International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-5, June 2013

Survey on Privacy and Data Security Issues in Cloud Computing

Mangala K. Pai, Jayalakshmi D.S.

***Abstract*— Cloud computing is a better way to run the business. Instead of running the apps by yourself, they are run on a shared data center. Cloud computing provides customers the illusion of infinite computing resources which are available from anywhere, anytime, on demand. Apart from these cloud computing is subject to privacy issues and security concerns. In this paper, we see the various types of issues in cloud computing and how to overcome that.**

***Keywords*—Cloud, threats, SaaS, Paas, IaaS, DoS, XSS, BGP, SQL injection**

I. INTRODUCTION

In the current day, the technology with most of the organizations is cloud computing. Cloud computing has the following advantages: i) Accessible from anywhere and at anytime, ii) reduced hardware cost as well as maintenance cost, iii) Software upgradation are automatic i.e. the client or the customer do not bother about updates.

The word cloud is used as a simile for the Internet. The resources are shared in cloud instead of having personal devices or local servers to handle applications. Resources such as servers, the storage and also some applications are given to organization's computers and devices through the Internet.

Instead of storing the photos online than on personal computer such as Dropbox, or making use of some online networking site or webmail is a “cloud computing” service. Cloud computing is fundamentally subscription based service where the storage space and resources can be obtained[10].

Traditional business application has been very expensive and complicated. The amount and variety of hardware and software required to run them are overwhelming. It may need a group of experts who install, configure, test, run, secure, and update them. While a traditional computer setup requires you to be in the same location as your data storage device, the cloud takes it away. The cloud makes it possible to access your information from anywhere at any time. The cloud removes the need for you to be in the same physical location as the hardware that stores your data. Your cloud provider can own and also house the hardware and software necessary to run your home or business applications. With cloud computing you are not managing hardware and software. It’s the responsibility of a knowledgeable vendor. In cloud, you only pay for what you need, scaling up or down is simple and upgrades are automatic. Cloud computing is fundamentally subscription based service where the storage space and resources can be obtained.

Manuscript published on 30 June 2013.
***** Correspondence Author (s)
Mangala K. Pai,
Jayalakshmi D.S.

This is helpful for businesses that cannot afford the same amount of hardware and storage space as a larger company. Small companies can store their information in the cloud, hence removing the cost of purchasing and storing memory devices. Furthermore, because you only need to buy the amount of storage space you will use, a business can buy more space or reduce their subscription as their business grows or as they find they need less storage space.

One requirement to access the cloud is that you need to have an internet connection. This means that if you want to see some specific document you have stored in the cloud, establish an internet connection either through a wired or wireless internet. The advantage is that you can access that same document from any device that can access the internet from wherever you are and at anytime. These devices could be a desktop, laptop, tablet, or phone. This can help the business to function more easily because anyone who can connect to the internet and your cloud can access software, work on documents and store data. This is the freedom that the cloud can provide for you[1].

Cloud computing has five fundamental characteristics defined by NIST (National Institute of Standards and Technology)

1. On-demand self-service. A consumer can unilaterally provision computing capabilities.
2. Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
3. Resource pooling. The provider’s computing resources are pooled to serve several consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
4. Rapid elasticity. Capabilities can be elastically and rapidly provisioned, in few cases automatically, to quickly scale out and rapidly released to quickly scale in.
5. Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service[13].

II. TYPES OF CLOUD AND SERVICE PROVIDERS

A. Types of Cloud

There are different types of clouds that you can use depending on your needs[10].

1. **Public Cloud:** A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space. As a home user or small business owner, you will most likely use public services. The cloud vendor hosts the

computing infrastructure at the vendor's premises. The customer has no control and visibility over where the computing infrastructure is hosted. The computing infrastructure is shared among any organizations. Some examples include services such as email services, online photo storage services or social networking sites.

