International Journal of Multimedia and Ubiquitous Engineering
Vol.9, No.9 (2014), pp.81-90
http://dx.doi.org/10.14257/ijmue.2014.9.9.09

Cloud Security Mechanisms for Data Protection: A Survey

Allen Oommen Joseph[1], Jaspher W. Kathrine[1*] and Rohit Vijayan[1]

[1]*School of Computer Science and Technology*
Karunya University
Coimbatore, India.
joseallen3@yahoo.com,
kathrine@karunya.edu, rohit.vij06@gmail.com

Abstract

Cloud computing has evolved over the years in providing various services to the end users. The cloud features makes it acceptable by the industries in leveraging most of its applications in to the cloud. Security concerns exist in most cloud platforms and are prone to various attacks. This paper focuses on various security mechanisms that are provided in the enterprises and also discusses few of the common security mechanisms like authentication, authorization, encryption and access control. The methods deployed within each security mechanisms are also analyzed.

Keywords: *cloud computing, authorization, authentication, access control, encryption*

1. Introduction

Cloud Computing has evolved over the past from utility computing, autonomic computing and grid computing through the sharing of resources, computation and storage capabilities. According to National Institute of Standards and Technology [1] cloud is a model for enabling ubiquitous, convenient, on demand network access to shared pool of resources which can be provisioned rapidly with minimum management and service provider interaction. The virtualization technology has brought a great revolution in cloud computing by making it different from the various other computing platforms. Virtualization has made the logical systems to appear like the original physical systems or resources. Virtualization provides for the maximum utilization of the various resources. Various features like scalability, availability, elasticity, multi-tenancy, flexibility, and ease of use has made cloud a dominant platform in today's world.

Cloud computing security is an apprehension that needs great courtesy. Cloud has been prone to various security issues like storage, computation and attacks like Denial of service, Distributed Denial of Service, Eavesdropping, insecure authentication or logging etc. The cloud needs to address the various security concerns in order to meet the users demand in providing them with high quality service and also offer essential amenities to the users meeting the various cloud standards and ensuring quality of service. End user migration into the cloud recently has brought about an increasing demand for shifting the various resources, photographs, files, remote servers etc in to the cloud and also accessing them with the help of an internet connection. Cloud computing has an intended power to profoundly rethink and redesign the enterprise business and Information Technology architecture. This paper provides an overview of the various cloud computing security concerns and solutions provided to overcome the security glitches.

* Corresponding Author

ISSN: 1975-0080 IJMUE

1.1. An Overview of Cloud Computing

Cloud computing can be a cluster of computers held together to perform various tasks, computations and other operations and is a substitute for distributed computing in which many number of applications or programs can be run simultaneously [2]. The various feature of cloud computing includes scalability, availability, flexibility, multi-tenancy, resource pooling, reliability and high capacity. The cloud usage is based on a payment basis in which the users have to pay for the resources that have been used by them. According to a recent study cloud vendors are growing rapidly at a rate of 90%.

The cloud computing can be classified in to various types and different models based on the various services they provide. The cloud computing types includes private cloud, public cloud, hybrid cloud and community cloud. The service delivery models can be classified as Software as a service (SAAS), Platform as a Service (PAAS) and Infrastructure as a Service (IAAS). The descriptions of each of these models are described below.

1.2. Types of Cloud based on Usage

1.2.1. Private Cloud: The private cloud is meant for or devoted to a single organization, in providing the various services necessary for its working. Many small developing organizations can use the private cloud for achieving low cost set up or little investment in developing. They can also scale well in to the next step or higher levels based on the capital investments and company profits. The cost in setting up a private cloud can vary. Some of the private cloud service providers includes Cloud stack, Rackspace, Red Hat cloud *etc*.

1.2.2. Public Cloud: The public cloud is meant for organizations sharing their resources or various infrastructure, softwares and platforms with the public. The sharing of resources and storage may take place over the internet. Bluelock, Microsoft and Google are examples of public cloud providers. The public cloud provides various features like scalability, flexibility, cost effectiveness and location independence [3]. The various public cloud vendors include Google, HP and Dell Inc.

1.2.3. Hybrid Cloud: Hybrid cloud model deploys the use of both public and private cloud. The main feature of hybrid cloud includes scaling across various clouds. The use of hybrid cloud may require the need for an on-premise as well as off-premise resources. Fault tolerance can be achieved at a very high level in hybrid clouds. The workload has to be balanced between the public and private cloud in order for the Hybrid cloud to become a realism .Voxen, VMware and Western Digital (WD) are some of the service providers for hybrid cloud.

