ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

An Innovative Method to Improve Security in Cloud: Using LDAP and OSSEC

Shikha Nema[1], Shailendra Singh Raghuwanshi[2]

Student, Dept. of C.S.E, Takshshila Institute of Engineering& Technology, Jabalpur (M.P.), India[1]

Professor, Dept. of C.S.E., Takshshila Institute of Engineering& Technology, Jabalpur (M.P.), India [2]

ABSTRACT: Cloud computing refers to the delivery of computing resources over the Internet. Cloud computing is a diverse technological concept that is consequence of decades of research in parallel computing, virtualization, networking and communication, utility computing and Service-Oriented Architecture (SOA). Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. It offers an on-demand and scalable access to a shared pool of resources hosted in a data centre at providers' site. It reduces the overheads of up-front investments and financial risks for the end- user. The qualitative services and lower cost of services are the key requirements of this technology. Owing to the financial nature of use of the cloud services based on Service Level Agreements (SLA) makes these issues even more serious that needs to be taken care of. This work presents an overview, style and actuality of cloud computing with the objective of presenting challenging issues concerned with various aspects of cloud computing

KEYWORDS*:* Cloud Computing, IT, IaaS, PaaS, SaaS, SOS, SLA

I. INTRODUCTION

Cloud computing offers the same model having above describe properties in which services are delivered over internet in an on-demand elastic way for which the charges are paid at release time of resources. In general, cloud is a multifarious technological paradigm that is an extension of many existing technologies viz. parallel and distributed computing, Service-Oriented-Architecture (SOA), virtualization, networking etc. The distributed computing, virtualization and internet works as indispensable building blocks of the cloud computing. It is a highly sharable computing paradigm where processing, storage, network, applications etc. are shared. The objective of the cloud computing is to provide secure, qualitative, scalable, quick, more responsive, on demand, cost-efficient and automatically provisioned services viz. computation services, storage services, networking etc. being provided in a transparent way (location independent). Cloud computing can help to improve business performance while making a contribution to control the cost of delivering IT resources to any organization.

The fundamental idea of cloud computing was pronounced way back in 1960 by Professor John McCarthy, as; "If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. The computer utility could become the basis of a new and important industry". Initially, telecommunication service providers delivered dedicated point-to-point circuit, which was the wastage of the bandwidth; the problem was solved by using VPN services where traffics could be switched to balance the utilization of the overall network. Cloud computing was a buzz word for many years and it turned into reality in 2007 when IT giants Google and IBM announced a collaboration in this domain followed by "Blue Cloud" announcement by IBM [2, 3, 4]. According to blog [5], the prediction of IT advisory company Gartner says that cloud computing business will surpass $148 billion mark by 2014 while its competitor, Forrester, says it will reach $118 billion. Another Gartner's Survey says that the investment on services in public cloud is expected to increase 18.6% in 2012 to $110.3B that achieves a 17.7% Compound Annual Growth Rate (CAGR) from 2011 through 2016 [1]. In general, the total market is likely to increase to $210B in 2016 from $76.9B in 2010. Figure 1 gives a glimpse of the distribution of workloads in cloud and a traditional data centre that shows that popularity of cloud will be grow with a very fast rate. Therefore, cloud computing area looks very promising for researchers and businesses. On

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

the other hand, its realization brings many challenging issues that need to be carefully addressed. The organization of remaining paper is as follows. Section 2 presents a overview of cloud computing, it's essential characteristics, different deployment models and service models. Section 3 describes the advantages and disadvantages of cloud. Section 4 describes various issues and challenges of cloud computing that are necessary to address in order to adopt this technology. Finally, section 5 concludes the papers.

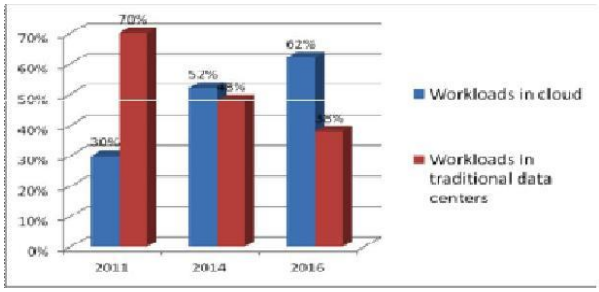

Fig.1.1Workload distribution in cloud and traditional data centers [1]

