ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

Emerging Security Issues and Challenges in Cloud Computing

S C Rachana[1], Dr. H S Guruprasad[2]

***Abstract*— Cloud computing is an Internet-based computing solution which provides the resources in an effective manner. A very serious issue in cloud computing is security which is a major obstacle for the adoption of cloud. The most important threats of cloud computing are identified and understood in this survey. This paper covers the information about the threats such as- Multitenancy, Availability, Loss of control, Loss of Data, outside attacks, DOS attacks, malicious insiders, etc. The solutions to overcome some of these threats have also been highlighted in this paper.**

***Index Terms*— Cloud Computing, Security Issues.**

I. INTRODUCTION

Cloud computing delivers the software (IT) as a service. In the cloud, many computers are configured to work together where the resources are allocated on demand. Cloud computing allows the customers to access resources through the internet from anywhere at any time without thinking about the management and maintenance issues of the resources. Resources of cloud computing can be provided dynamically. One of the important attribute of cloud computing is scalability which can be achieved through server virtualization. The best example of Cloud computing is Google Apps. The services can be accessed using Google Apps through the browser over the Internet. Cloud computing is cheaper than any other computing models. In cloud, the maintenance cost is zero as the clients are free from maintenance and management issues. Thus, cloud computing is also called 'Utility Computing' or 'IT on demand'.

Cloud Deployment Models: There are three types of cloud deployment models. They are private, public, and hybrid.

Public clouds: These type of the cloud models are owned by an organization who sells the cloud services. A public cloud provides the resources dynamically over the Internet using web applications.

Private clouds: They are available within the company and are managed by the organization. An individual can create this type of cloud and an organization is responsible for setting up, controlling and maintaining of this cloud.

Hybrid clouds: This type of cloud is a combination of the public and the private cloud and it uses the services that are available in both the public and private space. Management of the cloud is done by both public and private cloud providers.

Delivery Models: There are three types of cloud delivery models.

Software as a Service (SaaS): In SaaS software's which are available on the cloud server are provided as a services to the consumers according to their requirement.

Platform as a Service (PaaS): PaaS allows platform access for clients so that they can put their own software's and applications on to the cloud.

Infrastructure as a Service (IaaS): IaaS provides customers with the resources such as rent processing, storage, network capacity, and other basic computing resources. Also allows consumers to manage the operating systems, applications, storage, and network connectivity.

Security Issues in the Cloud

Security issues in cloud is a major obstacle for its adoption Security issues can be grouped into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. There are many other challenges and risks in cloud computing that leads to loss of security which has to be taken care in order to build trust in customers about cloud computing technology.

Akhil Behl et. al. [1] describe very common and critical security challenges. There are many security threats which comes from inside or outside of cloud provider's/consumer's environment which author has classified into insider

