Service Model–Oriented Security Considerations in Cloud Computing

Oliver Smith*, Dr. Charlotte Taylor

Department of Computer Science, University of Oxford, Oxford, England, UK
Department of Artificial Intelligence, University College London, London, England, UK

KEYWORDS: CSP, DDoS, IaaS, Data Segregation, VM's.

ABSTRACT
Cloud computing is individually defined and talked about across the ICT industry under different context and with different definitions attached to it. The mainstay point is that cloud computing means having a server firm that can host the services for users connected to it by a network. Technology has moved in this direction because of the advancement in computing, communication and networking technologies.

Cloud computing is clearly one of the most enticing technology areas of the current times of computing and networking, at least in part to its cost-efficiency and flexibility. There are significant, persistent concerns about cloud computing that are impeding the momentum and will eventually compromise the goals of cloud computing procurement model. Transparency is needed for regulatory reasons and to ease concern over the potential for data breaches. Open source software enables IT to quickly build and deploy applications, but at the cost of control and governance. For the enhancement of technology, and hence healthy growth of global economy, it is extremely important to iron out any issues that can cause road-blocks in this new paradigm of computing. This review paper gives an insight to various issues that hinder the momentum of cloud implementation and accelerate concerns for customers while adopting cloud services.

INTRODUCTION

Cloud Computing promises great flexibility in reserving, using and decommissioning resources depending on current requirements. A high level of savings is also anticipated in the area of IT systems which would otherwise need to be reserved, maintained and renewed at the local level. If the promised flexibility is to become reality, there is a great need to standardise the services offered by Cloud Computing and the related interfaces. Another advantage of Cloud Computing is the ubiquitous availability of business applications, a key issue in the increasing mobility of employees [1]. Facing a number of challenges which need to be resolved before business data or applications is outsourced to a public cloud. The reason for this with public Cloud Computing is that data and applications are outsourced away from the premises, the institution itself losing direct control of them. A large number of legal and contractual guidelines and rules, such as data protection requirements, also need to be taken into consideration if business-critical or personal data. With public Cloud Computing, moreover, unknown users share a common infrastructure. This increases the risk that core information security parameters might be violated [8]. Moreover, data and applications are being used via the Internet so that any failure in the Internet connection will render access impossible.

To be able to exploit the potential benefits of Cloud Computing while retaining control over the IT infrastructure, many users turn to their own virtualised data centres to provision services. But private clouds as well involve a number of threats which need to be protected against. A private cloud may also be highly complex, depending on its implementation [3]. Due to the number of configuration settings and mutually influencing parameters, many security problems

can also occur here, e.g. through data loss, unauthorised data access, reduced availability and even services failing. Cloud providers make a number of interfaces available to access their services. If these interfaces are insecurely programmed, an attacker may exploit vulnerabilities in order to access data without permission. Managing cloud platforms also presents a major challenge for both public and private clouds due to the complexity and dynamism of the underlying processes [10].

SECURITY ARCHITECTURE

If a Cloud Computing platform is to be made operationally secure, all the issues potentially posing a threat to the confidentiality, integrity and availability of the data stored there needs to be examined. Besides a well structured procedural model for all IT processes, it is important that security architecture be set up to protect resources and that the customer is securely isolated. A robust separation of customers at every level in the Cloud Computing stack is a fundamental requirement [26] that each Cloud Computing platform should meet. This requirement applies equally both to public and private clouds.

Data centre security

Data centres form the technical basis for Cloud Computing. To this extent, it is important that every CSP ensures their systems are secure in compliance with the current state the technology. Overall, a data centre should form a security area that affords adequate protection against, damage by the elements, e.g. caused by storms and flooding, and against unauthorised entry. If a customer requires a particularly high level of availability for their services, the CSP should also reserve capacities in backup or redundant data centres which can compensate for another data centre failing. The data centres should be located far enough away from each other geographically so that a controllable damage event, e.g. fire, explosion, road, rail, water or air accidents and natural disasters with a limited impact such as flooding does not simultaneously affect both the data centre originally being used and the one containing the backup capacities. In the SaaS area, many providers do not operate their own infrastructure. If this is the case, the requirements set out here must be met by the subcontractor used by the SaaS provider, i.e. in this case the data centre operator.