II. ISSUES AND CHALLENGES OF CLOUD COMPUTING

A. *Security and Privacy:*

The existing computing paradigms viz. distributed computing, SOA, networking etc. are building blocks of cloud computing. Current cloud adoption is associated with numerous challenges as shown in Figure 2 and 3 depicting the specific business risk of adopting cloud services and biggest barriers. Therefore, these issues must be addressed in order to provide high quality services to the users while complying with the service provider's needs. The issues can be organized into several different categories varying from security, protection, identity management, resource management, power and energy management, data isolation, availability of resources, and heterogeneity of resources. Although, there are several issues that demand attention but the following could be treated as of prime concern [11-14]:

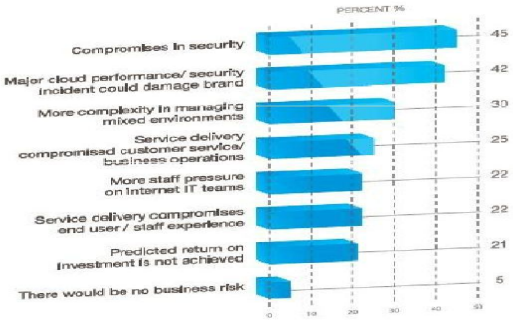

Fig. 2.1 Specific Business Risk of adopting cloud services

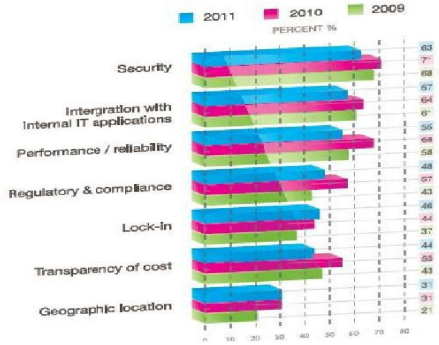

Fig. 2.2 Biggest Barriers to adoption of cloud services

According to the survey of International Data Corporation (IDC), Security, Performance and Availability are the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

three biggest issues in cloud adoption. The critical challenge is how it addresses security and privacy issues which occur due to movement of data and application on networks, loss of control on data, heterogeneous nature of resources and various security policies. Data stored, processing and movement of data outside the controls of an organization poses an inherent risk and making it vulnerable to various attacks. The security threats can be of two types viz. internal and external. The external risk is posed by various persons and organizations e.g. enemies or hackers that do not have direct access to the cloud. The internal security risk is a well-known issue, which can be posed by organizational, affiliates, contractors, current or former employees and other parties that have received access to an organization's servers, networks and data to facilitate operations. Cloud computing poses privacy concerns because the service providers may access the data that is on the cloud that could accidentally or deliberately be changed or even removed posing serious business trust and legal consequences [8, 11-14].

B. *Performance:*

According to IDC's survey, performance is the second biggest issue in cloud adoption. The cloud must provide improved performance when a user moves to cloud computing infrastructure. Performance is generally measured by capabilities of applications running on the cloud system. Poor performance can be caused by lack of proper resources viz. disk space, limited bandwidth, lower CPU speed, memory, network connections etc. Many times users prefer to use services from more than one cloud where some applications are located on private clouds while some other data or applications being on public and/or community cloud. The data intensive applications are more challenging to provide proper resources. Poor performance can results in end of service delivery, loss of customers, reduce bottom line revenues etc. [2, 11, 13].

C. *Reliability and Availability:*

Any technology's strength is measured by its degree of reliability and availability. Reliability denotes how often resources are available without disruption (loss of data, code reset during execution) and how often they fail. One of the important aspect that creates serious problems for the reliability of cloud computing is down time. One way to achieve reliability is redundant resource utilization. Availability can be understood as the possibility of obtaining the resources whenever they are needed with the consideration to the time it takes for these resources to be provisioned. Regardless of employing architectures having attributes for high reliability and availability, the services in cloud computing can experience denial of service attacks, performance slowdowns, equipment outages and natural disasters. Data shows that some of the current cloud computing providers have some frequent outages last year. e.g Amazon EC2 outage. In order to remove FUDD (fear, uncertainty, doubt, and disinformation), probably the reliability, availability and security are the important and prime concern to an organization. Therefore, the level of reliability and availability of cloud resources must be considered as a serious issue into the organization's planning to set up the cloud infrastructure in order to provide effective services to consumers [19].