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

threats, outsider malicious attacks, data loss, issues related to multi-tenancy, loss of control, service disruption. The security feature in a cloud environment has to be adopted to protect cloud virtual infrastructure. Availability and Performance, outside attacks, Malicious Insiders, Multitenancy, Loss of Control, and Service Disruptions are the kind of attacks which has to be mainly addressed. Farazi Sabhai et. al. [2] describes the well-known Gartner's seven security issues. The basic security issues such as Data leakage, DoS (Denial of Service) attacks are addressed. Some of the solutions for cloud security such as Access Control, Incident Counter measure and Response are proposed. Zhidong et. al. [6] address the cloud computing security challenges by proposing a solution called the Trusted Computing Platform (TCP). TCP is used to provide authentication, confidentiality and integrity in cloud computing environment. Trusted cloud computing system is built using TCP as the hardware for cloud computing and it ensures privacy and trust. The modules included in the proposed model are Authentication, Role Based Access Control, Data Security, Tracing of User's behavior. Cloud computing deployment and service models, security issues and challenges are introduced in [8]. Gartner's Seven Security Issues of cloud computing such as privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, long term viability are explained. Cloud computing challenges such as security, costing model, charging models, Service Level Agreements[SLA's], what to migrate to cloud, cloud interoperability issues are also described. A survey is performed in [9] about the market to understand continuous innovation, academic and industry research efforts and cloud computing challenges. Gartner's seven security issues are also described. Security measures such as Centralized data, Incident response, Password Assurance Testing, Secure software improvement are explained. Surianarayanan et. al. [15] describes cloud computing security issues. The focus is on providing security mechanisms at four levels such as Network, System, Virtual Machine, and Application. Cloud security policies and procedures are classified into three categories such as Pre-migration, In-operation, Termination. Many security control mechanisms are mentioned for security issues at these four levels. The security issues related to policies, software and hardware are described in [16]. Policies between Cloud Service Provider and Cloud Customer which ensures security must include factors that need to be considered during breach of security such as Insider threats, Access control, System Portability. Security is classified into Software Security such as virtualization software, encryption, host operating system and Physical security such as back-up, firewall, server location and these two types has to be addressed to provide secure cloud. The existing challenges and issues in cloud computing are analyzed and addressed in [17]. Multi-tenancy approaches are used to provide security. Cloud computing dependencies between the model layers are explained. In this model, functionality and security of a higher layer depends on lower ones. This dependency complicates cloud security problem. Other security measures of cloud are Identity and Access Management, Security Management, Key Management, Secure Software Development Lifecycle, Security Performance and Optimization.

Cloud computing concepts and its challenges are introduced in [5]. The most important security issues in cloud such as Data Privacy and Service Availability are explained briefly. Existing cloud computing systems such as Google, IBM and Amazon are explained. Amani et. al. [10] explain the security problems of cloud platform virtualization infrastructure. The existing security threats of Virtual infrastructure are mentioned by describing a threat model in which a hacker can be either cloud user or non-cloud user. Security attacks of Virtual infrastructure involve attacks such as hypervisor attacks, vSwitch attacks, Virtual machine attacks. A virtualization-aware security solution is proposed in which the security software is installed in a dedicated and privileged Virtual machine with privileged access to hypervisors to secure other Virtual machines. It is advised to use micro-hypervisor with microkernel to provide high level security. Cloud security risks and vulnerabilities are explained in [12]. Vulnerability characteristic which are essential for cloud such as unauthorized access to management interface, Internet protocol vulnerabilities, data recovery vulnerability, metering and billing evasion, identity, authentication, authorization, auditing mechanisms are described. Security control mechanisms are addressed against the risks. Cloud software infrastructure and environment vulnerabilities are mentioned. The main focus of [13] is on Virtualization and SOA technologies in cloud computing. Seven principles of Open Architecture Of Cloud Computing such as Integrated Ecosystem Management for cloud, Virtualization for Cloud infrastructure, Service-Orientation for common, Extensible Provisioning and Subscription for cloud, Configurable Enablement for cloud offerings, Unified Information Representation and Exchange framework, Cloud Quality and Governance are described. Cloud Computing issues such as Security, Privacy, Reliability, Legal Issues, Open standard, Compliance, Freedom, Long-term Viability are addressed and solutions for these issues are proposed.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

