SECURITY APPREHENSIONS IN DIFFERENT REGIONS OF CLOUD CAPTIOUS GROUNDS

Gurdev Singh[1] Amit Sharma[2] Manpreet Singh Lehal[3]

[1]Department of Computer Science and Engineering, Eternal University,
Baru Sahib, Sirmour, HP (India)
singh.gndu@gmail.com
[2]Department of Computer Science and Engineering, Eternal University,
Baru Sahib, Sirmour, HP (India)
amitsh2701@gmail.com
[3]Department of Computer Science and Engineering, Lyallpur Khalsa College,
Jalandhar, Punjab (India)
lkcmanpreet@hotmail.com

ABSTRACT

Cloud computing is a new innovative model for enterprise in which information is permanently stored on the servers and also manage how and when different resources are allocate to the requested users. It provides distributed approach through which resources are allocated dynamically to the users without investing in the infrastructure or licensing the software's on the client side. Using the cloud makes processing of information is more commodious but it also present them with new security problems about reliability.This phenomenon introduces serious problems regarding access mechanism to any information stored in the database and resources in the cloud. For the successful implementation of cloud computing it is necessary that we must know different areas where the security is needed. For this there should also governess strategy needed for secure communication between multi-clouds located in different geographical areas or in different countries. In this paper we discuss how to safely utilizing the benefit of cloud computing through the network where data security, provide authentication, integration, recovery, IP spoofing and Virtual Servers are the most captiousfields in the cloud.

KEYWORDS

Cloud Computing, Data Security, Secure Servers, Secure Network.

1. INTRODUCTION

Cloud computing is on demand model that covers virtualization concept used in physical servers. It offers an innovative model for enterprise to dynamically emerging applications and delivers a large pool of scalable resources to users [2], [16]**.**Clouds are a large pool of easily accessible and usable virtualized resources (such as development platforms, hardware, and/or services)[14].Cloud computing provides the next generation of internet-based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. It is a natural evolution of the widespread adoption of virtualization, service-oriented architecture, autonomic and utility computing. Details are abstracted from end-users, who no longer have need for expertise in, or control over, the technology infrastructure in the cloud that supports them.

In a cloud computing system, there is a significant workload shift. Normal systems no longer have to do all the heavy lifting when it comes to running applications. Using the Cloud Computing model hardware and software demands on the user's side decrease. There is only

need a cloud computing software which provide mediation layer or interface software, that is Web browser to access the cloud.

Cloud has centralized server administration system. Centralized server administers the system, balances the load between clients according to demands, monitors traffic and avoids congestion. Servers in the cloud use protocols called middleware that controls the communication of cloud network among them. With cloud computing different types of users can access different resources and applications via the internet from anywhere. For the successful implementation of cloud computing in the organization require proper planning and understanding the threats, vulnerabilities and security. In cloud computing we can share different resources and applications via the network in open environment, thus it makes security problems for us to develop the secure cloud [12]. Security problems become more complicated in cloud computing when we entered into the environment such as multi-tenancy, secure distributes environment, data security, server virtualization and provide authentication[7].

"Multi-tenancy" is for the benefit of the service provider so they can manage the resource utilization more efficiently [18]**.** Multi-tenancy implies sharing of computational resources, storage, services, and applications with other tenants.Unlike previous computing models, that uses dedicated resources to dedicated user, cloud computing is based on a business model in which resources are shared at the network, host and application level. To provide security in multi-tenancy there should be isolation among tenants' data to avoid attacks that attempt to co-locate with the victim assets.

Our main goal is to maintaining security without any loss of information. So we can achieve this, when any user sends request to server then user has to first register himself and after that login with its username and password that was provided to him. The security is provided when data is accessed in isolation, identify the user activities, provide secure mechanism to access server, some mechanism to track the forged IP and provide some laws for the successful implementation of the cloud.