D. *Scalability and Elasticity:*

Scalability and elasticity are the most amazing and unique features of the cloud computing. These features provide users to use cloud resources being provisioned as per their need in unlimited amount as required. Scalability can be defined as the ability of the system to perform well even when the resources have been scaled up. Elasticity, on the other hand, is the ability to scale resources both up and down as and when required. Elasticity goes one step further, though, and does also allow the dynamic integration and extraction of physical resources to the infrastructure. The elastic cloud computing means that allocation of resources can get bigger or smaller depending on the requirement. Elasticity enables scalability—which means the system can easily scale up or down the level of services to which the user has subscribed. Scalability can be provided in two ways- horizontally and vertically whereby horizontal scalability (Scale Out) refers to addition of more nodes to the system such as adding a new computer to an existing service provider system while vertical scalability (scale up) refers to addition of resources to a single node in the system, typically involving the addition of memory or processors to a single computer [19].

E. *Interoperability and Portability:*

Interoperability is the ability to use the same tools or application across various cloud service providers platforms. The interoperability can be defined at various levels viz. application, service, management and Data interoperability. Cloud users must have the flexibility of migrating in and out and switching to clouds whenever they want without no

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

vendor lock-in period. One of the adoption barriers in cloud computing interoperability is the vendor lock-in risk. The main problems to realize it are the lack of open standards, open APIs and lack of standard interfaces for VM formats and service deployment interfaces. Cloud portability ensures that one cloud solution will be able to work with other platforms and applications as well as with other clouds [14].

F. *Resource Management and Scheduling:*

Resources management can be consider at various levels viz. hardware, software, virtualization level with performance, security and other parameters being dependent on the management and provisioning of resources. It includes the management of memory, disk space, CPU's, cores, threads, VM images, I/O devices etc. Resource provisioning can be defined as allocation and management of resources to provide desired level of services. Job scheduling is a type of resource provisioning where jobs execution order is established in order to finish job execution to optimize some parameters viz. turnaround time, response time, waiting time, throughput and resource utilization. Since cloud computing is a combination of many existing technologies, existing job scheduling strategies are eligible to be applied on cloud system. The major issues of job scheduling on cloud systems are partitioning of jobs into parallel tasks, interconnection network between clouds or processors, assigning priority to jobs and selection of processors or cloud to allocate the job(s), job flexibility, level of pre-emption supported, workload characteristics, memory allocation, task execution monitoring, recourse allocation requirements, topology, nature of the job, effect of existing load, load balancing, parallelism, job migration policy, redundant Resource selection, synchronization, communication overheads, job pre processing requirements etc. The job scheduling is one of critical process that must be decided very carefully and wrong selection of scheduling strategy can lead to devastating effect on performance leading to wastage of resources while falling to meet Quality of Service (QoS) standards.

G. *Energy Consumption:*

According to a survey done by Amazon as shown in Figure 4, the cost consumption of Amazon data centers is shocking as 53% of the total cost is consumed by the servers for a 3-year amortization period while energy and cooling requirements consume 42% of the total budget including both direct power consumption (~19%) and the cooling requirements (23%) for amortization period of 15-years [16]. In 2006, data centers of United States consumed more than 1.5% of the total energy produced in that year, and this percentage is expected to increase 18% annually [15].

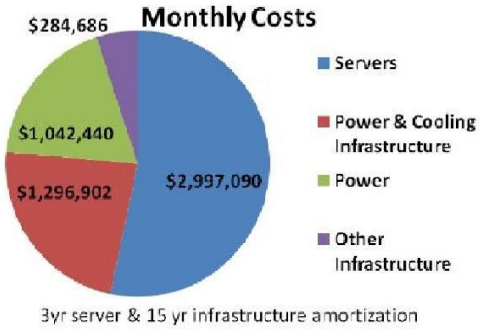

Fig. 2.3 Monthly server, Power and Infrastructure costs [16]

Cloud data centers house thousands of servers and set up the cooling infrastructure to remove heats generated by these servers. These servers and cooling infrastructure consume a large amount of energy and produces green house gases (GHGs). In addition, the cloud data centres which are inherent part of the cloud infrastructure are also very expensive to operate and consume energy at a very large scale. For example, the power consumption of Google data centre is equivalent to a city such as San Francisco. Since ICT aids towards developing applications and facilities for human prosperity, we require designing such hardware, software, scheduling policies, networks and other protocols that consume energy in eco-friendly and optimized manner. The goal is not only to reduce the consumption of energy and hence the cost consumed by data centers, but also to maintain environmental standards necessary not only to survive but to thrive [16, 20].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

III. PROPOSED WORK

This paper proposes a security solution to a number of challenges in a cloud environment, which leverages consumers from the security burden, by trusting a Third Party. Trust basically operates in a top-down approach, as each layer needs to trust the layer immediately below it, and requires a security guarantee at an operational, technical, procedural and legal level to enable secure communications with it. A trusted certificate serves as a reliable electronic ‘‘passport’’ that establishes an entity’s identity, credentials and responsibilities.