1.2.4. Community Cloud: According to National Institute of Standards and Technology community cloud is defined as a subclass of public cloud in which various resources and services like Softwares, platforms and infrastructures can be shared among various users [4]. In a crowded cloud market place various service providers can distinguish themselves using community cloud. In a research conducted by Cisco about 90% of the CIO's admit that the community cloud will be the most noticeable on demand model [5]. The community cloud providers include Intel Corporation and Cisco.

Service delivery models can be defined as a set of rules, standards and various guidelines that are provided for the various services in cloud. The services can be in terms of infrastructure which includes servers, networks, routers, switches etc as well as softwares and platforms which may include operating systems and other platforms like open stack, open nebula, Hadoop, and eucalyptus.

1.3. Types of Cloud Based On Service Delivery

1.3.1 Software as a Service: The software as a service (SAAS) model provides all the required softwares necessary for performing the various operations which meets the needs of the users. The users have to make a payment based on the usage of the software. The softwares are made available most of the time in cloud. According to a survey most of the public cloud sales are subjugated by the SAAS platform [6]. The various providers of SAAS include Salesforce.com, ZOHO and Google, Intuit etc.
Intuit [7] provides various security measures such as Advanced Encryption Standards using 256 bit encryption, video alarm monitoring and disaster recovery. Intuit is prone to outage at times which in turn affects the quality of service and cost is also a major concern that needs to be addressed. Sales force [8] one of the most innovative company in the United States provides security for its data stored in the cloud by firewall protection, intrusion detection, third party validation, and also periodic architectural reviews are conducted by security professionals. It is prone to phishing attacks and moreover privacy remains to be concern in Salesforce with respect to the data stored in its cloud.

1.3.2. Platform as a Service (PAAS): Hosting of various applications in the cloud in a fast and scalable manner and enabling the users to gain the advantages of using cloud computing model. The platform as a Service model manages the various administrative tools, softwares and a variety of applications which are required in building a cloud environment [9]. It also helps in developing applications that are nimble. It provides various features like auto scaling, extensibility, supports multiple hosting environments also openness in selecting from a set of choices. When moving in to the cloud data management is a major concern and the data transparency in the cloud has to be maintained by the provider itself.

Microsoft [10] is a leading platform as a service provider which provides the main security features like load balancers, firewall, third party attestation, security incident management and Transport layer security for secure transferring of data. A major drawback was that during data hosting outside the customer jurisdiction, data sovereignty issues might occur. Google [11] has provided an automatic encryption of the data in which it uses the 128 bit AES encryption standard, which provides security from unauthorized access that is when some entities tries to access the stored data and read the contents, an automatic encryption of data will take place. Google provides some security measures which include internal audits, Rat Proxy, debugging and maintenance based on Secure Shell Connection (SSH) cloud locks and also examination of logs. The major disadvantage was that there is a limit for storing data in Google and also outages and downtimes could also occur. Amazon S3 provides for storing large amount of user data can be stored at various storage servers located at various parts. The major security features provided by Amazon [12] includes Amazon Identity and access management, Amazon Cloud watch used to monitor Amazon resources and applications. Amazon Web Service management console, Hash- based Message Authentication Code (HMAC) and Secure Hash Algorithm (SHA 1) signature is used for authentication. Although, Amazon provides the best storage provider S3 and is reliable the web interface for uploads or downloads is slow and unreliable. Maintaining the data privacy is a concern and Amazon still needs its attention to address few of these challenges when becoming the leading storage provider.

1.3.3. Infrastructure as a Service (IAAS): According to Margaret Rouse Infrastructure as a service model includes the various resources like hardware, networking components and devices, storage etc which are needed for the proper operation of an organization. Various features for IAAS includes utility computing models, policy based services, desktop virtualization and automation of administrative tasks. Some of the real time providers include Qwest, EMC and Verizon Terrimark. Qwest provides security measures like web

defence, PCI compliant hosting and contact center solution, secure IP gateway, DDOS mitigation service and professional security services [13]. Other preventive methods like anti-virus/anti-spam, compliance auditing policy enforcement, hosted IVR for inbound call management, firewall, backup and storage.

EMC provides various security solutions like multiple recovery points for continuous data protection, RSA data loss prevention, RSA identity Protection and verification which provides fraud protection by preventing cybercrime identity theft. RSA secure ID which uses two factor authentication and secure tokens for ensuring the authenticity of a user [14]. Data at motion is encrypted through the Secure Socket Layer Version 3 and data at rest is encrypted using the 256 bit Advanced Encryption Standard.