2. DATA SECURITY IN THE CLOUD

Organizations are aware about the importance of securing their information systems to guarantee basic security requirements,i.e.Confidentiality and Availability [15]. The enterprise/personal that adopts the service of cloud computing, firstly the necessary condition is that both of the server and database on the front end must be trusted has to be satisfied [1]. With the increasing popularity of enterprise cloud computing and its public connectivity via the internet it is thenext frontier for viruses, worms, hackers and cyber-terrorists to start probing and attacking [8].

Software as a Service located on the top layer, cloud storage is always an important key factor for implement the application of cloud computing. Especially, the storage resource of the Infrastructure as a Service on the bottom layer is the most important factor for supporting the regular operation of networking service. This proposal gives more tractability to access data through web based application that provide interface to users in anytime at anywhere through network. While accessing these features in the cloud the main thing is security when accessing data online. However, data security on the cloud side is not only focused on the process of data transmission, but also the system security and data protection for those data stored on the storages of the cloud side [1]. In the following, some consideration regarding the security issues are to be focused.

2.1 Storage and system protection

Database can be defined as the capability of a system to provide reliable service even if any attack takes place. Security in the storage database is the concurrent existence of:

2.1.1 Availability

The cloud provider might, additionally, replicate the data at multiple locations across countries for the purposes of maintaining high availability [3]. The use of high availability is closely related with disaster recovery.Availability refers to the property of a system being accessible and usable upon demand by an authorized entity. Availability refers to data, software but also hardware being available to authorized users upon demand [4].

2.1.2 Integrity

Data integrity is one of the most critical elements in any system. Data integrity in the system is maintained via database constraints and transactions. Transactions should follow atomicity, consistency, isolation and durability properties to ensure data integrity. The lack of integrity controls at the data level could result in unplumbed problems. Developers need to approach this danger cautiously, making sure they do not compromise databases' integrity in their zeal to move to cloud computing [3]. In addition, the service provider must present the assurance of data integrity for the clients[1].

2.2 Data protection

The purpose of data protection legislation is to ensure that personal data is not processed without the knowledge and, except in certain cases, the consent of the data subject, to ensure that personal data which is processed is accurate, and to enforce a set of standards for the processing of such information. For those data stored on the service provider of the cloud side must not be accessed by unauthorized user and there should beseparate access mechanism for the employees of the service provider without authorization and authentication of request that presented by the user of the client side. Authorization becomes a challenge, especially when systems and participants get numerous, when interconnected applications evolve dynamically [26].Figure 1 shows intruder attack in the Cloud Database. In addition, the service provider must present the assurance of data protection for the client. The main data protection risks to your business are loss of data by third-party service providers are:

- unauthorized access to your data
- malicious activities targeting your service provider - e.g. hacking or viruses
- poor internal IT security compromising data protection [25]

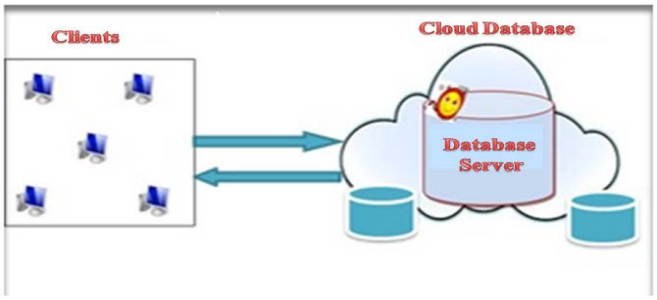

Figure1. Intruder attack

2.3 Recovery

Every service provider in cloud computing should have a disaster recovery protocol to protect user data. Disaster recovery capabilities are built into cloud computing environments and on-demand resource capacity can be used for better resilience when facing increased service demands or distributed denial of service attacks, and for quicker recovery from serious incidents[13].

