A Novel Approach to Enhanced Security in Public Cloud: Using LDAP Protocol

ShikhaNema , Prof.Shailendra Singh Raghuwanshi

***Abstract*-The modern appearance of cloud computing has considerably changed everyone's view of infrastructure architectures, software release and progress models. Projecting as an advancement step, following the transition from mainframe computers to client/server deployment models, cloud computing include elements from utility computing, grid computing and autonomic computing, into modern deployment architecture. This express conversion towards the clouds has increase concerns on a significant issue for the success of information systems and security. From a security point of view, a number of unchartered threats and challenges have been commenced from this replacement to the clouds, abating much of the usefulness of conventional safety mechanisms. As a result the aim of this paper is twofold; firstly to assess cloud security by identifying exclusive security requirements and secondly to attempt to present a feasible solution that reduce these potential threats. This paper proposes a Trusted Third Party, tasked with guarantee definite security characteristics within a cloud environment. The proposed solution calls upon higher bit cryptography, particularly Public Key Infrastructure operating in concert with LDAP, to make sure the integrity, authentication and confidentiality of concerned data and communications in cloud environment.**

***Keywords*- Authentication, integrity, certificate distribution, certificate based authorization, cryptography**

I. INTRODUCTION

Cloud Computing refers to manipulating, accessing and configuring the applications online. It offers online data storage, infrastructure and application. Cloud computing is an IT operation form, based on virtualization, where resources, in terms of infrastructure, appliance and data are deployed via the internet as a distributed service by one or some service providers[]. These services are scalable on require and can be valued on a pay per use basis. Cloud infrastructure provides extensive facilities for the client such as process, storage, power, networks, space and other computational possessions, so that the customer can set and perform their convention software as well as applications and operating system. Client does not supervise or organize the cloud infrastructure yet they have been in charge of on operating systems, applications, storage space and probably their collection and components.

Manuscript received Sep, 2014.

***Shikha Nema** , Department of Computer Science & Engineering, Takshshila Institute of Engineering &Technology,Jabalpur(M.P.).*
***Prof.Shailendra Singh Raghuwanshi**, , Department of Computer Science & Engineering, Takshshila Institute of Engineering & Technology, Jabalpur(M.P.).*

One of the main apprehension in cloud computing is the possibility of incursion of privacy. As cloud computing is achieving augmented popularity, apprehension are being voiced about the safety issues bring in through the acceptance of this new model. The usefulness and efficiency of conventional protection mechanismsare being reconsidered, as the description of this inventive deployment model, be different broadly from them of conventional architectures. In this thesis we attempt to expose the exclusive security challenges introduced in cloud surroundings and clarify issues from a safety standpoint.

II. CLOUD COMPUTING TECHNOLOGIES

There are definite technologies that are working at the back the cloud computing stage making cloud computing flexible, trustworthy and usable. These technologies are listed below:

1. Virtualization
2. Service-Oriented Architecture (SOA)
3. Grid Computing

A. Virtualization

Virtualization is a technique, which allows sharing single physical instance of an application or resource among multiple organizations or tenants (customers). It does so by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded. The Multitenant architecture offers virtual isolation among the multiple tenants and therefore the organizations can use and customize the application as though they each have its own instance running.

B. Service-Oriented Architecture (SOA)

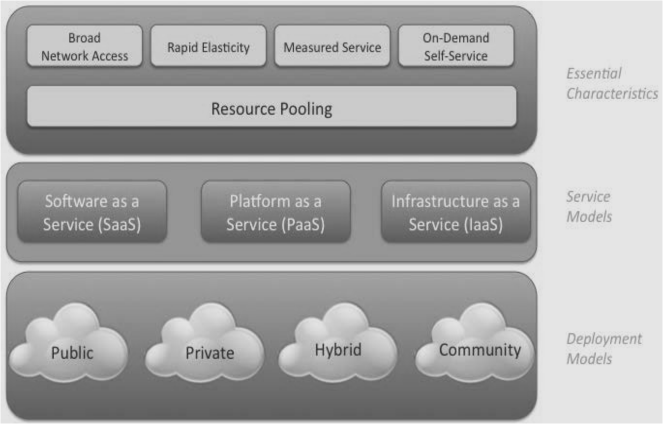
Service-Oriented Architecture helps to use applications as a service for other relevance regardless the type of trader, creation or technology. Therefore, it is potential to substitute of data among applications of different merchant without other programming or making changes to services. Cloud computing-service familiarized architecture.