Server security

The servers represent the environment for performing the processes and their computations. For this reason the operating systems deployed on the servers should be hardened to the extent that they offer the smallest possible area to attack. To achieve this, when the basic installation is being undertaken, only the necessary software packages should be added and any superfluous programs and services should be disabled or, better, uninstalled. Standard measures to protect IT systems, such as host firewalls, host-based intrusion detection systems, etc. should be implemented and regular integrity reviews run on important system files. Host-based intrusion detection systems are characterised by the fact that they are run on the IT system to be monitored. They are typically deployed to detect attacks made at the application or operating system level. Examples of such attacks are policy violations by users, failed login attempts and malware such as Trojan horses.

The technical basis for providing and using cloud services reliably and securely are provided by a broadband connection, standardised and widely-used transmission protocols, a service-oriented architecture and, above all, virtualisation. Providers deploy different hypervisors for server virtualisation. The hypervisor is the central component of server virtualisation controlling access to shared resources. With a few exceptions, no attacks on the hypervisor have yet appeared in the wild [8] - they have only been described in theoretical terms or as

proof-of-concept. Should an attack succeed, however, the consequences are devastating. The hypervisor can be attacked, for example, by manipulating CPU registers that control the virtualisation functions. Errors in implementing the resources provided by the hypervisor to the virtual machines (VMs) can also cause the hypervisor to be compromised. To this extent, CSPs who deploy server virtualisation should revert to certified, hardened hypervisors. The recommendations that manufacturers publish on configuring virtualisation servers securely should be used when hardening hypervisors. Certification should be based on the globally accepted "Common Criteria for Information Technology Security Evaluation", known as the Common Criteria for short. The depth of testing that should be achieved in the certification process is evaluation assurance level EAL 4 at least.

In the case of offerings in the "IaaS compute" form, virtual machines are provided to the customer, e.g. via a web interface. In terms of making the virtual machines secure, it is helpful if the provider gives their customer guidelines on hardening the virtual machines. The customer should also be able to upload their own images for the virtual machines or to purchase quality-assured images from the provider. PaaS or SaaS providers using server virtualisation, such as Microsoft with the Windows Azure platform, should also guarantee the security of the guest operating systems.

Network security

In the past, Cloud Computing platforms have often been misused either by placing malware there which is then used to send spam, or their processing power has been exploited to crack passwords using brute force attacks or to hide command and control servers (C&C servers) used to control. To prevent these and similar attacks as well as the misuse of resources, each CSP should take effective security measures to defend against network-based attacks. As well as the usual IT security measures such as anti-virus protection, Trojan detection, spam protection, firewalls, Application Layer Gateway and IDS/IPS systems, and particular care should be taken to encrypt all communication between the CSP and the customer and between the provider's sites. If a third party provider is required to deliver the services, the communication with them also needs to be encrypted.

Because of the concentration of resources in centralised data centres, an attack which is a particular threat to public Cloud Computing platforms is the Distributed Denial of Service (DDoS) [27] attack. According to a report by Arbor Networks, a provider of security solutions, DDoS attacks (such as the DNS Amplification/Reflection Attack) can now achieve enormous bit rates (over 100 Gbps) [9]. A standard backbone is designed for a far lower data rate. As a result, many CSPs can hardly defend against DDoS attacks using high data rates. This can have serious consequences for both the victim themselves and other connected customers. Against this background, each public CSP should undertake suitable measures to defend against DDoS attacks. Owing to the fact that many CSPs can scarcely protect themselves against DDoS attacks [32] using high data rates, the option exists to buy these mitigation services from larger Internet service providers (ISPs) and regulate their use in agreements. Measures should also be implemented to detect internal DDoS attacks by cloud customers on other cloud customers.