2.4 Update process

The data stored in the cloud may be frequently updated by the users, including insertion, updating, appending etc. It is important to check correctness of data that is updated by user under the dynamic process. It is ensure that data is updated frequently and inform to the customers immediately that these changes have been made. It also affects the configuration that affects the instances in the cloud because when data has been updated then there is also necessary to secure that data so that data are in consistent state and saved correctly in proper place and provided to the customers. If any intruder enters in the cloud and copied that data then the customer may not know, because data have been widely spread throughout the network. Unless the cloud provider has developed some sort of monitoring software which can group/sort processes which have occurred for each user then this could be a large security risk and make attacking clouds even more attractive for cyber criminals [2].

2.5 Data Isolation

All data entering in the cloud provider's environment is encrypted with customer-controlled keys; the data is isolated from processes and changes implemented by the cloud provider [17]. In database systems, isolation is a property that defines how/when the changes made by one operation become visible to other concurrent operations [19]. For an application to run safely in a public cloud, it needs to be isolated from the environment around it at all times. This isolation is not just a matter of keeping protecting data and applications from threats, but also keeping things such that unwanted changes by the cloud provider that could compromise your existing security process [20].For deployed applications, it includes records and other content created or used by the applications, as well as account information about the users of the applications. Cloud providers need to ensure isolation of access - that software, data and services can be safely partitioned within the cloud and that tenants sharing physical facilities cannot tap into their neighbors proprietary information and applications[6].

2.6 Data Sanitization

Sanitization is the removal of sensitive data from a storage device in various situations, such as when a storage device is removed from service or moved elsewhere to be stored. Data sanitization also applies to backup copies made for recovery and restoration of service, and also residual data remaining upon termination of service[11].In a cloud computing environment, data from one subscriber is physically commingled with the data of other subscribers, which can complicate matters. For instance, many examples exist of researchers obtaining used drives from online auctions and other sources and recovering large amounts of sensitive information from them. With the proper skills and equipment, it is also possible to recover data from failed drives that are not disposed of properly by cloud providers.

2.7 Note the Client's Behavior

There are different types of user and different user's access different data from the databases in the cloud. It should be difficult to find that which user have access which type of information, so it is necessary to find the activity of the user because data stored in the cloud may be personal. When user want to access data in the cloud firstly to provide some identity to user. When the user login in the cloud computing environment his identity should be recorded and verify firstly. If the user is authorized then he will be allowed to enter in the cloud, if user is unauthorized then there is no permission to enter in the cloud and access information in the cloud. If the identity matches then provide the access to user and also note his behavior using log files in separate system in the cloud. If user behavior like trespasser then they will be tracked and punished with the cloud legal and regulatory services rules. In order to achieve the

trusted computing in the cloud computing system, we should have the mechanism to know not only what the participants can do, but also what the participant have done. So the monitoring function should be integrated into the cloud computing system to supervise the participant's behavior [12].

Access controls are one means to keep data away from unauthorized users; encryption is another. Access controls are typically identity-based, which makes authentication of the user's identity an important issue in cloud computing[11].

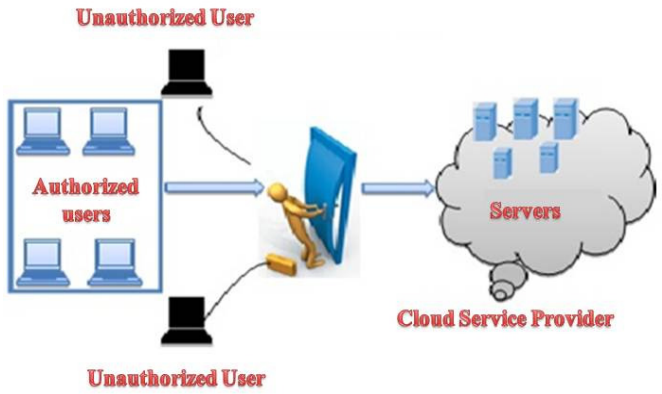

Figure 2. Access control mechanism

3. SECURE SERVERS

Hypervisor is the "virtualizer" that maps from physical resources to virtualized resources and vice versa. This virtualization not only reduces the system cost but also can dramatically reduce the installation space of physical readers and the operation cost[24]. It is the main controller of any access to the physical server resources by Virtual Machines[10].Over the last several years, virtualization has become a fundamental technology in cloud computing and enabled cloud computing platforms to dynamically allocate virtual machines as scalable Internet services. However, Virtual Machine technology is going main stream in the IT industry, security of VMs becomes the significant concern. Virtualization brings a more complex and risky security environment [7].