C. Grid Computing

Grid Computing refers to distributed computing in which a collection of computers from numerous locations are associated with each other to accomplish common objective. These computer resources are diverse and geographically spread. Grid Computing breaks multipart task into minor pieces. These smaller pieces are distributed to CPUs that inhabit contained by the grid.Usefulness computing is based on pay per model. It proposes computational resources on require as a metered provision. Cloud computing, managed IT services and grid computing are based on the conception of utility computing.

III. CLOUD COMPUTING ARCHITECTURE

The Architectural Componentsof the Reference Architecture describes the important aspects of service deployment and service orchestration. The overall service management of the cloud is acknowledged as an important element in the scheme of the architecture. Business Support mechanisms are in place to recognize customer management issues like contracts, accounting and pricing and are vital to cloud computing.



A. SAAS (Software as a Service)

SAAS is a software form provided by the merchant through an online facility. It provides network-based right of entry to commercially accessible software. User interface powered by "thin client" relevance cloud mechanism; statement via (Application Program Interfaces (APIs), loosely coupled, stateless, semantic, interoperability modular. This will stay away from capital overheads on software and expansion resources; reduced Return on Investment (ROI) risk, modernized and iterative updates. On the different, Centralization of data involves new/different sanctuary measures. Examples of SaaS consist of Netflix, Intuit QuickBooks Online, Gmail, and Google Docs. The four most important advantages of Saas are:-

1. Lowered cost of implementation and upgrades
2. Reduced support requirements
3. Increased user adoption
4. Increased speed of deployment

B. PAAS (Platform as a Service)

PaaS enables companies to develop submission more swiftly and efficiently in a cloud background using programming languages and tools supported by the contributor. The significant factor that makes PaaS unique is that it lets developers assemble and deploy web applications on a hosted communications. All centralized system requires new/different protection measures. Common examples of platforms consist of, Linux, Windows™ and Apple Mac OS X for operating systems;, Windows Mobile, Google Android and Apple iOS for mobile computing and Microsoft .NET Framework or Adobe AIR the for software frameworks.

C. IAAS (Infrastructure as a Service)

This is the bottom layer of the cloud stack. It serves as a foundation for the other two layers, for their implementation. The keyword at the back this stack is virtualization. Usually platform-independent, infrastructure expenses are shared and thus abridged, service level agreements (SLAs), self-scaling, pay by usage. Keep away from capital expenditure on hardware and human resources, reduced ROI risk; low barricade to entry, streamlined and automated scaling but shortcoming are business competence and productivity mainly depends on the merchant capabilities, potentially larger long-term cost, centralization have need of new/different defence measures. With, a corporation can rent essential computing resources for deploying and storing data or running applications. IaaS enables express deployment of applications and get better the quickness of IT services by instantly adding computing processing command and storage capacity when necessary.

IV. CLOUD SECURITY CHALLENGES

Cloud Computing, an emergence technology, has placed many challenges in different aspects. Some of these are shown in the following diagram:

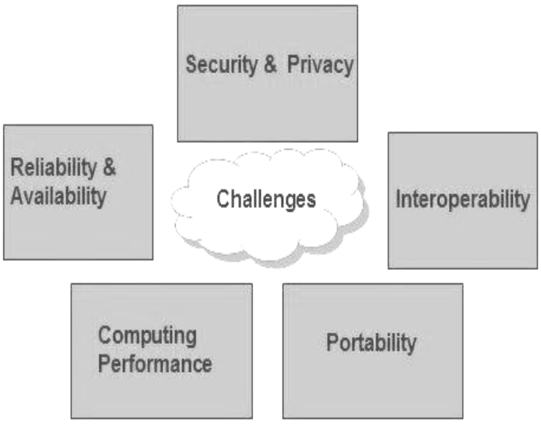


Fig. 4.1 Security Challenges In Cloud

A. Security & Privacy

Security and privacy of information is the major challenge to cloud computing. Security and privacy issues can be defeated by employing security applications, security hardware and encryption.