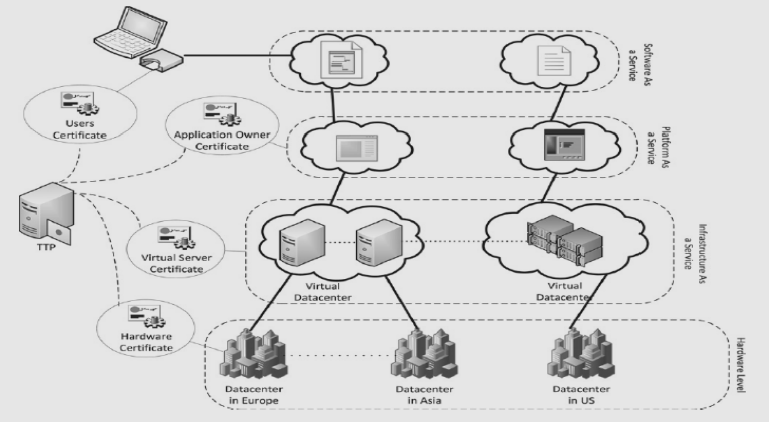

Fig.3.1 Certificate Moving Through Different Layer in Cloud Environment

A Trusted Third Party is able to provide the required trust by guaranteeing that communicating parties are who they claim to be and have been scrutinized to adhere to strict requirements. This process is performed through the certification process, during which an entity requiring certification is required to conform to a set of policies and requirements. TTP is an ideal security facilitator in a distributed cloud environment where entities belonging to separate administrative domains, with no prior knowledge of each other, require establishing secure interactions. An end user is required to use his personal digital certificate to strongly authenticate himself with a cloud service and validate his access rights to a required resource. This certificate is used in combination with the service provider’s certificate (PaaS, SaaS or IsaS level) to create a secure SSL connection between them and the certificate moving through different layers in cloud and different environments.

The proposed solution calls leading LDAP protocol infrastructure, to ensure the authentication, integrity and confidentiality of involved data and communications. A TTP is tasked with assuring specific security characteristics within a cloud environment, while realizing a trust mesh between involved entities, forming federations of clouds. This approach makes use of a combination of Public Key Cryptography, Single-Sign-On technology and LDAP directories to securely identify and authenticate implicated entities. The model presented in this paper offers the advantages of each single technology used and deals with their deficiencies through their combined implementation. The trusted third party can be relied upon for:

- Generating Security Domains.
- Low and High level confidentiality
- Server and Client Authentication.
- Certificate-Based Authorization
- Cryptographic Separation of Data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

A. *Implementation of OSSEC in Cloud*:

OSSEC is an open source host-based intrusion detection system (HIDS). OSSEC is a scalable, multi-platform, open source , Host based Intrusion Detection System (HIDS). It has a powerful association and analysis mechanism, integrating log analysis; file veracity checking, centralized policy enforcement, Windows registry monitoring, root kit detection, active response and real-time alerting. It runs on most operating systems, including OpenBSD Linux, MacOS, FreeBSD, Solaris and Windows. OSSEC is composed of several pieces. It has a central manager monitoring the whole thing and accepting information from agents, databases, syslog and from agent less devices. This diagram shows the central manager receiving events from the system logs from remote devices and agents. When something is detected, active responses can be executed and the admin is notified.

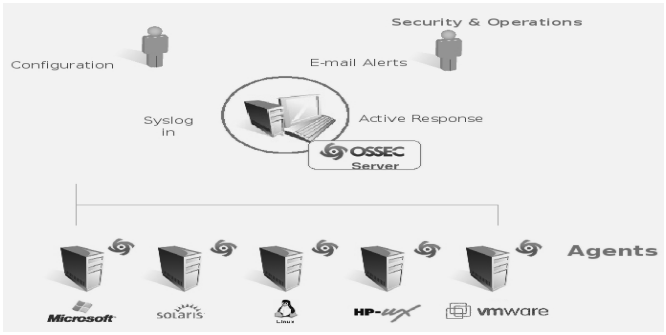

Fig.3.2 Architecture of OSSEC

We are using OSSEC HIDS because it not only does all the analysis we mention in here, but also has rules for multiple log formats, making our correlation simpler. There are two models for OSSEC implementation.