Verizon [15] provides the inbound and outbound scanning which are used for anti- virus, anti-spam, URL filtering and image control. A network based DDOS protection scheme is also enabled. Tape encryption and Incident response management are the other major functionalities provided by Verizon. The disadvantage of Verizon includes its user transparency in which the user doesn't get to know the various operations. The configurability of different server hardware is also a concern. The Cloud platform needs to be maintained at an accepted cost which is not possible in Verizon. Verizon's Hybrid Cloud solutions have not yet addressed the key management problem.

2. Security Issues in Cloud Storage

Security is one of the main reasons that most of the industries are still holding back its data to be stored and processed in the cloud. Security can be varied in the cloud like storage security, computation security, network security etc. The figure 1 illustrates how the security is applied in a corporate network. The cloud technology is a jargon computing which is deployed on top of all these corporate networks. The industries leverage their computing tasks and services to the cloud, wherein the data is accessed based on a pay-as–you-use measure.

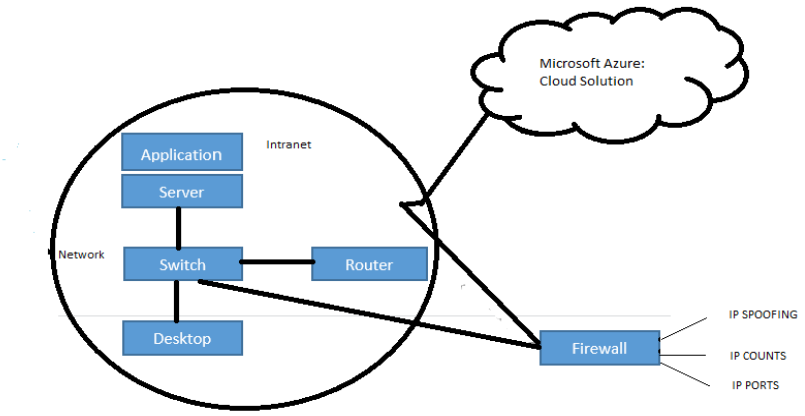

Figure 1. The Cloud Security Architecture

Figure1 illustrates the various users connected to the network components through which the packets are routed and information processing and various computations are done. The network indeed is connected to the server on top of which the various applications run. Some of the reasons the industries have adopted cloud computing involves,

1. Short period requirement / adhoc requirements
2. Companies do not want to do a capital investment rather it wanted to take the service which is at an opaque cost.

3. Availability of Platforms
4. Cost of Operations.
5. Skilled Resource Avoidance
6. Better Turn around Time (TAT) on capacity enhancement and application hosting.

Various types of attacks are possible in cloud. Most of the attacks focused on real time industries and also are applicable f**o**r cloud environments. Some of the attacks include IP Spoofing, IP ports, IP counts, DDOS, phishing, modification of messages, masquerade, traffic analysis *etc*. Some of the security measures adopted by the cloud in securing its data include authentication, authorization, access control and encryption. These methods are discussed below with the various solutions they provide for the cloud storage security. The table 1 provides an overview of the various security solutions applicable to network and cloud at the desktop, server and user/ application levels.

Table 1. Security Measures Adopted for Cloud and Network in Real Time Industries

Security Solutions	Desktop (user) Windows 7	Server (Application Platform) Windows 2008	User Application
OS Hardened (not required services or ports to be blocked)	Yes	Yes	No
Antivirus, Malware, Spyware	Yes	Yes	No
Vulnerability assessment and fixing for OS/App	Yes	Yes	Yes
Patch Management (updates)	Yes	Yes	Yes
Access Control	No	No	Yes
Segregation of Duties	No	No	Yes
Auditing	No	No	Yes

2.1. Authentication in Cloud

Authentication is the process of ensuring that the right entity is accessing the data. In cloud authentication refers to making sure that the user is storing the data by giving a valid user name and password which is a single factor authentication method employed. The user has to prove his/her identity to the cloud service provider to access the various data stored in the cloud. RSA [16] considers that the private and public cloud has different authentication schemes. A single login using trust policies and strong authentication methods are used. It has proposed a centralized virtualization management console which is used to safeguard the private clouds from unauthorized access. Some of the authentication schemes adopted by the RSA includes knowledge based authentication, two factor authentication and adaptive authentication. Reduced cost and improved security is provided.