B. Portability

This is an additional challenge to cloud computing that applications have to easily be migrated from one cloud provider to another. There should not be merchant lock-in. However, it is not yet made promising because each of the cloud providers uses diverse standard languages for their platforms.

C. Interoperability

Applications on one platform have to be able to incorporate services from other platform. It is made possible via web services. Other than writing such web services is very complex.

D. Computing Performance

To carry data intensive applications on cloud have need of high network bandwidth, which results in high price. If done at low bandwidth, then it does not get together the required computing performance of cloud application.

E. Reliability and Availability

It is essential for cloud systems to be consistent and robust because mainly of the businesses are now becoming dependent relative on services provided by third-party.

F. Authentication

Cloud service providers ask for customers to store their account information in the cloud, Cloud service providers have the right of entry to this information. This presents a privacy issue to the customer's privacy information. Many SLAs have specified the privacy of the susceptible information; however, it is not easy for customers to make sure the correct rules are enforced. There is being short of of transparency in the cloud that permits the customers to monitor their own seclusion information. When a customer decide to use multiple cloud service, the customer will have to store his/her password in multiple cloud, the more cloud service the customer is subscript to, the more copy of the user's information will be. This is a safety issue for the customers and the cloud service providers. The numerous copies of account will lead to several authentication processes. Cloud service providers use diverse authentication technologies for authenticating users, this might have less impact on SaaS than PaaS and IaaS, but it is current challenge to the customers.

G. Confidentiality

Confidentiality refers to only authorized parties or systems having the capacity to right of entry protected data. The threat of data negotiation increases in the cloud, due to the increased amount of devices, parties and applications involved, that leads to an enlarge in the number of points of admission. Delegating data manage to the cloud, the wrong way round leads to an increase in the risk of data compromise, as the data becomes easy to get to to an augmented number of parties.

H. Integrity

A key feature of information security is integrity. Integrity means that assets can be customized only by authorized parties or in authorized ways and refers to data, software and the hardware. A cloud computing contributor is trusted to preserve data integrity and accuracy. The cloud model presents a number of threats counting sophisticated insider attacks on these data aspects. Software Integrity refers to defending software from unauthorized modification, deletion, theft or fabrication. Deletion, fabrication or modification can be intentional or unintentional.

I. Availability

Availability refers to the property of a system being easy to get to and usable upon insist by an authorized entity. System availability comprises a systems ability to carry on operations even when some authorities behave badly. To guarantee that information and information processing is offered to clients upon demand. The security objectives within a distributed system are essentially.

V. TRUSTED THIRD PARTY

We declare that employing Trusted Third Party services within the cloud, leads to the establishment of the essential Trust level and provides ideal solutions to protect the confidentiality, authenticity and integrity of data and communications. This infrastructure lever ages a system of digital certificate distribution and a mechanism for associating these certificates with known origin and target sites at every participating server. TTP services are provided and underwritten not only by technical, but also by legal, financial, and structural means.

The trusted third party can be relied upon for:

1. Certificate-Based Authorization.
2. Creation of Security Domains.
3. Server and Client Authentication.
4. Cryptographic Separation of Data.
5. Low and High level confidentiality.