2. **Private Cloud:** A private cloud is established for a specific group or organization and limits access to just that group. The computing infrastructure is not shared with any other organization and is dedicated only to that organization. Private clouds are more secure and more expensive when compared to public clouds. They allow the organization to host applications in the cloud, at the same time addressing concerns regarding data security and control, which is frequently lacking in a public cloud environment. There are 2 types of private cloud:
   a. **On-Premise Private Cloud:** This is also known as an "internal cloud". It is hosted within an organization's own data center. It provides a standardized process and protection, but often limited in scalability and size. In addition the organization's IT department would incur the operational and capital costs for the physical resources with this model. On-premise private clouds are mostly used for applications that require complete configurability and control of the infrastructure.
   b. **Externally-Hosted Private Cloud:** This is the private cloud model which is hosted by an external cloud computing provider. The service provider facilitates cloud environment with full assurance of privacy. This format is recommended for organizations that prefer not to use a public cloud infrastructure due to the risks associated with the sharing of physical resources
3. **Community Cloud:** A community cloud is shared among two or more organizations that have similar cloud requirements. The service is shared by several organizations and made available only to those groups. For example, all government organizations within the state may share computing infrastructure on the cloud to manage data related to citizens residing in state.

Hybrid Cloud: A hybrid cloud is essentially a combination of at least two clouds, where the clouds integrated are a mixture of public, private, or community. Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both public and private clouds together is called hybrid cloud[10].

B. Types of Service Provider

Each provider serves a specific function. They give the users more or less control over their cloud depending on the type. When you choose a service provider, compare your needs to the services available in the cloud. Cloud needs will differ depending on how you mean to use the space and resources associated with the cloud. If it will be for personal use, you will need a different provider and cloud type than if you will be using the cloud for business. Taking into account, that the cloud provider will be pay-as-you-go, meaning that if the technological needs change at any point you can purchase more storage space (or less for that matter) from your cloud provider[10].

There are three types of cloud providers that you can subscribe to:

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

These three types differ in the amount of control that you have over your information, and conversely, how much you can expect your provider to do for you.

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. A SaaS provider gives subscribers access to both resources and applications. SaaS makes it unnecessary for you to keep a physical copy of software to be installed on your devices. And also, SaaS makes it easier to have the same software on all of your devices at once by accessing it on the cloud. You have the least control over the cloud in a SaaS agreement.

Platform as a Service: is a paradigm for delivering operating systems and associated services over the Internet without downloads or installation. A PaaS system goes a level above the Software as a Service setup. A PaaS provider gives subscribers the access to the components that they require to develop and operate applications over the internet.

Infrastructure as a Service: involves outsourcing the equipment used to support the operations, including hardware, storage, servers and networking components. As the name states IaaS agreement deals primarily with computational infrastructure and the subscriber completely outsources the storage and resources such as the software and hardware that they need.

The entire data reside over a set of networked resources in the cloud computing environment, enabling the data to be accessed through virtual machines. These data centers may lie in any corner of the world beyond the reach and control of users, there are different security and privacy challenges that need to be understood and taken care of.

With a rise towards the deployment of Cloud Computing, the consistent security and privacy issues have become more complicated. The potential of cyber attacks also increases with the increase of on-demand application usage. Individual users have to provide online information about their identification frequently and these could be used by attackers for identity theft. To maintain various security and privacy issues like: operational integrity, confidentiality, disaster recovery and identity management, the subsequent schemes should be deployed at least to ensure data security to some extent like:

- To ensure data security by using an encryption scheme in a highly interfering environment maintaining security standards against popular threats and data storage security.
- Limited access to the data has to be given to the service providers, just to manage it without being able to see what exactly the data is.
- Stringent access controls to prevent illegal and unauthorized access to the servers controlling the network.
- Redundant data storage and data backups to make data retrieval easy due to any type of loss unlike the recent breakdown issues

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

with the Amazon cloud.

- User security and distributed identity management is to be maintained by using either Lightweight Directory Access Protocol (LDAP), or published APIs (Application Programming Interfaces) to connect into identity systems.

III. SECURITY CONCERNS IN CLOUD COMPUTING

Cloud services are applications running somewhere in the Cloud Computing infrastructures through internal network or Internet. For users, they don't know or care about the data where to be stored or services where to be provided. Cloud computing allows the providers to develop the application, deploy and run, that can easily grow in terms of capacity or scalability, work rapidly i.e. performance, and never or at least rarely fail which means reliability, without any concerns on the properties and the locations of the underlying infrastructures. The penalty of obtaining these properties of Cloud Computing are to store individual private data on the other side of the Internet and get service from other parties (i.e. Cloud providers, Cloud service providers), and consequently result in security and privacy issues. Then, what kind of security is sufficient for users?
To achieve adequate security, it contains 5 goals: They are availability, data integrity, confidentiality, control and audit. The five goals are integrated systematically, and none of them could be forfeited to achieve the adequate security. Nevertheless, few Cloud Computing systems can achieve the five goals together nowadays[2].