The incorrect configuring of a system is frequently the reason for successful attacks. As Cloud Computing platforms consist of many different components, the overall configuration is very complex. Changing a configuration parameter for one component (e.g. virtualisation server) can, when interacting with other components (e. g. network or storage) lead to security vulnerabilities, faulty functions and/or failures. For this reason, the components deployed are needed to be securely and carefully configured. All CSPs should also ensure that their networks

are suitably segmented, preventing any faults from spreading freely [24]. In this context the option exists to define and set up different security zones within the provider's network, based on the protection requirement. Examples include:
a. Security zone for managing the cloud
b. Security zone for the live migration, if server virtualisation is being used
c. Security zone for the storage network
d. With IaaS, customer to have their own security zones for the virtual machines The CSP's management network should be isolated from the data network.
If the cloud infrastructure or cloud services are being administered remotely, this needs to be accomplished via a secure communication channel. If a service consumer has particularly high availability requirements in terms of the services they are drawing down, the CSP's sites should be networked on a mutually redundant basis.

Application and platform security
In the case of offerings in the PaaS area, customers no longer have to worry specifically about database accesses, scalability, access controls, etc., as the platform provides these functionalities for them. Due to the fact that the customers use the platform's core functionalities to develop their own software, they can only succeed in developing software securely, if the entire software stack on the platform is developed and upgraded professionally and securely [23]. CSPs typically deploy not just a large number of different software components, but they also continue to upgrade them in order to be able to optimally provide their customers with the services in the runtime environment. When developing software, all CSPs must have established security as a fixed component in the software development life cycle process (SDLC process). Security issues need to be addressed at each phase of the software development process, and programs and modules may only be deployed if they have been properly tested and approved by the CSP's security manager. While software developed by the customer requires a secure basis (to be provided by the CSP), security issues also need to be considered in this respect. It is recommended that the CSP provides appropriate user guidelines for customers to create secure applications so that the programs the customer develops themselves fulfil certain minimum requirements in terms of security, documentation and quality. This is not only helpful for the customers but also emphasises the provider's expertise and reduces the danger of security vulnerabilities in customer software impacting on other customers. If the CSP also calls in other suppliers to provide the platform's services, these requirements apply equally to them. Alongside code reviews, automated review tools should also be deployed and vulnerability tests run. Automated review tools can, for example, detect common programming errors such as infinite loops and null pointer exceptions. Where there is a higher level of protection requirement, the CSP should also automatically check the code the customers have developed themselves for vulnerabilities. With PaaS, multiple customers share a common platform to run software. The customers' applications need to have guaranteed secure isolation, for example by using sandboxing technologies. Strict isolation of customer areas helps, for example, to prevent one application from unauthorised accessing another application's data.
As the cloud communication is fundamentally based purely on web technologies, e.g. web interfaces for cloud users and application administrators, application frameworks such as Java and .NET, communication via HTTP(S), the security of cloud applications against attacks at the application level takes on even more importance than is the case with traditional web applications. Therefore all CSPs should ensure that they comply with the principles of secure software development as specified in the Open Web Application Security Project when producing the applications designed against the main security risks for web applications (OWASP Top 10) [10]. It is still important to have a well-integrated, effective patch and change

management system so that operating faults are avoided and security vulnerabilities are minimised and can quickly be resolved. For quality assurance and in order to be able to detect errors and prevent future errors, each patch and each change should be adequately tested and their effectiveness evaluated before they are implemented.

Data security

The data life cycle comprises its generation, data storage, data usage, data distribution and data destruction. Each CSP should support all these phases in the data life cycle with appropriate security mechanisms. A number of storage technologies, e.g. NAS, SAN, Object Storage, etc., are used to store data. Common to all these storage technologies is the fact that many customers share common data storage. In this type of constellation, a secure separation of customer data is essential and should, therefore, be guaranteed [13].

The distinction between customers is then achieved using a so-called tenant ID. If the web application is insecurely programmed, a customer could possibly use an SQL injection to gain unauthorised access to another customer's data, and delete or manipulate it.