The In- Sync cloud [17] provides authentication by checking in the Active Directory server. The end point authentication is done through corporate firewalls. Some of the authentication schemes include password, username and an authentication key used to authenticate the users which is reset after every use. The demilitarized zone is deployed in which the access is provided using the public IP address.

Amazon Web Services (AWS) [18] focuses on the exchange of confidential information between the browser and the web server in which an Amazon virtual private cloud is used. The various authentication techniques like multifactor authentication and AWS identity and access management are being addressed. Open ID [19] used for user authentication doesn't require the separate adhoc networks and is an open standard. A third party service is used to maintain the different identities by authenticating the various users.

Shibboleth [20] is another standard that is used for authenticating to different entities using only a single piece of information. The various resources of clients that lie within or outside an organization can be accessed by others using the open standard Open Authentication (OAuth). The main advantage of OAuth is its interoperability.

The strong authentication server (SA Server) verifies the user's certificate with the local certificate authority. Various attacks such as phishing, SQL injection, cookie tampering and session hijacking can be prevented. In [21] a method which allows users to be authenticated to multiple services using only one password has been proposed. This method was proven to be secure against dictionary attacks and honeypot attacks. Companies like Microsoft, Google and Facebook has adopted this method.

The use of Proxy settings allows for the needed IP addresses to be authenticated to an external site. The proxy URL will white list the various contents and will provide access to trusted sites only. The Table 2 illustrates some of the authentication schemes that are used for securing the data contents.

Table 2. Authentication Mechanisms Adopted for Securing the Data in Cloud

Vendors	Authentication mechanisms	Advantages
RSA	Knowledge based authentication Two factor authentication Adaptive authentication	Reduced Cost Improved security
AWS	Multifactor authentication	Identity Management Access Management
Facebook	Single password authentication	Secure against dictionary attacks and honeypot attacks.

2.2. Authorization

Authorization ensures that the user submits its user identity in order to login to a particular service. This method is the step followed after authentication. Oracle [22] has proposed an Oracle Database Vault which protects the application data from various administrative users and also provides authorization. An access control mechanism based on Role Based Access [23] was proposed for multi-tenancy method of protecting the data in cloud environments. The segregation of duties of various administrators is provided such that an administrator in a particular domain will not be able to access the other domain.

A policy based authorization scheme [24] which can be run as an Infrastructure as a Service model in order to protect the users privacy by ensuring that they can set their own privacy policies in order to protect the user data from unauthorized access. The OASIS cloud authorization [25] has provisions for the management of authorizations in the cloud service delivery models. It maintains a log of where the users are and the details of the devices that are being used by them.

VMware [26] has provided a strong authorization scheme by integrating the corporate directories and various policies with the policies of the service providers. Two factor hard or soft tokens or certificates are provided to ensure that the end user is authorized in a secure manner. The table 3 indicates the various authorization schemes adopted for securing the data that is stored in cloud environments.

Table 3. Authorization Schemes Adopted for Securing the Data

Vendors	Authorization Technique	Advantages
ORACLE	Oracle Database Vault	Secure the administrative data
OASIS CLOUD	CloudAuthZ	Maintaining of user logs Management of authorization schemes
VMware	Two Factor hard or soft tokens	Secure authorization

2.3. Encryption

Encryption is the process of making plaintext in to an unreadable format by a user or a third party. The conversion is made in to cipher text which has to be decrypted at the receiving side. The data is encrypted before it is stored in to the cloud to ensure that the cloud service providers does not read or modify the data contents stored in the cloud. The cloud service provider may either sell the data or view the contents by violating the security of the user.

Dell [27] data protection/encryption has allowed for protecting the various user data that is being stored on an external drive or media. Software and hardware based encryption schemes are deployed. The main advantage being that the user intervention is not required to enforce policies and they are easy to deploy and manage as well. Dell also has employed the Transparent File Encryption in which a control over the various users accessing the data is maintained. In this method a white list of users are created who will be given the access to services and to share files. The monitoring of the usage, auditing of events and report creation and the workload of the compliance is also reduced.

The Wuala cloud [28] provides for the encryption of data in personal computers before sending or transferring it to the cloud. This ensures that only the user has access to the data and not even the provider. A Hierarchical Attribute Based Encryption method has been proposed in [29] where fine grained access control and also high performance is achieved. A predicate encryption method is proposed in [30] using various search operations and privacy of the users is also ensured. This method enables the owners to control their own data and its lifetime.