- Local (when you have just one system to monitor).
- Client/Server for centralized analysis.

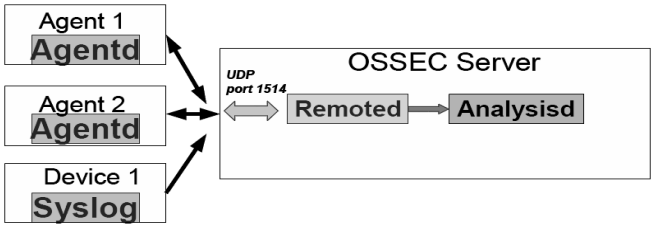

Fig 3.3 Agent/Server Network Communication

Focus now on the main process (ossec-analysisd)

- It does the log decoding and analysis
- Hard worker!

Log pre-decoding
Log decoding
Log Analysis
Example of alerts

Log analysis is one of the most overlooked aspects of intrusion detection. These are some of the things your analysis tool should do:

- Understand your logs. Know what is good and what is bad.
- Correlate the bad events looking for patterns that may indicate an attack or intrusion.
- Correlate the good events with the bad events (eg. multiple failed logins followed by a successful one).
- Correlate the good events (eg. too many successful logins for the same user across multiple hosts in a small period of time).
- Look for unusual patterns that are not in your good or bad list.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

B. *Algorithm Steps of Authentication and Security Implementation:*

This section presents the algorithm of complete certificate based multi-level authentication technique. Multi-level authentication system reads the details given by organization, team and user and produces the password output at different levels. After making user request for cloud services, these steps are followed by the organization:

Step1. First both the ends are authenticating themselves by simple server and client Authentication.

Step2. After that in cloud service layer a certificate based authorization is generated for authenticate and validate the requested user and data.

Step3. The same digital certificate is moved to different cloud layer to validate user and protect data by using LDAP protocol to identify threads.

Step4. At same time the information is detected by using OSSEC system that avoids intrusions based on specific events or set of events.

Therefore, we conclude that by using multi-level authentication technique, we can improve the security folder.

C. *Comparisons of Proposed Model:*

Points for Discussion	Credentials on Based Model	Credentials on Based Model	Secured Channel	Proposed Model
Information leakage probability	Medium	Medium	Medium	Low
Security Breaking Probability	Medium	Medium	Medium	Low than others
Cost of Establishing	Low	Medium	High	Medium
Execution Time	Small	Medium	Small	Medium

Table 3.1 Advantages of the Proposed Model

IV. CONCLUSION

Cloud computing can be considered as an integral component of almost all businesses in near future and it is expected to change the landscape of IT industry. It is based on the model of delivering services on internet with pay-as-you-go model with advantages like no up-front cost, lower IT staff, lower cost of operation to name a few. Although cloud computing has bright prospects both for business and researchers certain challenging issues including security, performance, reliability, scalability, interoperability, virtualization etc. needs to be addressed carefully. Many e-governments and business standards provide guidelines on the strong authentication. They mandate use of two-factor authentication and concentrate on different aspects of authentication like authentication token, token management and communication protocols. We describe the security issues related to the cloud computing; help to better understand the protocols and the principles behind it thus make better authentication. A combination of LDAP protocol can address most of the identified threats in cloud computing dealing with the integrity, confidentiality. The server and agents communicate securely by means of encryption. OSSEC also has intrusion avoidance features, being able to respond to specific events or set of events by using commands and active responses.

REFERENCES

1. Upen Nathwani, Irvin Dua, Ved Vyas Dwivedi, 'Authentication in Cloud Application: Claims-Based Identity Model, 'International Journal Inventi (Impact/Rapid) - Cloud Computing, Research Article, Jan 1, 2013 Volume, Issue 1, pages 1 – 3.
2. RajkumarChalse, Ashwin Selokar & ArunKatara, 2013, "A Nesw Technique of Data Integrity for Analysis of the Cloud Computing Security", 5th International Conference on Computational Intelligence and Communication Networks, 978-0-7695-5069-5/13, pp.469-473.
3. Puya Ghazizadeh, Ravi Mukkamala & Stephan Olariu, 2013, "Data Integrity Evaluation in Cloud Database-as-a-Service", IEEE Ninth World Congress on Services, 978-0-7695-5024-4/13, DOI 10.1109/SERVICES.2013.40, pp.280-285.
4. V. Nirmala, R. K. Sivanandhan& Dr. R. Shanmugalakshmi, 2013, "Proceedings of 2013 International Conference on Green High Performance Computing", India, 978-1-4673-2594-3/13.
5. GurudattKulkarni ,Jayant Gambhir Gurudatt Kulkarni , Jayant Gambhir, Tejswini Patil & Amruta Dongare, 2012, "A Security Aspects in Cloud Computing", Journal of Engineering Science and Technology (IJEST), pp.447-450.
6. D. Sureshraj & Dr. V. Murali Bhaskaran, 2012, "Automatic Dna Sequence Generation For Secured Cost-Effective Multi -Cloud Storage", Ieee.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