To avoid data losses, each CSP should do regular data backups based on a data security plan. Technical defects, incorrect parameterisation, obsolescent media, inadequate data media administration and non-compliance with regulations stipulated in a data security plan can result in an inability to reinstall backups and reconstruct the data inventory. So there is a need to sporadically check whether the data backups created to restore lost data can be re-used. Depending on the length of time between backing up the data and restoring the data due to data loss or some other incident, the most recent data modifications may be lost. So a CSP should immediately notify its customers if data backups need to be restored, and in particular indicate the status of the backup. The backing up of data should be transparent and editable for the customers.

Because of the underlying multi-tenant architecture, customer data can often only be deleted permanently and reliably at the request. The SLAs should make this period clear. When the specified time-scale has elapsed, all the customer data must then be fully and reliably deleted from each storage media. To delete data selectively, care must be taken to delete not only the current version but all previous versions, including temporary files and file fragments. Therefore all CSPs should have an effective procedure for securely deleting or destroying data and data media. Customers should ensure that their agreement specifies at which time and in which manner the CSP must completely delete or destroy their data or data media.

SECURITY MANAGEMENT

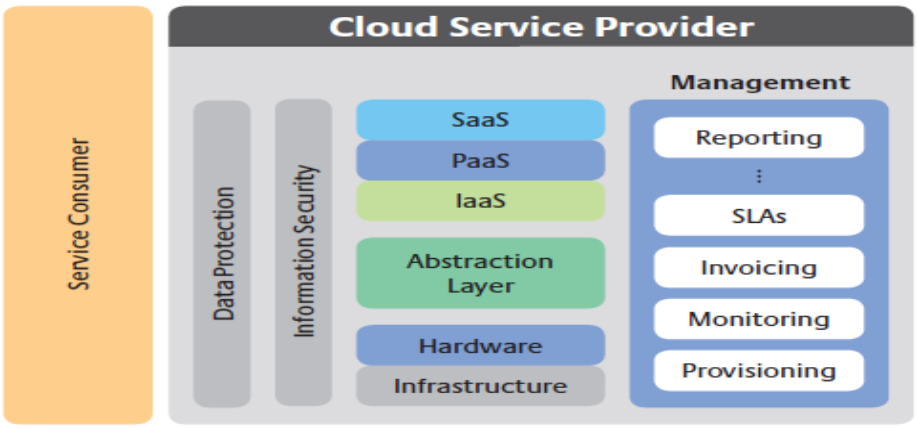

Figure 1: Reference architecture for Cloud computing platforms

A close look at the underlying reference architecture reveals that a provider needs to address a large number of tasks in order to provide cloud services. The tasks typical to a public CSP include:
. Providing a catalogue of services which describes the services being offered,
. Provisioning and de-provisioning resources such as virtual machines, load balancers, virtual data storages, IP and MAC addresses.

Another key task is to monitor the services provided to be able to comply with the guaranteed service quality. This monitoring is a continuing process. Any faults or failures in resources, e.g. virtualisation servers, virtual machines, load balancers, etc. need to be detected quickly so that appropriate countermeasures can be taken as rapidly as possible. Besides security management, other tasks that are usually part of a CSP's repertoire are[17]:
a. Patch and change management
b. Configuration management
c. Network management
d. System management
e. Application management
f. Reporting

The complexity and number of the above tasks require a structured approach. To this extent, each CSP should deploy standard procedural models such as ITIL and COBIT which can be used as guides when implementing IT processes. Trusting the CSP and their offerings is currently cited as a key motivator when users are asked why they decide for or are against cloud offerings. Trust is based on the assessment as to whether a provider has covered all the risks, both those in the data security area and in areas such as data protection, technology and the law – sufficiently, adequately and sustainably.

SECURITY ISSUES IN SERVICE MODELS

Cloud computing has three service models or delivery models; they are SaaS, PaaS and IaaS. This provides different kinds of services like application platform, software and infrastructure resources. Each delivery model has its own security issues.Table.1.describes the various types of security issues in delivery models.