Online Tech [31] has given solutions to provide cloud security by encrypting the data by methods such as Full Disk Encryption which encrypts the data stored on a hard disk during the booting operation and Whole Disk Encryption which encrypts the data at rest using the Advanced Encryption Standard algorithm. A bit locker password is encrypted that ensures that the data is safe if the device has been stolen. The Linux disk encryption is used to encrypt the data which lies within the kernel. The main advantage being that the partitioned data can be encrypted. Table 4 gives an overview of the various encryption techniques available for protecting the data stored in the cloud.

Table 4. Encryption Techniques Adopted for Cloud Security

VENDORS	ENCRYPTION TECHNIQUE	ADVANTAGES
DELL	Hardware based Encryption Software based Encryption Transparent File Encryption	User Intervention is not required. Easy to deploy Control over the users accessing data Compliance workload reduced
WUALA	Encrypting data in personal computers	Only user has access to the data
ONLINE TECH	Full Disk Encryption Whole Disk Encryption	Partitioned data can be decrypted Encryption of data at rest

2.4. Access Control

Access control is the method of ensuring that the access is provided only to the authorized users and hence the data is stored in a secure manner. Various access control mechanisms such as firewall, Intrusion detection and segregation of duties are enabled at various layers of the network and cloud. Various access control Lists (ACL) are created in which users are classified as white list and black list for separating and providing access based on a Defence in Depth method. The firewall is deployed in the network to allow only the filtered contents to pass through which can be set up by the users based on a certain set of policies. The Demilitarized zone is put in to the firewall wherein, it provides an extra layer of security and make sure that the data is safe.

On accessing certain sites, automatic email will be send to the monitoring team. In this method, a threshold value on the various IP addresses of certain sites is set. An SMS or email will be send to the nominated group, once the value has exceeded beyond its limits. Weekly reports and alerts are sent to the respective providers and also a log is maintained on the various visited sites. The industries use the BMC Remedy software which is integrated in to the incident management tool, which raises an alert when an incident occurs. The cloud police method provides access control to the various hypervisors. The cloud security is provided to the multi-tenant cloud environments. Various access control policies such as inter tenant communication, Fair- sharing among tenants and Rate limiting tenants existed. The main advantage provided by the paper includes the scalability and simplicity.

MacAfee has provided access control by using various methods such as MacAfee Web Gateway, MacAfee Single Sign on (CSSO) and MacAfee one time password. Fujitsu has provided security from unauthorized access and problems like injection attacks and cross-site scripting. The various authorization schemes like Central Management Authorization and Virtual System Management Authorization has been provided by Fujitsu. The table 5 illustrates the security solutions provided by various organizations in protecting its data stored in the cloud.

Table 5. Security Solutions Provided for Access Control Mechanisms

VENDORS	ENCRYPTION TECHNIQUES	ADVANTAGES
MCAFEE	MacAfee Web Gateway MacAfee Single Sign On MacAfee One Time Password	Policy Management Data loss is prevented.
FUJITSU	Central Management Authorization Virtual system Management Authorization	Prevents Injection attacks and Cross-site scripting

3. Conclusion

Cloud computing has brought about a big revolution in the information technology field, business and various other applications. Cloud offers benefits such as scalability, elasticity, multi-tenancy, cost effectiveness and reliability. Even though cloud offers a lot of benefits, there are various disadvantages in cloud like security, downtime, and technical issues and are also prone to a variety of attacks like Denial of Service (DOS), Distributed Denial of Service (DDOS), Man –in-the-Middle, IP Spoofing, etc. The various security mechanisms provided to overcome these attacks like authentication, authorization, access control and encryption techniques are discussed and also the various measures adopted by these mechanisms with respect to the use in industry for protection from attacks are also taken to

consideration. The data transmission over the channels needs to be secured in the most effective manner in order to avoid attacks and leakage of data that is sent to the cloud. The future work focuses on protection of the messages transmitted over an insecure channel by providing various security measures like encryption and also digitally signed certificate generation.