A new secure framework for cloud computing is proposed in [3] which consists of many machines and the software layer. The software layer is called as Hadoop layer and its responsibility is to distribute application data across machine and manage the application execution across the machines parallely. The hadoop layer is also responsible to detect and recover from machine failures. Authentication procedure is added into this framework which uses hashing techniques for user authentication. The basic cloud computing concepts such as cloud computing model, service models, deployment models and its characteristics are described in [4]. A data security model is proposed and it uses an encryption algorithm in Amazon EC2 Micro platform to provide security. An encryption algorithm which recovers fast from failures is selected by comparing with few other encryption algorithms based on P-value and rejection rate. It is advised to use AES (Advanced Encryption Standard) for higher security requirements. The Cloud storage and its security are explained in [11]. Architecture for Cloud storage is proposed which consists of four layers such as storage, basis of management, application interface and access layers. Storage safety design model is proposed to secure cloud storage and this design achieves storage encryption, backup encryption, and exchange of encryption. The cloud computing concepts and security issues are introduced briefly in [14]. Literature review on few papers is also included. The most common attacks such as tampering, dropping, replay attack, identity spoofing etc. is described. Technologies for securing data such as Mirage Image Management Systems, Client-Based Privacy Manager, Transparent Cloud Protection System, Secure and Efficient Access to Outsourced Data are mentioned. In [21], Security Audit as a Service (SAaaS) architecture is proposed which is a cloud audit system and its aim is to increase trust in cloud infrastructures by hiding details of what is happening in cloud from user and cloud provider. Whenever an infrastructure change takes place this architecture shows how autonomous agents detect the change, automatically recalculate the security status of the cloud and inform the user through an audit report about the change. Two use cases are considered for cloud audits and a high level overview of how events are generated, preprocessed, combined and forwarded within the SAaaS architecture is described. The overview is divided into three logical layers such as Input, Processing and Presentation layer. Tomohisa et. al. [24] proposes FBCrypt as a solution for avoiding information leakage through the management VM in out-of-band remote management. The FBCrypt encrypts the inputs and outputs between a VNC client and a user VM using the VMM (Virtual Machine Monitor). The VMM decrypts the inputs encrypted by a VNC client when a user VM reads them. Whenever a user VM updates a frame buffer, the VMM encrypts the updated pixel data, which are decrypted by a VNC client. Thus the sensitive information is located in the middle which is protected against the management VM.

In [25], a CLOUDWATCHER is used to provide monitoring services for large and dynamic clouds. The Cloud Watcher automatically detects the network packets which needs be inspected by using the pre-installed network security devices. A simple policy script is used for these operations and thus a cloud network administrator is able to protect his cloud network easily. A cloud operator can monitor the cloud easily and efficiently with CLOUDWATCHER and it provides security monitoring as a service to all its tenants. CLOUDWATCHER provide practical and feasible network security monitoring in a cloud network. Francisco et. al. [26], present a sophisticated attack which involves compromising of sensitive information in the memory area of a particular process which is executing in a virtual machine. A solution is presented for securing the inter-VM communication and another protection mechanism is proposed for malicious insider threat. Architecture is proposed for cloud servers which architecture involves the trusted computing base. Michael et. al. [27] proposes a technique to prevent cache-based side-channels. This technique is implemented within the server of a Cloud system and it is done so that there is no interference with the Cloud's methods of operation. The solution addresses cache-based side channels in the Cloud and it does not interfere with the Cloud model which requires no changes to the client-side code, or to the underlying hardware. In [29], IDM (Identity management) approach is proposed which has the ability to use identity data on untrusted hosts. This approach uses the predicates over encrypted data and multi-party computing for the use of a cloud service. It uses active middleware agent that includes privacy policies, a virtual machine that enforces the policies, and has a set of protection mechanisms to protect itself. An active agent interacts in the place of a user to authenticate to cloud services using user's privacy policies. The security issues associated with the virtual machine (VM) migration from one cloud platform to the other in an Infrastructure-as-a-Service (IaaS) cloud service model is a factor of consideration in [30]. A protocol called "Trust_Token" is proposed which guarantees that the user VM can only be migrated to a cloud platform which is trustable. In the proposed protocol, the cloud user can define the migration policy and the user can later audit the VM migration process which is performed by the cloud provider. The Trust_Token used for the migration ensures that the user VM is never migrated to an untrusted platform.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