VI. CROSS-CERTIFICATION

Cross-certification extends third-party trust relationships between Certification Authority domains. For example, two trading partners, each with their own CA, may want to validate certificates issued by the other partner's CA. Alternatively, a large, distributed organization may require multiple CAs in various geographic regions. Cross-certification allows different CA domains to establish and maintain trustworthy electronic relationships. The term cross-certification refers to two operations. The first operation, which is generally executed infrequently, is the establishment of a trust relationship between two CAs. In the case of bilateral cross-certification, two CAs securely exchange their verification keys. These are the keys used to verify the CAs' signatures on certificates. To complete the operation, each CA signs the other CA’s verification key in a certificate referred to as a “cross-certificate”. The second operation is done by the client-side software. The operation, which is executed frequently, involves verifying the trustworthiness of a user certificate signed by a cross-certified CA. The operation is often referred to as “walking a chain of trust”. The “chain” refers to a list of cross-certificate validations that are “walked” (or traced) from the CA key of the verifying user to the CA key required to validate the other user’s certificate.When walking a chain of cross-certificates, each cross-certificate be checked to ensure that it is still trusted. User certificates must be able to be revoked; so must cross-certificates. This requirement is frequently overlooked in discussions regarding cross-certification.

VII. 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.).

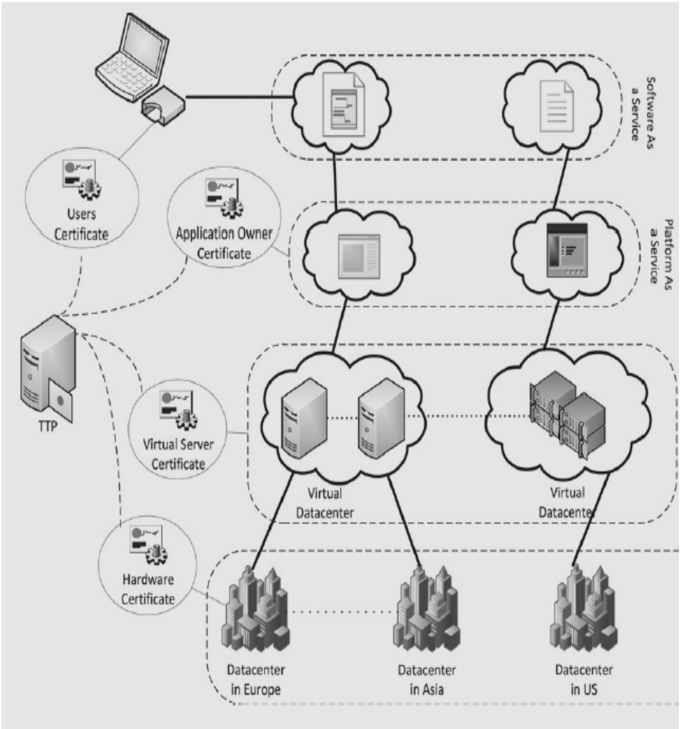


Fig.7.1 Certificate Moving Through Different Layer in Cloud Environment

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:

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

A. Implementation of OSSEC in Cloud

OSSEC is an open source host-based intrusion detection system (HIDS). OSSEC is ascalable, multi-platform, open source,Host basedIntrusion Detection System (HIDS). Ithas a powerful association and analysis mechanism,integrating log analysis; file veracitychecking, centralized policy enforcement, Windows registry monitoring, root kit detection, active responseand real-time alerting. Itruns on most operating systems, includingOpenBSDLinux, MacOS, FreeBSD,Solarisand 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.

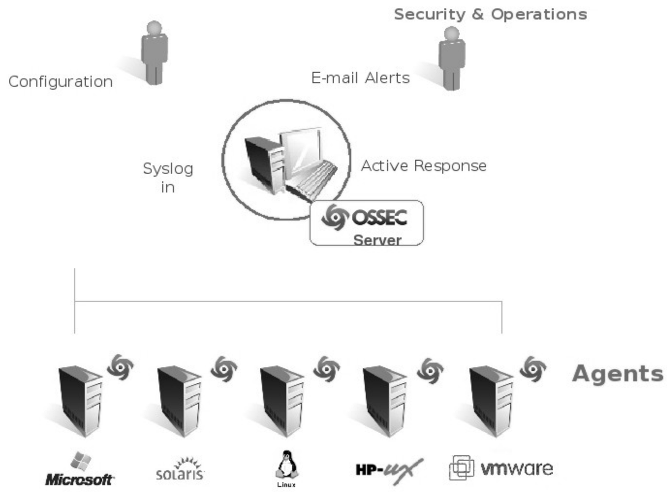


Fig.7.2 Architecture of OSSEC

We are using OSSEC HIDS because it not only does all theanalysis we mention in here, but also has rulesfor multiple log formats, making our correlationsimpler. There are two models for OSSEC implementation.
1. Local (when you have just one system to monitor).
2. Client/Server for centralized analysis.