A. *Availability*

The goal of availability for cloud computing systems including applications and its infrastructures is to ensure its users can use them at any time, at any place. Cloud computing system enables its users to access the system from anywhere (e.g., applications, services). This is true for all the Cloud Computing systems (e.g., DaaS, SaaS, PaaS, IaaS, and etc.). Required to be accessed at any time, the Cloud Computing system should be severing all the time for all the users (say it is scalable for any number of users). Two strategies, redundancy and hardening, are mainly used to enhance the availability of the Cloud system or applications hosted on it.

B. *Confidentiality*

Confidentiality means keeping user's data secret in the Cloud systems. The confidentiality in Cloud systems is a big obstacle for users to step into it, as many users say "My sensitive corporate data will never be in the Cloud" in the article named "Above the Cloud". Cloud Computing system offerings are basically public networks. The applications or systems are exposed to more attacks when comparison to those hosted in the private data centers. Hence, keeping all confidential data of user's secret in the cloud is a fundamental requirement which will attract even more users consequently. Usually, there are two basic approaches (i.e., physical isolation and cryptography) to achieve such confidentiality, which are broadly adopted by the Cloud Computing vendors. Encrypted storage is another choice to enhance the confidentiality. For example, encrypt the data before placing it in a cloud. This approach may be even more secure than unencrypted data in a local data center.[7]

C. *Data Integrity*

In the Cloud system data integrity means preserve information integrity i.e., not modified or lost unauthorized users. The data is the base for providing Cloud Computing services, such as Software as a Service, Data as a Services, Platform as a Service, keeping data integrity is a primary task. Data integrity is fundamental for Cloud Computing system, and it is expectant to be achieved by techniques such as digital signatures, RAID-liked strategies and so on.

D. *Control*

Control in the Cloud system means to regulate the use of the system, together with the applications, infrastructure and the data. Cloud computing system at all times involves distributed computation on multiple large-scale data sets across a large number of computer nodes. Every internet user is able to contribute his or her individual data to the Cloud Computer systems which are situated on the other side of the Internet, and utilize them. For instance, a user's click stream across a set of webs (e.g., Google search web pages, Amazon book store, etc.) can be used to present targeted advertising. Future healthcare applications might use an individual's DNA sequence (which is captured by hospitals) to develop tailored drugs and other personalized medical treatments. When all these private data are stored in the Cloud Computing system environment, users of Cloud Computing systems might face many threats to their individual data[6].

E. *Audit*

Audit means to watch what happened in the Cloud system. Auditability can be added as an additional layer above the virtualized operation system or virtualized application environment hosted on the virtual machine to provide facilities watching what happened in the system. It is more secure than that which is built into the applications or into the software themselves, because it is able to watch the entire access duration. For such kind of scenarios, three main attributes should be audited:

1. Events: The state changes and other factors that affected the system availability.
2. Logs: Comprehensive information about users' application and its runtime environment.
3. Monitoring: Should not be intrusive and must be limited to what the Cloud provider reasonably needs in order to run their facility.

IV. THREATS TO SECURITY IN CLOUD COMPUTING

Cloud computing may not increase the risk that personal information will be improperly exposed or misused; it could increase the chances of exposure. The aggregation of data in a cloud provider can make that data very attractive to cybercriminals. Additionally, given how inexpensive it is to keep data in the cloud, there may be a tendency to retain it for an indefinite period, thereby increasing the risk of breaches.
The chief concern in cloud environments is to provide security around multi-tenancy and isolation; giving customers more comfort in addition "trust us" idea of clouds. Security at different levels such as Host level, Network level and Application level is necessary to keep the cloud up and running continuously.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

A. Basic Security

Web 2.0, a key technology towards enabling the use of Software as a Service relieves the users from tasks like installation and maintenance of software. It's widely used all over. The security has become more important than ever for such environment, as the user community using Web 2.0 is rising.

SQL injection attacks: are the one in which a malicious code is inserted into a standard SQL code and thus the attackers gain unauthorized access to a database and become able to access sensitive information. At times, the hacker's input data is misunderstood by the web-site as the user data and allows it to be accessed by the SQL server and this lets the attacker to have know-how of the functioning of the website and make changes into that. Techniques like avoiding the usage of dynamically generated SQL in the code, using filtering techniques to clean the user input etc. has to be used to check the SQL injection attacks.