In [7], homomorphic encryption is used to secure the cloud. The working of homomorphic encryption is explained and Gentry's fully homomorphic encryption is achieved. Since, homomorphic encryption requires more time and computational resources, Searchable Symmetric Encryption is used. In Searchable Symmetric Encryption, an encryption layer is proposed on top of the encrypted files which are to be stored on cloud. Lifei et. al. [18] addresses the issues such as security and privacy and system architecture is designed to overcome these issues. The architecture includes the models such as Storage-cheating model, Computation-cheating model, and Privacy-cheating model. Merkle hash tree is an authentication tree structure which is constructed as a binary tree. Each leaf in this tree is a hash value of authenticated data values which is often used to ensure the authenticity and integrity. The cloud computation auditing protocol is used which is based on Merkle hash tree based commitment. Huan et. al. [19] describes the three environments to explain how the cloud affects the security. The three different environments include tools that exist on the same lab where the targets are, tools that are not on the same lab but on the same campus, and tools that exists off-campus. A method called SVA (Security Vulnerability Assessment) process is used which is a risk-based and performance-based method which involves five steps such as Apply SVA Tools, Assessment Report, Vulnerability Analysis, Risk Assessment, Counter measures Analysis. Udaya et. al. [20] analyze the security issues related to TVD and propose few security measures to deal with the attacks in TVD. The techniques for the deploying the TVD on Xen virtual machine monitor is discussed and the attacks on the TVD virtual machines are explained. Few techniques to assure security in TVD are proposed. TVDSEC is a technique uses different components to deal with the attacks in the TVD-LAN. Trust enhanced security architecture for cloud is proposed in [22]. An attacker model for the cloud is described and some of the challenges with the current TPM based attestation techniques are explained. An attestation based technique is used to address the challenges with the current attestation techniques and this technique effectively deals with the attacks in the cloud. In [23], Host Identity Protocol (HIP) is a proposed solution which provides a way to authenticate and protect data flows between tenants belonging to the same security domain. HIP is experimented under different conditions to address the multi-tenancy challenges for public and hybrid IaaS clouds. In this solution, developers and administrators can access cloud services directly over HIP, whereas consumers access the cloud without HIP using a reverse HTTP proxy which also acts as a load balancer for a distributed test service. HIP was used to secure internal connectivity in the clouds and a load balancer terminated HIP tunnels towards end-users. A "live migration defense framework" (LMDF) is developed in [28], which can be used for incorporating security policy within a VM. It is shown that with the LMDF two times more integrity checks can be performed, nearly three times more data can be encrypted and the VM is relocated. The LMDF can estimate the distance between the old and the new location and perform internal adaptations and corresponding actions based on the location fingerprint training.

II. CONCLUSION

This paper surveys the emerging challenges, threats and concerns in cloud computing security. Various cloud computing security and problems and possible strategies are focused. The cloud computing security frameworks and the technology support are also discussed.

ACKNOWLEDGMENT

The authors would like to acknowledge and thank Technical Education Quality Improvement Program [TEQIP] Phase 2, BMS College of Engineering and SPFU [State Project Facilitation Unit], Karnataka for supporting the research work.

REFERENCES

[1] Akhil Bhel, "Emerging Security Challenges in Cloud Computing", Information and Communication Technologies, 2011 World Congress on, Mumbai, 11th - 14th Dec 2011, pp 217 - 222, Print ISBN: 978-1-4673-0127-5, DOI: 10.1109/WICT.2011.6141247.

[2] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE 3rd International Conference on Communication software and Networks(ICCSN), 27-29 May 2011, pp 245-249, Print ISBN: 978-1-61284-485-5, DOI: 10.1109/ICCSN.2011.6014715.

[3] K.Mukherjee, G.Sahoo, "A Secure Cloud Computing", International Conference on Recent Trends in Information, Telecommunication and Computing, Mar 12th 2010, Washington DC, pp 369-371, ISBN: 978-0-7695-3975-1, DOI: 10.1109/ITC.2010.95.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

[4] Eman M.Mohamed, Hatem S Abdelkader, Sherif EI-Etriby, "Enhanced Data Security Model for Cloud Computing", 8th International Conference on Informatics and Systems(INFOS), Cairo, 14-16 May 2012, pp 12-17, Print ISBN: 978-1-4673-0828-1.

[5] Wentao Liu, "Research on Cloud Computing Security Problem and Strategy", 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 21-23 April 2012, pp 1216-1219, Print ISBN: 978-1-4577-1414-6, DOI: 10.1109/CECNet.2012. 6202020.

[6] Zhidong Shen, Qiang Tong " The Security of Cloud Computing System enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems, Dalian, (ICSPS), 5-7 July 2010, Vol 2, pp 11-15, Print ISBN: 978-1-4244-6892-8, DOI: 10.1109/ICSPS.2010.5555234.