3.1 Denial of service (DOS) vulnerabilities

A denial-of-service attack (DoS attack) is attempts to make computer resources are unavailable to its intended users [21]. The resources are unavailable to users when attacker sends large volume of malicious packets which legitimate the user to access the services. In virtualization environment, services such as CPU, memory, disk and network are shared by VMs and the host. So it is possible that a DOS will be imposed to Virtual Machines which correspondingly take all the possible resources from the host. As a result, the system will deny any request from the guests because of no resources available [7]. Therefore our prime concern is to find out the no of packets being malicious in the legitimate requests and then mitigates them by an appropriate mechanism.

3.2 Spoofing virtual network

IP Spoofingis a technique of hijacking browsers by redirecting the Internet user to a falsified website. The interloper has the ability to fissure several networks in order to do this crime. In the route mode, route plays a role as a "virtual switch". The virtual switch uses a dedicated

virtual interface to connect each VM. In this case, a VM can do an Address Resolution Protocol (ARP) spoofing, redirecting packets to them and be able to sniff packets going to and coming from other VMs [7].

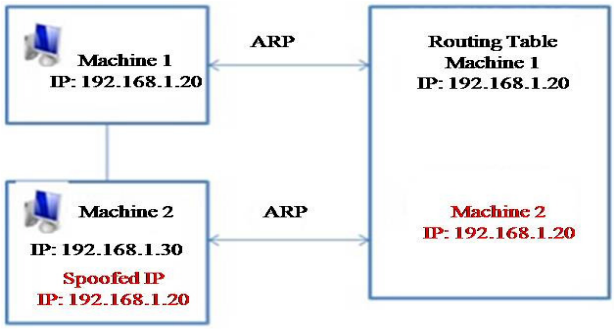

Figure 3. Spoofing IP in Virtual Network

Figure shows spoofing of IP in virtual Environment. A virtual route starts up and initializes the routing table by sending an ARP command to each VM in boot time. In this example, Virtual Machine2 makes an ARP spoofing attack. It forged a same IP address with Virtual Machine1 and sent an ARP to the virtual route. The virtual route will update the routing table information when it receives the ARP request from Virtual Machine2 [7].

One way to handle this problem we can use authentication based on key exchange between the machines on your network; something like Internet Protocol Security(IPSec) will overcomethe risk of spoofing.Internet Protocol Security is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

4. SECURITIES DURING TRANSMISSION

Using Cloud reduce the cost, greater flexibility and dynamic allocation of the resources provide greater advantages for the users but despite these advantages there are also challenges when transmit data from cloud to user and one cloud to other cloud. So there are mechanisms to provide security during transmission that are as under

4.1 Provide Authentication

In cloud computing environment, different users from different origin can appeal to join the Cloud. Then the first step is to prove their identities to the cloud computing system administrator. Because in cloud computing different users demand different resources and other applications, so the authentication is important and it is difficult process. It should be ensuring that administrator has different access mechanism and users have different access mechanism. If access is granted to the administrator, it does not necessarily mean access is granted to other users.

Our main goal is to maintaining security without any loss of information. So we can achieve this, firstly when any user sends request to server then user has to first register himself and after that login with its username and password that was provided to him. If the user is valid then server creates its log file that contains the information regarding its login and role of information accessed. After this process there should be encryption scheme with keys that the server creates unique key and send to client for the decryption. Then the client decrypts data with this key[5]. It is very important in this type of shared environment to properly and securely authenticate system users and administrators, and provide them with access to only the resources they need to do their jobs or the resources that they own within the system.