References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, **(2011),** pp. 1-3.
[2] A. Merrihew, Cloud Computing: How to explain it to others in your organization [DB/OL].
[3] B. Butler, "Are Community Cloud Services the Next Hot Thing", [DB/OL].
[4] M. Samuels, "Community Clouds: why they're a step too far for Organisations", [DB/OL].
[5] D. Linthicum, SaaS is Cloud Computing's quiet killer app [DB/OL].
[6] A. Chriss, Intuit Customer Solution Case Study [DB/OL].
[7] http://www.salesforce.com/assets/pdf/misc/WP_Forcedotcom-Security.pdf **(2010-07-06)**
[8] D. Juengs, What is Platform as a Service [DB/OL].
[9] file:///C:/Users/staff/Downloads/CloudSecurityConsiderations_MicrosoftOffice365.pdf **(2011-07-06)**
[10] https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf **(2012).**
[11] D. Todorov and Y. Ozkan, http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf **(2013-11-04)**
[12] http://www.questsys.com/cloudServices.aspx **(2013-11-04)**
[13] http://www.gemalto.com/press/Gartner_Magic_Quadrant_2013.html **(2013-03-05)**
[14] http://www.terremark.com/uploads/documents/WP14970.a.Online_Identity_Mgmt_03_PrePress.pdf **(2012-10-23)**
[15] E. Baize, Cloud and Virtualization: Surpassing Current levels of security [DB/OL].
[16] http://www.druva.com/documents/Druva-inSync-Security-Q115-R54-10062.pdf **(2014)**
[17] J. Barr, A. Narin, and J. Varia, "Building Fault-Tolerant Applications on AWS", Amazon Web Services **(2011)**, pp.1-15.
[18] U. Khalid, A. Ghafoor, M. Irum and M. Awais Shibli, "Cloud Based Secure and Privacy Enhanced Authentication and Authorization Protocol", Procedia, **(2013)**, Vol.22, pp. 680-688.
[19] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues", Future Generation Computer Systems, **(2012)**, Vol. 28, Issue 3, pp.583-592.
[20] T. Acar, M. Belenkiy and A. Kupcu, "Single Password Authentication" Computer Networks, **(2013)**, vol. 57, no. 13, pp. 2597-2614.
[21] Oracle, Private Database Cloud [DB/OL].
[22] J. B. Bernabe, J. M. Marin Perez, J. M. Alcaraz Calero, F. J. Garcia Clemente and G. M. Perez, "Semantic-Aware – multitenancy-authorization system for cloud architectures", Future Generation Computer Systems, **(2014),** vol. 32, pp. 154-167.
[23] D. W. Chadwick and K. Fatema, "A privacy preserving authorization system for the Cloud", Journal of Computer and System Sciences, **(2012**), vol. 78, no. 5, pp. 1359-1373.
[24] A. Saldhana, R. Marian, A. Barbir and S. A. Jabbar, OASIS Cloud Authorization (CloudAuthZ) TC [DB/OL].
[25] http://www.vmware.com/files/pdf/partners/vmware-public-cloud-security-wp.pdf?src=vcld-2012-1-blog-PCSA%20whitepaper-ex-41 **(2012)**
[26] http://www.dell.com/learn/us/en/04/campaigns/dell-data-protection-solutions, **(2013-11-06)**
[27] http://www.wuala.com/en/learn/technology, **(2014-01-03)**
[28] G. Wang, Q. Liu, J. Wu and M. Guo, "Hierarchical Attribute Based Encryption and Scalable User Revocation for Sharing Data in Cloud Servers", Computers and Security, **(2011)**, vol. 30, no. 5, pp. 320-331.
[29] C. I. Fan and S.-Y. Huang, "Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage", Future Generation Computer Systems, **(2013)**, vol. 29, no. 7, pp. 1716-1724.
[30] http://www.onlinetech.com/cloud-computing-hosting/overview **(2014)**
[31] L. Popa, M. Yu, S. Y. Ko, S. Ratnasamy and I. Stoica, "CloudPolice: taking access control out of the Network", ACM Sigcomm Workshop, (**2010**).

Authors

Allen Oomen Joseph, He received his BE (CSE) from Anna University, India and his Masters in Network and Internet Engineering from Karunya University, India. Currently he is working as a desktop security administrator at ZS Associates, Pune, India. His interests include Network Security, Information security and Database management.

G. Jaspher Willsie Kathrine, She received her BE (EEE) from Bharathiar University, India and her Masters in Computer Science and Engineering from Anna University, India. Currently she is pursuing her PhD in Karunya University, Coimbatore, in the area of Grid Security. Now she is an Assistant Professor in the School of Computer Science and Technology, Karunya University. Her interests include computer security, grid and cloud computing, image processing.

Rohit Vijayan , He received his Masters in Network and Internet Engineering from Karunya University, India. His interests include cloud computing, Information security and Database management.