[7] Aderemi A Atayero, Oluwaseyi Feyisetan, "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", Journal of Emerging Trends in Computing and Information Sciences, 1st Oct 2011, Volume 2, Issue 10, pp 546-552, ISSN: 2079-8407.

[8] Kuyoro S. O., Ibikunle F. & Awodele O., "Cloud Computing Security Issues and Challenges", 24-28 May 2010, pp 344-349, print ISBN: 978-1-4244-7763-0.

[9] Traian Andrei, "Cloud Computing Challenges and Related Security Issues", May 2012.

[10] Amani S. Ibrahim, James Hamlyn-Harris and John Grundy, "Emerging Security Challenges of Cloud Virtual Infrastructure", 17th Asia-Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop, 30 November-03 December 2010.

[11] Youchan Zhu, Yaduan Wang, "A safety design of cloud storage", Computational and informational sciences(ICCSIS), International Conference, 17-19 Aug. 2012, pp 1054-1057, print ISBN: 978-1-4673-2406-9, DOI: 10.1109/ICCIS.2012.41.

[12] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker "Understanding Cloud Computing Vulnerabilities", IEEE Journal of Security and Privacy, Vol 9, Issue 2, March 2011, pp 50-57, ISSN: 1540-7993, DOI: 10.1109/MSP .2010.115.

[13] Ashutosh Kumar Singh, Dr. Ramapati Mishra, Fuzail Ahmad, Raj Kumar Sagar, Anil Kumar Chaudhary, "A Review of Cloud Computing Open Architecture and Its Security Issues", International Journal Of Scientific & Technology Research, Issue 6, Vol 7, july 2012, pp 65-67, ISSN: 2277-8616.

[14] Ayesha Malik, Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review", CIS Journal, Vol. 3, March 2012, ISSN: 2079-8407.

[15] Suba Surianarayanan, T.Santhanam, "Security Issues and Control Mechanisms in Cloud", International Conference, 2012, pp 74-76, ISBN: 97 8-1-4673-4416-6 /12.

[16] Eystein Mathisen, "Security Challenges and Solutions in Cloud Computing", International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 31 May -3 June 2011, Daejeon, Korea, pp 208-212, ISBN: 978-1-4577-0872-5.

[17] Anas BOUA Y AD, Asmae BLILA T, Nour el houda MEJHED, Mohammed EL GHAZI, "Cloud computing : security challenges", Information Science and Technology(CIST) 2012 Colloquim, Fez, 22-24 Oct. 2012, pp 26 - 31, print ISBN: 978-1-4673-2726-8, DOI: 10.1109/CIST.2012.6388058.

[18] Lifei Wei, Haojin Zhu, Zhenfu Cao, Weiwei Jia, Athanasios V. Vasilakos, "SecCloud: Bridging Secure Storage and Computation in Cloud", IEEE Distributed Computing Systems Workshops (ICDCSW), Genova, 21-25 June 2010, pp 52 - 61, ISSN: 1545-0678, Print ISBN: 978-1-4244-7471-4, DOI: 10.1109/ICDCSW .2010.36

[19] Huan-Chung Li, Po-Huei Liang, Jiann-Min Yang, Shiang-Jiun Chen, "Analysis on Cloud-Based Security Vulnerability Assessment", e-Business Engineering (ICEBE), 2010 IEEE 7th International Conference, Shanghai, 10-12 Nov. 2010, pp 490 – 494, Print ISBN: 978-1-4244-8386-0, DOI: 10.1109/ICEBE.2010.77.

[20] Udaya Tupakula Vijay Varadharajan, "TVDSEC: Trusted Virtual Domain Security", Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference, Victoria, NSW, 5-8 Dec. 2011, pp 57 – 64, Print ISBN: 978-1-4577-2116-8, DOI: 10.1109/UCC.2011.18.