For all of the enterprises, the management of user's accounts is very important and must be strictly defined. A lot of enterprises usually confront the problem of user account such as the adoption of single sign on or each employee will be dispatched some different accounts to access different systems. Thus, multi-authentication for each employee might be very often to be confronted in an enterprise. Those accounts that come along with each individuals might be the same or different. Therefore, it is very difficult for the administrator to manage those user's identification accounts. Through the implement of Identity and Access Management, every enterprise could easily establish a managing mechanism to achieve the goal of user identification, authentication, and authorization simultaneously [1].

4.2 Network Security

As for large size enterprises or business corporations, in order to assure the use of the application of cloud computing, the service providers of cloud computing had better construct a model that utilizing the network communication with the enterprise. In addition, the encryption system and authenticating mechanism must be compulsive to maintain the information security in the process of communication [1].

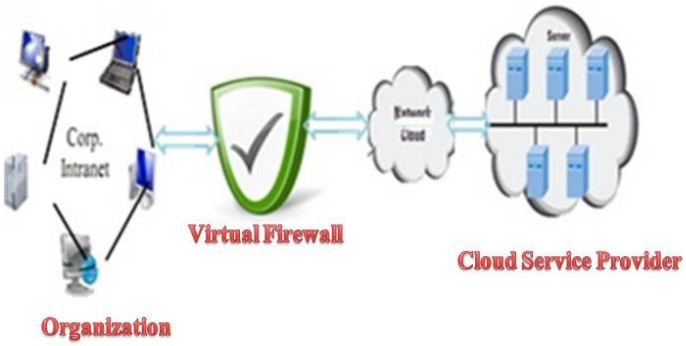

Figure 4. Virtual Firewall

Figure 4 shows virtual Firewall thatsupports filtering of packets, traffic management and access control. In this way, it can mitigate the risks of viruses, worms, Trojans, and inappropriate use in a virtual environment in the same way that a physical firewall could mitigate those risks if every physical server was directly connect to a physical firewall[32]. A virtual Firewall provides multiple logical firewalls for multiple networks on a single system. Using Virtual Firewall you can control bandwidth utilization of each virtual machine in your infrastructure, preventing overutilization and denial of service to critical applications.

5. CLOUD LEGAL AND REGULATORY SERVICES

With cloud computing, sometimes it is possible that physical location of data is spread across different regions and countries. The main problem with this widely spread data across different countries is that they have different laws to that data on the cloud and that could be a big issue if the host country does not have adequate laws to protect sensitive data[8]. Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the security rules of those jurisdictions.

The majority of respondents believed that data should not encounter compatibility problems if transported across different cloud providers if necessary, and the service level agreement should contain details about such transfer of data [22].Therefore it reveals a clear need for Cloud Computing customers to include specific clauses in their services agreement that prohibit the

provider from monitoring the customer's data usage or using this information for any purpose other than providing services to the customer.

6. ASSOCIATION OF SECURITY AMONG MULTI-CLOUDS

In Cloud Computing when customer wants to access data from different cloud then according the services provided from different clouds there must be security provided on both the clouds so that there is no loss of data during transfer. The same case when multiple clouds integrate together to deliver a bigger pool of resources or integrated services, their security requirements needs to be federated and enforced on different involved cloud platforms [10].

An SLA represents the understanding between the cloud subscriber and cloud provider about the expected level of service to be delivered and, in the event that the provider fails to deliver the service at the level specified, the compensation available to the cloud subscriber [13].In addition, an enterprise that use the application of cloud computing must have Service Level Agreement (SLA). In SLA is an agreement that records the services provides to user, guarantee and responsibility in the cloud so that information will not be access by any unauthorized user.