A. Security Issues in SaaS In a conventional on-premise application deployment model, the confidential information of each organization persists to reside within the organizational boundary and which subject to its personnel security and access control policies, logical and physical. However, in the Software as a Service model, the organization information is kept beyond the organizational boundary, at the SaaS. Accordingly, the SaaS service provider should take on extra security polices to prevent data security and breaks due to security exposures in the application. Data location, Data Disposal, data Integrity, data Confidentiality, authorization and authentication, network attacks and data availability are challenges of Software as a Service delivery model[36].

a. Data Location Data Segregations and Data Location are also security issues in cloud, it provides shared resources of cloud and data locations. Cloud provider requires disclosing of information, Sometime Natural Disasters like flooding, extreme weather and earthquake breaks the security of customer's data.

b. Data Disposal Data disposal is refers to cloud preserving multiple copies of the single data. It leads to high availability of the data, but at the same time it is a major issue of cloud

computing data integrity. More copies of data are available in cloud, so deletion operation becomes more difficult for the cloud customers to preserve data integrity.

Security Issues	Affected Delivery Models			Solutions
	Saas	Paas	Iaas	
Offensive use of cloud computing	NO	YES	YES	Strong authentication and monitoring
Data Interruption	YES	YES	NO	High data protection
Malicious Insiders	YES	YES	YES	Cloud Transparency for management and security
Denial Of Service (DOS)	NO	YES	YES	Cloud Service provider delivers reliability and availability
Privacy breaks	YES	YES	YES	Provide communication protection
Shared Technology Issues	NO	NO	YES	Use Access Control mechanism
Service hijacking	YES	YES	YES	Provide security police and activity monitoring

Table.1.Describes the various types of security issues in delivery models

c. Data Integrity Data Integrity is the basic requirement of data security because the data integrity signifies protecting information from unauthorized modifications or deletion. CSP provides mechanisms for ensuring the data integrity. The Data Integrity also guarantees for data consistency, completeness and wholeness.

d. Data Confidentiality Data Confidentiality means provide data access by authorized users and systems. Strong authentication lacking is leads to illegal access. Cloud storage requires confidentiality because cloud provider should not access any user's data. Guarantees should be delivered to the customers, privacy policies, proper practices and procedures should be placed in cloud users of the data security.

e. Authorization and Authentication Mash-Up authorization explains attackers can pull data from the data sources or data leakages. Sometime, centralized access control techniques are may not be favor for all kind of customer's data. Increased authentication demands allows only thin clients to accessing cloud data because it supports only limited hosting of applications and data in cloud.

f. Network Attacks Social networking attacks, cloud storage stores large set of customer data. The pair of relationships between customers, suppliers, cloud providers and vendors connected to each other. It refers to data-loss.

g. Data Availability Cloud storage normally preserves multiple copies of single customer data on different servers often exist in different clouds or different locations. When a user tries to access some data or information, corresponding data should be available to access. The software and hardware should be available during the time of access based on demand of authorized users. Network availability is a major concern of Data Availability.

B. Security Issues in PaaS The users can use the intermediate equipment to create his program and provide it to the customers over the servers and internets. The user's controls the applications that run in cloud environment, but it does not control the hardware or network substructure and operating systems. Lack of validation, anonymous sign ups and service fraud are major issues of PaaS.

C. Security Issues in IaaS Cloud computing service provider delivers resources to authorized users at Pay-Per- use basis it reduces the initial investment in hardware such as processing power and networking devices. IaaS provides additional capabilities like more quickly and cost-effectively data access in an internal data centers. Reliability and physical locations are major issues in IaaS service model. But it does not provide reliability to the customer or user on the physical locations of cloud environment. In Iaas security issues are based on cloud deployment model. Issue depends on three kinds of parameters like infrastructure management

and ownership, infrastructure location and Access and consumption. Public cloud deployment model has major risk during data transformation time rather than the other cloud deployment models.