[21] Frank Doelitzscher∗, Christian Fischer∗, Denis Moskal∗, Christoph Reich∗, Martin Knahl∗ and Nathan Clarke, "Validating Cloud Infrastructure Changes By Cloud Audits", Services (SERVICES), 2012 IEEE Eighth World Congress, Honolulu, HI, 24-29 June 2012, pp 377 - 384, Print ISBN: 978-1-4673-3053-4, DOI: 10.1109/ SERVICES.2012.12.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

[22] Vijay Varadharajan Udaya Tupakula, "TREASURE: Trust Enhanced Security for Cloud Environments", Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference, Liverpool, 25-27 June 2012, pp 145 – 152, Print ISBN: 978-1-4673-2172-3, DOI : 10.1109/TrustCom.2012.283.

[23] Miika Komu, Mohit Sethi, Ramasivakarthik Mallavarapu, Heikki Oirola and Rasib Khan, Sasu Tarkoma "Secure Networking for Virtual Machines in the Cloud", Cluster Computing Workshops (CLUSTER WORKSHOPS), IEEE International Conference, Beijing, 24-28 Sept. 2012, pp 88 – 96, Print ISBN: 978-1-4673-2893-7, DOI: 10.1109/ClusterW.2012.29.

[24] Tomohisa Egawa, Naoki Nishimura, Kenichi Kourai "Dependable and Secure Remote Management in IaaS Clouds", IEEE International Conference on Cloud Computing Technology and Science, ISSN: 978-1-4673-4510-1.

[25] Seungwon Shin, Guofei Gu," CloudWatcher: Network Security Monitoring Using OpenFlow in Dynamic Cloud Networks", Network Protocols (ICNP), 2012 20th IEEE International Conference, Austin, TX, Oct. 30 2012-Nov. 2 2012, pp 1-6, Print ISBN: 978-1-4673-2445-8, DOI: 10.1109/ICNP.2012.6459946.

[26] Francisco Rocha, Thomas Gross, Aad van Moorsel, "Defense-in-depth Against Malicious Insiders in the Cloud", IEEE International Conference on Cloud Engineering, pp 88-97, ISSN: 978-0-7695-4945-3, DOI: 10.1109/IC2E.2013.20.

[27] Michael Godfrey & Mohammad Zulkernine, "A Server-Side Solution to Cache-Based Side-Channel Attacks in the Cloud", IEEE Sixth International Conference on Cloud Computing, Washington, DC, USA, pp 163-170, ISBN: 978-0-7695-5028-2, DOI: 10.1109/CLOUD .2013. 21.

[28] Sebastian Biedermann, Martin Zittel and Stefan Katzenbeisser, "Improving Security of Virtual Machines during Live Migrations", Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference, Tarragona, 10-12 July 2013, pp 352 - 357, DOI: 10.1109/PST.2013.6596088.

[29] Rohit Ranchal, Bharat Bhargava, Lotfi Ben Othmane, Leszek Lilien, Anya Kim, Myong Kang, Mark Linderman, "Protection of Identity Information in Cloud Computing without Trusted Third Party", Reliable Distributed Systems, 2010 29th IEEE Symposium, New Delhi, Oct. 31 2010-Nov. 3 2010, pp 368 – 372, ISSN : 1060-9857, Print ISBN: 978-0-7695-4250-8, DOI: 10.1109/SRDS.2010.57.

[30] Mudassar Aslam, Christian Gehrmann, Mats Bj¨orkman, "Security and Trust Preserving VM Migrations in Public Clouds", Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference, Liverpool, 25-27 June 2012, pp 869 - 876, Print ISBN: 978-1-4673-2172-3, DOI: 10.1109 /TrustCom.2012.256.

AUTHOR BIOGRAPHY

Ms. S C Rachana is a PG Scholar in Computer Networks and Engineering at B.M.S College Of Engineering, Bangalore. My research areas are Cloud Computing and Its security, Computer network.

Dr. H S Guruprasad is working as Professor and Head, Information Science Department at BMS College of Engineering, Bangalore. He has twenty four years of teaching experience. He has been awarded with Rashtriya Gaurav award in 2012. His research areas are Network Communications, algorithms, Cloud Computing and Sensor Networks.