud Security Issues

The cloud computing have become more popular because many users start to realize its benefits. It allows the user to easily shrink the operation and also help to save cost. However, with the increased adoption rate of the cloud service, the security issues and risk have been increased as well [21]. In order to make cloud computing a better option to increase the user storage capacity and save their confidential information securely, there are few solutions and practice that helps.

4.1. Vulnerability shielding

The cloud service provider should improve the patch management. They should check the vulnerability of their cloud service frequently and always update and maintain the cloud to limit the possible access point and reduce the risk of attack of the cloud by the hackers. The cloud service provider might also use the Intrusion Detection System (IDS) to make sure the cloud service provided is secure and safe.

4.2. Trusted cloud service provider

The user should make sure that they find the right cloud service provider. Each cloud service provider have different approaches on data management in the cloud. Well established and experienced cloud service provider is more trust worthy and better choice. Besides, the standards and regulations of the cloud service provider is also very important. Examples of trusted clouds service providers are Amazon Web Services (AWS), IBM, Google and Microsoft. [22] shares the comparison of cloud database so that user can have better understanding of each database and choose the appropriate database accordingly. In order to guide users in choosing the best cloud service provide, CloudCmp

have been developed in studies by [23]. They claimed that the application compares the cost and performance of cloud service providers and ensure fairness, representativeness and compliance while limiting measurement cost structure.

4.3. Use cloud service wisely

The data stored in the cloud should be confidential and even the cloud service provider should not have access to those information [24]. The data stored in the cloud should be well encrypted to ensure the security of the users' information. Anyone who need access to the data in the cloud should ask for the permission of the users before doing so.

4.4. Security check events

The users should have clear contract with the cloud service provider so that the users can claim if any accidents or breaches of the sensitive data stored in the cloud. The users must have clear agreement with the cloud service provider before using the cloud services provided by that particular cloud service provider. The users should ensure that the cloud service provider give enough details about fulfilments of promises, break remediation and reporting contingency.

4.5. Data storage regulations

The architecture of the cloud environment is an important aspect to ensure the security of the data stored in the cloud. The users must understand the concept of the data storage regulations which the cloud service provider follows. Cloud service provider that provide security solution compliant with regulations such as HIPAA, PCI DSS, and EU data protection laws are some of the best choice.

4.6. Facilities for recovery

Cloud service provider should take the responsibility to recover the data of the users if there is any data loss due to certain issues [25]. Cloud service provider should make sure that they have proper backup and can retrieve and recover the confidential data of the users that might be costly. Moreover, the cloud service providers can also implement the following solutions to ensure data recovery [26]:

i. Using fastest disk technology in event of disaster for replication of data in danger.
ii. Changing dirty page threshold.
iii. Prediction and replacement of risky devices.

4.7. Enterprise infrastructure

The user must secured the data that they want to keep in the cloud infrastructure. The cloud service provider should provide an infrastructure that give facilitates for the users to install and configure hardware components like firewalls, routers, server and proxy server.

4.8. Access control

The cloud service provider should set up the data access control with rights and the users who access the data should be verified by the cloud service provider every time. The cloud service provider must ensure that only the authorized users may have access to the data stored in cloud. The method can help to reduce the risk of the data access by the unauthorized users and thus provide a much secure environment to store sensitive data. In addition, third party auditing can also be one of the alternatives to ensure data integrity of the storage in the cloud [27]. However, the auditing procedure should have the following properties:

i. Confidentiality: Auditing protocols should keep user's data confidential against auditor.
ii. Dynamic auditing: Auditing protocol should support updates of data in the cloud.
iii. Batch auditing: Auditing protocol shoud support batch auditing for multiple users and clouds.

4.9. Identification management and authentication

When the user want to access the data stored in the cloud, they must be authenticated not only by using the username and password but also the digital data. Multi-level authentication technique introduced by [28] can also be implemented in cloud computing. The technique generates password in several levels before the user can access the cloud services. Anonymous authentication (i.e. identity of user is protected from the cloud) can also be implemented where only valid users are able to decrypt the information [27]. Other than that, proposed scheme by [29] can also be applied in cloud computing where they claimed that their new password authentication scheme are secured from impersonation , off-line guessing and man in the middle attack. Furthermore, leakage-resilient authentication can also be utilised in order to improve the security of the cloud services [30].

5. Conclusion

Cloud computing is a model that helps to speed up and increase the flexibility of data management with reduced cost. It is undeniable that cloud computing has brings us lots of benefits and becoming more popular nowadays. Many large companies start using cloud service in their business. While the cloud computing is widely used, the security becomes a concern to everyone who use cloud services. There is a lot of security arises continuously while there are improvement as well on the security model of the cloud service provided. Despite the increasing use of the cloud service, the user should use the cloud service provided wisely in a way that always ensure good security practices so that this technology have the potential to bring the information technology to the next level. Cloud computing might help us to separate he software from the hardware as more technologies are used as service using cloud and software might have a highly abstract space with the computer hardware. It is expected that this paper provides some basis or foundation in regards to issues and challenges in cloud computing.