Cross Site Scripting (XSS) attacks: which inject malicious scripts into web contents has become quite popular since the inception of Web 2.0. A website can be classified as static or dynamic. Static websites do not suffer from the security threats which the dynamic websites do because of their dynamism in providing multi-fold services to the users. Consequently, these dynamic websites get victimized by XSS attacks. Quite often it's observed that while working on net or surfing, some pop ups or web-pages get opened up with the request of being clicked away to view the content contained in them. Often either unintentionally about the possible hazards or out of curiosity users clicks on these hazardous links and thus the intruding third party gets control over the user's private information or hack their accounts after having known the information available to them. Various techniques like: Content Based Data Leakage Prevention Technology, Active Content Filtering, Web Application Vulnerability Detection Technology have already been proposed. These technologies adopt various methodologies to detect security flaw and try to fix them.

Man in the Middle attacks: Here an intruder tries to intrude in an ongoing conversation between a sender and a client to inject false information and to have knowledge of the important data transferred between them. Many tools implementing strong encryption technologies like: Cain, Dsniff, Wsniff, Ettercap, Airjack etc. have been developed in order to provide safeguard against them. Hence, security at different levels is necessary in order to ensure proper implementation of cloud computing such as: internet access security, server access security, data privacy access security, database security and program access security. Additionally, we need to ensure data security at network layer, and data security at application and physical layer to maintain a secure cloud.

B. Network Level Security

Networks are classified into many types like: public or private, shared and non-shared, small area or large area networks and each of them have a number of security threats to deal with. To guarantee network security following points such as: proper access control, confidentiality and integrity in the network, and maintaining security against the external third party threats should be considered while providing network level security.[5]

Problems related with the network level security includes: DNS attacks, Sniffer attacks, issue of reused IP address, Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) etc.

DNS Attacks: A Domain Name Server (DNS) server performs the translation of a domain name to an IP address since the domain names are much easy to remember. Therefore, the DNS servers are needed. There are cases where the user has been routed to some other evil cloud instead of the one he asked for by having called the server by name and so using IP address is not always feasible. Using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that the route selected between the sender and receiver cause security problems even after all the DNS security measures are taken.

Sniffer Attacks: These types of attacks are launched by applications that can capture packets flowing in a network. The data that is being transferred through these packets can be read if the data is not encrypted and there are chances that sensitive information flowing across the network can be captured and traced. Through the NIC (Network Interface Card), a sniffer program ensures that the data/traffic linked to other systems on the network gets recorded.[11] This can be achieved by placing the NIC in promiscuous mode and in this mode it can track all data flow on the same network. A malevolent sniffing detection platform can be used to detect a sniffing system running on a network based on RTT (round trip time) and ARP (address resolution protocol).

Issue of reused IP Addresses: IP-address is basically a finite quantity. Each node of a network is provided an IP address. A large number of cases have been observed related to re-used IP-address. When a particular user moves out of a network then the IP-address associated with him is assigned to a new user. This risks the security of the new user as there is certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And thus, we can sometimes say that though the old IP address is being assigned to a new user, the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user.

BGP Prefix Hijacking: Prefix hijacking is a type of network attack in which a wrong announcement related to the IP addresses associated with an Autonomous system (AS) is made and hence malicious parties get access to the untraceable IP addresses. In the internet, IP space is associated in blocks and will remain under the control of AS's. The information of an IP contained in its regime to all its neighbors can be broadcast by an autonomous system. These AS communicate through the Border Gateway Protocol (BGP) model. At times, because of few errors, a faulty AS may broadcast wrongly about the IPs related with it. In such case, the actual traffic gets routed to some IP other than the intended one. Consequently, data is leaked or reaches to some other destination that it actually should not.

C. Application Level Security

Application level security refers to the usage of hardware and software

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

resources to provide security to applications such that the attackers are not able to get control over these applications and make desirable changes to their format. In the current day, attacks are launched, being masked as a trusted user and the system considers them as a trusted user allows full access to the attacking party and gets victimized. The reason behind this is that the obsolete network level security policies allow only the authorized users to access the specific IP address. With the technological progression, these security policies have become outdated as there have been instances when the system's security has been breached by accessing the system in the disguise of a trusted user. It's quite possible to imitate a trusted user and corrupt entire data without even being noticed. Thus, it is necessary to install higher level of security checks to minimize these risks.