7. CLOUD ACCESS SECURITY

In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most common adoption [1].SSL (Secure Socket Layer) delivery, or https, encrypts your data in transit as it goes through the Content Distributed Network. Your content remains encrypted all the way from the origin servers out to the browser. You can choose to serve your content over SSL on a per object basis simply by using your SSL (Secure Socket Layer) URL [23].

VPN and FTP in case of VMs and storage services, Security controls should target vulnerabilities related to these protocols to protect data transferred between the cloud platform and the consumers [10].

8. CONCLUSION

Cloud computing is one of the bright model for both cloud providers and consumers. There are many advantages using cloud computing model but despite these advantages there are also challenges-specifically, security challenges in the cloud. We need to immobilize all the areas where security must be needed for accessing the information and sharing the resources. In this paper we discuss the most common unaddressed security areas in the cloud computing. For the secure environment in the cloud we need to provide some authentication mechanism for accessing the information as well as accessing the resources and also there should be system that monitor whole process and save the log files in that system. Though there are many concerns regarding dynamic allocation and information storage security my research much more concern to derive the areas where security needed.

9. REFERENCES

[1] Chang-Lung Tsai, Uei-Chin Lin, (2011) “Information Security of Cloud Computing for Enterprises”, Advances on Information Sciences and Service Sciences. Volume 3, Number 1, February 2011.

[2] Sean Carlin, Kevin Curran,(2011) “Cloud Computing Security”, International Journal of Ambient Computing and Intelligence, Vol. 3, No. 1, pp:38-46, April-June 2011, ISSN: 1941-6237, IGI Publishing.

[3] S. Subashini, V. Kavitha, (2011) “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications 34 (2011) 1–11.

[4] Dimitrios Zissis, Dimitrios Lekkas, (2010) "Addressing cloud computing security issues", 0167-739X/$ – see front matter © 2010 Elsevier B.V. All rights reserved.doi:10.1016/j.future.2010.12.006

[5] Cong Wang, Qian Wang, KuiRenandWenjing Lou, (2009) "Ensuring Data Storage Security in Cloud Computing", Quality of Service, 2009. IWQoS. 17th International Workshop on 13-15 July 2009.

[6] S.BIRUNTHA, V.VENKATESA KUMAR,S.PALANISWAMI, (2010) "Enabling Data Storage Security in Cloud Computing for Banking Enterprise"Recent Advances in Networking, VLSI and Signal Processing 2010.

[7] Hanqian Wu, Yi Ding, Chuck Winer, Li Yao, (2010) "Network Security for Virtual Machine in Cloud Computing", Proceeding 5th International Conference on Computer Sciences and Convergence Information Technology 2010.

[8] Anthony Bisong1 and Syed (Shawon) M. Rahman, (2011) "AN OVERVIEW OF THE SECURITY CONCERNS IN ENTERPRISE CLOUD COMPUTING" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.

[9] S. Subashini, V. Kavitha, (2011) "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications 34 (2011) 1–11 1084-8045/$ - see front matter & 2010 Elsevier Ltd. All rights reserved.doi:10.1016/j.jnca.2010.07.006.

[10] Mohamed Al Morsy, John Grundy and Ingo Müller, (2010) "An Analysis of the Cloud Computing Security Problem", Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[11] Wayne A. Jansen, (2011) "Cloud Hooks: Security and Privacy Issues in Cloud Computing" The 44th Hawaii International Conference on System Sciences – 2011.

[12] Ramya Devi M, Balamurugan P S, Thanushkodi K,(2011) "The Trusted Computing exemplary with Astonishing Security for Cloud Computing" IJCSNS International Journal of Computer Science and Network 206 Security, VOL.11 No.1, January 2011.

[13] Wayne Jansen, Timothy Grance,(2011) "Guidelines on Security and Privacy in Public Cloud Computing" Draft Special Publication 800-144.

[14] Mithun Paul and Ashutosh Saxena,(2010) "ZERO DATA REMNANCE PROOF IN CLOUD STORAGE", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.