7. Su Qinggang& Wang Fu, 2012, "Study of Cloud Computing Security Service Model" , IEEE the information security industrialization project, National Development and m Commission, No. [2010] 3044.
8. IaaS - Which One is for You?", posted Tuesday, June 28, 2011. Eman M. Mohamed, Sherif EI-Etriby & Hatem S. Abdelkader, 2012, "Enhanced Data Security Model for Cloud Computing" , IEEE The 8th International Conference on Informatics and Systems (INFOS2012) - 14-16 May Cloud and Mobile Computing Track, pp. cc-12 – cc-17.
9. Zhongbin Tang, Xiaoling Wang, Li Jia, Xin Zhang, Wenhui Man, 2012, "Study on Data Security of Cloud Computing", 978-1-4577-1964-6/12.
10. Ling Lang & Lin wang, 2012, "Research on cloud computing and key technologies", IEEE International Conference on Computer Science and Information Processing (CSIP), 978-1-4673-1411-4/12, pp.863-866.
11. Suba Surianarayanan & T. Santhanam, 2012, "Security Issues and Control Mechanisms in Cloud", Proceedings of 2012 International Conference on Cloud Computing, Technologies, Applications & Management 97 8-1-4673-4416-6 /12, pp.74-76.
12. Gebeyehu Belay Gerbremeskel, Chengling Wang & Zhongshi He, 2012, "The Paradigm Integration of Computation Intelligence Performance in Cloud Computing Towards Data Security", IEEE 2012 Fifth International Conference on Information and Computing Science, 2160-7443/12, pp.19-22
13. Parikshit Prasad, BadrinathOjha, Rajeev Ranjanshahi & Abhishek Vaish, 2011, "3 Dimensional Security in Cloud Computing", 978-1-61284-840-2/11, pp. 198-201
14. Amir Mohamed Talib, Rodziah Atan, Rusli Abdullah &Masrah Azrifah, 2011, "Cloud Zone: Towards an Integrity Layer of Cloud Data Storage Based on Multi Agent System Architecture", IEEE Conference on Open Systems (ICOS2011), September 25 - 28, 2011, Langkawi, Malaysia, 978-1-61284-931-7/11, pp. 127-132
15. Uma Somani, Kanika Lakhani, Manish Mundra , 2010,"Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC) ,pp.211-216
16. Chenguang Wang & Huaizhi Yan, 2010 , "Study of Cloud Computing Security Based on Private Face Recognition", IEEE Basic Research Program of Beijing Institute of Technology ,978-1-4244-5392-4/10
17. P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar, H. Medhioub, and D. Zeghlache, "Challenges for Cloud Networking Security", Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 68, Part VII, 298-13, DOI: 10.1007/978-3-642-21444-8_26 , Springer Link, 2011.
18. Basant Narayan Singh," Cloud Service Models - SaaS PaaS
19. D. Molnar, S. Schechter, (2010) self hosting vs. cloud hosting: accounting for the security impact of hosting in the cloud. In: Workshop on the economics of information security.
20. OSSEC Homepage - www.ossec.net

BIOGRAPHY

Mrs.Shikha Nema is a student of Takshshila Institute of Engineering & Technology, Jabalpur (M.P.) India. Presently she is pursuing her M.Tech [CSE] from this college and she received her B.E degree from TIETECH, affiliated to RGTU University, Bhopal, in the year 2004. She has published three International paper and two paper presented in National Confreance .Her area of interest includes Networking and Network Security, all current trends and techniques in Computer Science.

Prof. Shailendra Singh Raghuwanshi received the B.E. & M.E.degree on Computer Science & Engineering form R.G.P.V University in 2005 and 2013.. He has been doing lectureship since 2005 and promoted to Associate Professor at CSE Department, since 2013. He has published two conference, journal papers and one paper presented . His research interests are as follows: Networking, Cloud Computing, Network Security, Computer Architecture, Speech/ Image processing and applications.