Denial of Service Attacks: DoS attempts to make the services assigned to the authorized users not able to be used by them. In such an attack, the service becomes unavailable to the authorized user because the server providing the service is flooded by a large number of requests leading to the denial of service. Sometimes, we are unable to access the site and observe an error due to overloading of the server with the requests to access the site. This happens when the server exceeds its capacity to handle the number of requests[11]. The occurrence of a DoS attack increases bandwidth consumption in addition causing congestion and making certain parts of the clouds inaccessible to the users. Using an Intrusion Detection System (IDS) is the most popular method of defense against this type of attacks.

Cookie Positioning: It involves modifying or changing the contents of cookie to make unauthorized access to a webpage or to an application. Cookies mostly contain the user's identity related credentials. Once these cookies are available, the content of these cookies can be forged to imitate an authorized user. This can be avoided either by implementing an encryption scheme for the cookie data or by performing regular cookie cleanup.

Hidden field manipulation: While accessing a web-page, there are some fields that are hidden and contain the page related information which are basically used by developers. These fields are highly prone to a hacker attack as they can be changed easily and posted on the web-page. This results in severe security violations.

Google Hacking: Google is the best option for finding details regarding anything on the net. Google hacking means using Google search engine to trace sensitive information that a hacker can use to his benefit while hacking a user's account. Usually, hackers try to hit upon the security loopholes by probing out on Google about the system they wish to hack and then after having collected the essential information, the hacker carry out the hacking of the concerned system. Sometimes, a hacker is not sure of the target. As an alternative, he tries to Google out the target based on the loophole he wishes to hack a system upon. The hacker then searches for all the possible systems with such a loophole and finds out those having the loopholes he wishes to hack upon. These had been some of the security threats that can be launched at the application level and cause a system downtime disabling the application access even to the authorized users.[7]

V. ENSURING SECURE CLOUD STORAGE

In order to secure the cloud against the various security threats and attacks like: SQL injection, Cross Site Scripting (XSS) attacks, DoS attacks, Google Hacking and Forced Hacking, the cloud service providers take up different techniques. Some standard techniques so as to detect the above mentioned attacks are as: avoid the usage of dynamically generated SQL in the code, validating all user entered parameters, finding the meta-structures used in the code, removal and disallowing unwanted data and characters, etc. For an optimized cost performance ratio, a general security framework needs to be worked out. The main criterion to be fulfilled by the generic security framework is to interface with any type of cloud environment, and to be able to detect and handle customized as well as predefined security policies.[3]

Security Scheme	*Suggested Approach*	*Strengths*	*Limitations*
Data Storage security[12]	Uses homomorphic token with distributed verification of erasure-coded data towards ensuring data storage security and locating the server being attacked.	1. Supports dynamic operations on data blocks such as: update, delete and append without data corruption and loss. 2. Efficient against data modification and server colluding attacks as well as against byzantine failures.	The security in case of dynamic data storage has been considered. However, the issues with fine grained data error location remain to be addressed.
User identity safety in cloud computing	Uses active bundles scheme, whereby predicates are compared over encrypted data and multiparty computing.	Does not need trusted third party (TTP) for the verification or approval of user identity. Thus the user's identity is not disclosed. The TTP remains free and could be used for other purposes such as decryption.	Active bundle may not be executed at all at the host of the requested service. It would leave the system vulnerable. The identity remains a secret and the user is not granted permission to his requests.
Trust model for interoperability and security in cross cloud [2]	1. Separate domains for providers and users, each with a special trust agent. 2. Different trust strategies for service providers and customers. 3. Time and transaction factors are taken into account for trust assignment.	1. Helps the customers to avoid malicious suppliers. 2. Helps the providers to avoid cooperating/ serving malicious users.	Security in a very large scale cross cloud environment. This scheme is able to handle only a limited number of security threats in a fairly small environment.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Virtualized defence and reputation based trust management	1. Uses a hierarchy of DHT-based overlay networks, with specific tasks to be performed by each layer. 2. Lowest layer deals with reputation aggregation and probing colluders. The highest layer deals with various attacks.	Extensive use of virtualization for securing clouds	The proposed model is in its early developmental stage and needs further simulations to verify the performance.
Secure virtualization[13]	1. Idea of an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware is proposed. 2. Behaviour of cloud components can be monitored by logging and periodic checking of executable system files.	A virtualized network is prone to different types of security attacks that can be launched by a guest VM, an ACPS system monitors the guest VM without being noticed and hence any suspicious activity can be blocked and system's security system notified.	System performance gets marginally degraded and a small performance penalty is encountered. This acts as a limitation towards the acceptance of an ACPS system.
Safe, virtual network in cloud environment	Cloud Providers have been suggested to obscure the internal structure of their services and placement policy in the cloud and also to focus on side-channel risks in order to reduce the chances of information leakage.	Ensures the identification of adversary or the attacking party and helping us find a far off place for an attacking party from its target and hence ensuring a more secure environment for the other VMs.	If the adversary gets to know the location of the other VMs, it may try to attack them. This may harm the other VMs in between.
Border Gateway Protocol (BGP)[14]	A pretty good BGP (PGBGP) architecture has been suggested to check the cases where an Autonomous system may announce itself wrongly as the destination for all the data that is being transferred over that network..	Checks the autonomous systems (ASs) and performs anomaly detection with a response system to ensure that the data doesn't get routed to the wrong AS. It also gives us the flexibility to run the PGBGP protocol on some of the ASs towards protecting the entire network.	Vulnerable to Denial of Service (DoS) attacks. This approach only takes care of the routing control messages but doesn't verify the path that actual traffic follows.