References

[1] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I and Zaharia M 2010 A view of cloud computing, Communications of the ACM Magazine, **53** 4 50-58

[2] Ashraf I 2014 An overview of service model of cloud computing *Int. J. of Multidisciplinary and Current Research* **2** 779-783

[3] BalaNarayada Reddy G 2013 Cloud computing-types of cloud Retrieved from http://bigdatariding.blogspot.my/2013/10/cloud-computing-types-of-cloud.html

[4] Christina A A 2015 Proactive measures on account hijacking in cloud computing network *Asian Journal of Computer Science and Technology* **4** 2 31-34

[5] Choubey R, Dubey R and Bhattacharjee J 2011 A survey on cloud computing security challenges and threats *International Journal on Computer Science and Engineering (IJCSE)* **3** 3 1227-1231

[6] Cloud Security Alliance 2013 The notorious nine: Cloud computing top threats in 2013 Retrieved from https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

[7] Dinesha H A and Agrawal V K 2012 Multi-level authentication technique for accessing cloud services *International Journal on Cloud Computing: Services and Architecture (IJCCSA)* **2** 3 31-39

[8] Doelitzscher F, Sulistio A, Reich C, Kuijs H and Wolf D 2011 Private cloud for collaboration and e-Learning services: from IaaS to SaaS *J. Computing-Cloud Computing* **91** 1 23-42

[9] Hamlen K, Kantarcioglu M, Khan L and Thuraisingham B 2012 Security issues for cloud computing *Optimizing Information Security and Advancing Privacy Assurance: New Technologies* **8** 150-162

[10] Jain S, Kumar R, Kumawat S and Jangir S K 2014 An analysis of security and privacy issues,

Challenges with possible solution in cloud computing *Proc. of the National Conf. on Computational and Mathematical Sciences (COMPUTATIA-IV)* 1-7
[11] Kandias M, Virvilis N and Gritzalis D 2011 The insider threat in cloud computing *Proc. of 6th International Conf. on Critical Infrastructure Security* 95-106
[12] Khoshkholghi M A, Abdullah A, Latip R, Subramaniam S and Othman M 2014 Disaster Recovery in Cloud Computing: A Survey *Computer and Information Science* **7** 4 39-54
[13] Khurana S and Verma A G 2013 Comparisons of cloud computing service model: SaaS, PaaS, IaaS *International Journal of Electronics & Communication Technology (IJECT)* **4** 3 29-32
[14] Kiblin T 2011 How to use cloud computing for disaster recovery Retrieved from http://www.crn.com/blogs-op-ed/channel-voices/230700011/how-to-use-cloud-computing-for-disaster-recovery.htm
[15] Kill A 2013 Cloud computing risk: Due diligence and insurance Retrieved from http://www.metrocorpcounsel.com/articles/17928/cloud-computing-risks-due-diligence-and-insurance
[16] King N J and Raja V T 2012 Protecting the privacy and security of sensitive customer data in the cloud *Computer law & Security Review* **28** 308-319
[17] Kuyoro S O, Ibikunie F and Awodele O 2011 Cloud computing security issues and challenges *International Journal of Computer Networks (IJCN)* **3** 5 247-255
[18] Li A, Yang X, Kandula S and Zhang M 2010 CloudCmp: Comparing public cloud providers *Proc. of the 10th ACM SIGCOMM Conf. on Internet measurements* 1-14
[19] Malimi N 2014 Cloud computing Retrieved from http://ngeleki.blogspot.my/2014/03/what-is-cloud-computing.html
[20] McDowell M 2009 Understanding denial-of-service attack Retrieved from https://www.us-cert.gov/ncas/tips/ST04-015
[21] Mell P and Grance T 2011 The NIST definition of cloud computing Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-145
[22] Ramanathan S, Goel S and Alagumalai S 2011 Comparison of cloud database: Amazon's SimpleDB and Google's Bigtable *International Journal of Computer Science Issues* **8** 6 2 243-246.
[23] Rocha F and Correia M 2011 Lucy in the sky without diamonds: Stealing confidential data in the cloud *Proc. of the 1st Int. Workshop on Dependability of Clouds Data Centers and Virtual Computing Environments (DCDV)* 1-6
[24] Mujinga M. 2013 Privacy and legal issus in cloud computing SMME position in South Africa *Proc. Of the 11th Autralian Information Security Management Conf*. 49-59
[25] Sekhar R V, Nandini N, Bhanumathy D and Hemalatha M 2015 Identity based authentication for data stored in cloud *International Journal of Advanced Research in Computer Science and Software Engineering* **5** 3 243-247
[26] Sen J 2013 Security and privacy issues in cloud computing Retrieved from arxiv.org/pdf/1303.4814
[27] Sharma S, Soni S and Sengar S 2012 Security in cloud computing *National Conf. on Security Issues in Network Technologies* 1-6
[28] Shin S H and Kobara K 2010 Towards secure cloud storage Demo for CloudCom2010
[29] Sirisha A and Kumari G G 2010 API access control in cloud using the role based access control model *Trendz in Information Sciences & Computing (TISC)* 135-137
[30] Yassin A A, Jin H, Ibrahim A, Qiang W and Zou D 2012 Efficient password-based two factors authentication in cloud computing *International Journal of Security and Its Applications* **6** 2 143-148