CONCLUSION

Cloud computing is the Internet based computing technology, which is empowered by virtualization. It describes a new model of IT services based on user consumption and delivery services. Virtualization is a creation of virtual or logical version rather than physical such as: hardware, platform, operating system and storage or network resources. Virtualization in cloud computing achieves high level of resource utilization by allowing one server to compute several task concurrently. The main motive of cloud computing is to offer robustness and ease over traffic congestion for IT services over the network. In business environment cloud computing concept is growing fast to increase facilities. Gradually more and more individuals and companies are placing information and data in cloud environment, thus arise a number of serious issues, such as: how much secure their services are, how service providers are providing data and application safety in cloud environment. Despite of all beneficial services enterprise customers are still unwilling to deploy their business in cloud. Hence security is the major issue to slow down the growth of cloud computing adaption. In addition, around 40% of total respondents said that there had been increased attacked against their customers by technical sophistications [6]. New risks and possible threats are exploited in cloud computing services. It is necessary to analyze and understand cloud computing risks and threats in order to protect systems and data from vulnerabilities. Improvement of cloud computing security mechanisms are primary step towards ensuring secure cloud computing environment. Consumer only can rely on cloud computing if their services are secure enough to use. Hence some security challenges are needed to be concern about such as: application security, data transmission security, storage security and security related to use third party resources. And this can be achieved by service model specific security deployment in cloud Computing.

REFERENCES

1. C. Linda Hepsiba, J.G.R.Sathiaseelan, Security Issues in Service Models of Cloud Computing IJCSMC, Vol. 5, Issue. 3, March 2016, pg.610 – 615. ISSN 2320–088X.
2. PENG Yong, ZHAO Wei, DAI Zhong-hua and CHEN Dong-qing.”Secure cloud storage based on cryptographic techniques”. The Journal of China Universities of Posts and Telecommunications.ELSEVIER, 2012. S1005-8885(11). pp:182- 189.
3. Koorosh Goodarzi and Abbas karimi. “Cloud Computing Security by Integrating Classical Encryption ”. International Conference on Robert PRIDE.ELESVIER, 2014. 1877-0509. pp: 320-326.
4. M.Bhavana Sharma. “ Security Architecture of Cloud Computing based on Elliptic Curve Cryptography(ECC) “.International Journal of Advances in Engineering Sciences, 2013.Vol.3(3). E-ISSN: 2231-0347. Print-ISSN: 2231-2013.
5. Swarnalata Bollavarap and Bharat Gupta. “Data Security in Cloud Computing”. International Journal of Advanced Research in Computer Science and Software Engineering, 2014.Volume 4. Issue 3. Pp: 1208-1215.
6. Dimitrios Zissis and Dimitrios Lekkas. “Addressing Cloud Computing Security Issues”. ELESVIER, 2012.pp. 583-592.
7. Jawahar Thakur and Nagesh Kumar. “DES, AES and BLOWFISH : Symmetric key Cryptography Algorithms Simulation Based Performance Analysis”. International Journal of Emerging Technology and Advanced Engineering, 2011. Volume 1.Issue 2. ISSN: 2250-2459
8. Neha Mishra, Shahid Siddiqui and Jitesh P.Tripathi. “A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues”. BVICAM’s International Journal of Information Technology , 2015.Vol.7 No.1. ISSN: 0973-5658.
9. Alowolodu O.D , Alese B.K, Adetunmbi A.O., Adewale O.S and Ogundele O.S. “Elliptic Curve Cryptography for Securing Cloud Computing Applications”. International Journal of Computer Applications, 2013. (0975-8887).
10. Gopinath.v and Bhuvaneswaran R.S. “Study on Secure Cloud Computing with Elliptic Curve Cryptography”. International Journal of Computer Science Issues, 2014.Vol.11. Issue 5. No2.E-ISSN:1694-0784. Print- ISSN: 1694-0814.