Table 1. Comparative analysis of different techniques

VI. CONCLUSION

To facilitate the cloud secure, the security threats should be controlled. Furthermore data residing in the cloud is prone to various threats and number of issues like confidentiality and integrity of data should be well thought-out while buying storage services from a cloud service provider. At regular intervals, Auditing of the cloud needs to be done to protect the cloud against exterior threats. Apart from this, cloud service providers must make sure that all the SLA's are met and human errors from their side are minimized, which enables smooth functioning. In this paper a variety of security concerns for cloud computing environment from several perspective and the solutions to avoid them have been discussed, compared and classified.

REFERENCES

1. Jansen, Wayne & Grance, Timothy. *Guidelines on Security and Privacy in Public Cloud Computing.* National Institute of Standards and Technology, 2011.
2. Aderemi A. Atayero, Oluwaseyi Feyisetan G., "Security Issues in Cloud Computing: *The Potentials of Homomorphic Encryption",* Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 10, October 2011, ISSN 2079-8407
3. Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A NewTrusted and Collaborative Agent Based Approach for Ensuring Cloud Security," Annals of Faculty Engineering, Hunedoara International Journal of Engineering, Year 2012, ISSN 1584-2665
4. John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the world of cloud computing", IEEE Compute r and Relia bility Societies.
5. Grobauer, B.; Walloschek, T.; Stocker, E., "Understanding Cloud Computing Vulnerabilities," *Security & Privacy, IEEE* , vol.9, no.2, March-April 2012
6. Jian Wang; Yan Zhao; Shuo Jiang; Jiajin Le, "Providing privacy preserving in Cloud computing," *Human System Interactions (HSI), 2011, 3rd conference.*
7. Zhidong Shen; Li Li; Fei Yan; Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform," *Intelligent Computation Technology and Automation (ICICTA), International Conference on* , vol.1., 2012.
8. Zhidong Shen; Qiang Tong, "The security of cloud computing system enabled by trusted computing technology," *Signal Processing Systems (ICSPS), 2011 2nd International Conference,* vol.2.
9. The NIST Definition of Cloud Computing, version 15, by Peter Mell and Tim Grance, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory.
10. Alexa Huth, James Cebula "The basics of cloud computing", http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

11. Sugata Sanyal, Ajit Shelat, Amit Gupta, "new frontiers of network security: The threat within"
12. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," 17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4.
13. Wayne Jansen, Timothy Grance, "NIST Guidelines on Security and Privacy in Public Cloud Computing," Draft special Publication 800-144, 2011.http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800 144_cloud-computing.pdf.
14. Josh Karlin, Stephanie Forrest, Jennifer Rexford, "Autonomous Security for Autonomous Systems," Proc. Of Complex Computer and Communication Networks; vol. 52, issue. 15, pp. 2908- 2923, Elsevier,NY,USA,2008