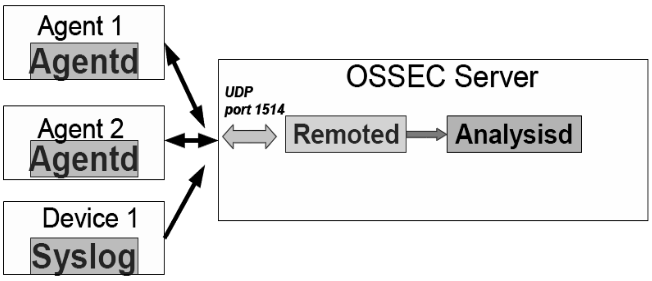


Fig 7.3 Agent/Server Network Communication

Focus now on the main process (**ossec-analysisd**)
1. It does the log decoding and analysis
2.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:
1. Understand your logs. Know what is good and what is bad.
2. Correlate the bad events looking for patterns that may indicate an attack or intrusion.
3. Correlate the good events with the bad events (eg. multiple failed logins followed by a successful one).
4. Correlate the good events (eg. too many successful logins for the same user across multiple hostsin a small period of time).
5. Look for unusual patterns that are not in your good or bad list.

VIII. CONCLUSION

This thesis provides insight in different aspects of information security. The thesis thoroughly analysed the security risks related to content management systems. It analyses different security threats and their potential impact on an information system in the cloud. The risk to an information system is a function of the probability of threat occurrence and its potential impact. The risks exposed to the information system can be mitigated by a strong authentication mechanism. 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]. UpenNathwani, Irvin Dua, VedVyasDwivedi, '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, AshwinSelokar&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]. PuyaGhazizadeh, 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]. Mohammed A. AlZain& Ben Soh and Eric Pardede, 2013, "A New Approach Using Redundancy Technique to Improve Security in Cloud Computing", pp. 230-235.

[6]. GurudattKulkarni ,JayantGambhirGurudattKulkarni , JayantGambhir, TejswiniPatil&AmrutaDongare, 2012, "A Security Aspects in Cloud Computing", Journal of Engineering Science and Technology (IJEST), pp.447-450.

[7]. D. Sureshraj& Dr. V. MuraliBhaskaran, 2012, "Automatic Dna Sequence Generation For Secured Cost-Effective Multi -Cloud Storage", Ieee.

[8]. 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.

[9]. 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.

[10]. Zhongbin Tang, Xiaoling Wang, Li Jia, Xin Zhang, Wenhui Man, 2012, "Study on Data Security of Cloud Computing", 978-1-4577-1964-6/12.

[11]. 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.

[12]. SubaSurianarayanan& 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.

[13]. 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

[14]. Parikshit Prasad, BadrinathOjha, Rajeev Ranjanshahi&AbhishekVaish, 2011, "3 Dimensional Security in Cloud Computing", 978-1-61284-840-2/11, pp. 198-201

[15]. Amir Mohamed Talib, RodziahAtan, Rusli Abdullah &MasrahAzrifah, 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

[16]. Uma Somani, KanikaLakhani, 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

[17]. 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

[18]. 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.

[19]. Basant Narayan Singh," Cloud Service Models - SaaSPaaSIaaS - Which One is for You?", posted Tuesday, June 28, 2011.

[20]. 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.

[21]. B. Hay, K.L. Nance and M. Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing", in Proceedings of HICSS, PP 1-7, 2011

[22]. OSSEC Homepage - www.ossec.net

Mrs.Shikha Nema is a student of Takshshila Institute of Engineering &Technology, Jabalpur (M.P.) India. Presently she ispursuing herM.Tech [CSE] from this college and she received her B.E degreefrom TIETECH, affiliated toRGTU University, Bhopal, in the year 2004. 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 CSEDepartment, 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.