11. F.Amounas and E.H.El Kinani. "ECC Encryption and Decryption with a Data Sequence".Applied Mathematical Sciences, 2012. Vol.6. No. 101, 5039-5047.
12. Parsi Kalpana and Sudha Singaraju. "Data Security in Cloud Computing using RSA Algorithm". International Journal of Research in Computer and Communication Technology, 2012.Vol.1. Issue 4. ISSN: 2278- 5841.
13. Chandu Vaidya and Prashant Khobragade. " Data Security in Cloud Computing". International Journal on Research and Innovation Trends in Computing and Communication, 2015. Volume ,3. Issue.5. ISSN: 2321-6169. pp: 167-170.
14. Veerraju Gampala, Srilakshmi Inuganti and Satish Muppidi. "Data security in Cloud Computing With Elliptic Curve Cryptography". International Journal of soft Computing and Engineering, 2012. Volume.2. Issue.3.ISSN: 2231-2307.
15. Lo'ai Tawalbeh1, , Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari1. "A Secure Cloud Computing Model based on Data Classification". First International Workshop on Mobile Cloud Computing Systems, Management, and Security.ELESVIER, 2015. 1153 – 1158.
16. Prince Jain, "Security Issues and their Solution in Cloud Computing", International Journal of Computing & Business Research ISSN (Online):2229-6166.
17. Hashizume et al. "An Analysis of Security Issues for Cloud Computing", Journal of Internet Services and Applications. Springer, 2013.
18. Osama Harfoushi, Bader Alfawwaz, Nazeeh A, Ghatasheh, Ruba Obiedat, Mua'ad M. Abu-Faraj and Hossam Faris,"Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review" .Communications and Network, 2014, 6, 15-21.
19. A.P.Bhutada and S.L.Magar. "Executing DES Algorithm in Cloud Data Protection". International Journal of Innovative Research in Engineering and Technology**.**Leiutis, 2015. Volume.1.Issue.1.
20. Shivali munjal and Ramandeep singh. " Data Security in Cloud Computing" IJSER, 2014. Volume.5, Issue.3,ISSN :2229- 5518.
21. M.Mohamed Sirajudeen and Dr. K. Subramanian, "Security Issues on Data Transfer under Clouds – An Overview" September – October 2014 International Journal of Information Technology Infrastructure. Volume.3. No.5.ISSN: 2320 2629.
22. Kuyoro S.O,Ibikunllef and Awodele.O,"Cloud Computing security issues and challenges",IJCN,2011.
23. Mohammed A.Alzain,Ben Soh and Eric Pardede, "A survey on data security in cloud Computing,"Journal of software, May 2013.
24. M.Ali, S.U.Khan and A.V.Vasilakos. "Security in Cloud Computing: Opportunities and Challenges". Information Sciences.ELESVIER, 2015.INS 11378.
25. Ramgovind S, Eloff MM and Smith E. "The Management of Security in Cloud Computing". IEEE. 2010. 978-1-4244-549.
26. Kulvinder Singh, Sarita Negi "Service Model Specific Security Requirements and Threats in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 7, July 2015
27. Kulvinder Singh, Tanshu Gairola "Cloud Security Issues: Counter DDOS Attack by Integrating IP Monitoring and Routing Protocol" IJARCSSE, Volume 6, Issue 7, July 2016
28. M. Sugumaran ,BalaMurugans D. Kamalraj. "An Architecture for Data Security in Cloud Computing" .World Congress on Computing and Communication Technologies. 2014
29. Shuai Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, "Cloud Computing Research and Development Trend", 2010 Second International Conference on Future Networks.
30. Siyuan Xin, Yong Zhao, Yu Li, "Property-Based Remote Attestation Oriented to Cloud Computing"**,** 2011 Seventh International Conference on Computational Intelligence and Security2011 .
31. Amazon.com, Amazon Web Services (AWS). Online at http://aws.amazon.com.
32. Kulvinder Singh, Tanshu Gairola "A Review on DOS and DDOS Attacks in Cloud Environment & Security Solutions" International Journal of Computer Science and Mobile Computing,Vol. 5, Issue. 7, July 2016, pg.136 – 141
33. http://www.pcmag.com/article2/0,2817,2372163,00.asp.
34. http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html.
35. Kangchan Lee, "Security Threats in Cloud Computing Environments1"**,** International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012
36. P. A. Karger, "Multi-Level Security Requirements for Hypervisors", ISBN: 0-7695-2461-3, 21st Annual Computer Security Applications Conference, **(2005)** December 5-9, pp. – 275.
37. Cloud Computing and Security, A Natural Match, http://www.trustedcomputinggroup.org/files/resource_files/1F4DEE3D-1A4B B294D0AD0742BA449E07/Cloud%20Computing%20and%20Security%20Whitepaper_July29.2010.pdf, **(2010)**.