[15] Ryma Abass and Sihem Guemara El Fatmi, (2009) "EXECUTABLE SECURITY POLICIES: SPECIFICATION AND VALIDATION OF SECURITY POLICIES" International Journal of Wireless & Mobile Networks (IJWMN), Vol 1, No 1, August 2009.

[16] Aiiad Albeshri and William Caelli, (2010) "Mutual Protection in a Cloud Computing Environment", 12th IEEE International Conference on High Performance Computing and Communications 2010.

[17] "Cloud Isolation", http://www.cloudswitch.com/ blog/tag/cloud%20isolation

[18] "Multi-tenancy in cloud computing", http://horicky.blogspot.com/2009/08/multi-tenancy-in-cloud-computing.html

[19] "Isolation (database systems)", http://en.wikipedia.org/ wiki/Isolation_%28database_systems%29.

[20] "True Isolation Makes the Public Cloud Work like a Private Cloud", http://www.cloudswitch.com/page/true-isolation-makes-the-public-cloud-work-like-a-private-cloud.

[21] "Denial-of-service attack", http://en.wikipedia.org/wiki/Denial-of-service_attack

[22] "My Master of Law conclusion on the legal advice in cloud computing"http://www.ecademy.com/node.php? Id=158539.

[23] "Rackspace Cloud Files CDN launches SSL Delivery", http://www.rackspace.com/cloud/blog/2011/03/10/ rackspace-cloud-files-cdn-launches-ssl-delivery/.

[24] Shin-ichiKuribayashi and Yasunori Osana, (2010) "System Virtualization and Efficient ID Transmission Method for RFID Tag Infrastructure Network", International Journal of Computer Networks & Communications (IJCNC) Vol.2, No.6, November 2010.

[25] "Dataprotectionandcloudcomputing" http://www.businesslink.gov.uk/bdotg/action/detail?itemId =1084 89193&type=RESOURCES

[26] Ulrich Lang, (2010) "OpenPMFSCaaS: Authorization as a Service for Cloud & SOA Applications", 2nd IEEE International Conference on Cloud Computing Technology and Science 2010.

Authors

Dr. Gurdev Singh was born in 1982 in Amritsar, India. He received his M.Sc. in Mathematics in 2002, M.Tech. in information Technology in 2004 and Ph.D. in 2010. Presently, He is working as Associate Professor & Head, Department of Computer Science & Engineering, Eternal University,Baru Sahib, Himachal Pradesh, India. In addition he has the responsibilities of Assistant Dean of Studies, Assistant Controller of examination, Eternal University, Baru Sahib. He is also heading "Chhina Insurance Agency" as 'Director of Technology' at P.O. Box 964, Manteca, CA 95336, USA. During his work for 7 years, he has numerous challenging assignments to his credit, in the areas of Computer Science. He has chaired many technical sessions in National seminars and conferences. He had worked on various software engineering projects. His research interest includes Software Testing, Cloud Security and Quality Insurance.

Amit Sharma received his B.Tech degree in Computer Science & Engineering. in 2008 from Kurkshetra University and pursuing M.Tech (part time) in Computer Science and Engineering at Eternal University, Baru Sahib (H.P). He is currently a Lecturer in department of Computer Science & Engineering at Eternal University (www.eternaluniversity.edu.in), Baru Sahib (H.P). He has a total experience of 2 years in teaching. His research interests include Cloud Computing Security, Software Engineering and Network Security.

Manpreet Singh Lehal received his M.Sc. in Mathematics in 2002, M.Tech. in information Technology in 2004. He is presently working as Assistant Professor, Post Graduate Department of Computer Science, Lyallpur Khalsa College, Jalandhar, and Punjab, India. He has more than 6 years of experience in teaching. His areas of interest are computer graphics, fuzzy logic and cloud Computing. He worked on a number of major and minor projects.