International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 04 | July-2015 www.irjet.net p-ISSN: 2395-0072

Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey

B. Rex Cyril[1], DR. S. Britto Ramesh Kumar[2]

[1] *Research Scholar and Assistant Professor, Department Of Computer Science, St.Joseph's College (Autonomous), Trichy, Tamilnadu, India. rexcyrilsjc@gmail.com*

[2] *Asst.Professor, Department Of Computer Science, St.Joseph's College (Autonomous), Trichy, Tamilnadu, India. brittork@gmail.com*

Abstract

Data security has a major issue in cloud computing environment; it becomes a serious problem due to the data which is stored diversely over the cloud. Data ***privacy and security are the two main aspects of user's*** *concern in cloud information technology. Numerous techniques regarding these aspects are gaining attention over the cloud computing environments and are examined in both industries and academics. Data privacy and security protection are becoming the most significant aspects for the future enhancement and development of cloud computing technology in the field of business and government sectors. Thus, in this paper, the cloud computing security techniques are assessed and its challenges regarding data protection are discussed. The main aim of this proposed work is to enhance the data privacy and security for the reliable cloud environment. This comparative research investigation of the existing cloud security approach regarding the data privacy and security techniques utilized in the cloud computing. It will be useful toenhance the security of data storage in a cloud environment.*

Key words: Cloud Computing, Security Issues and challenges, Cloud Architecture, Data Privacy

1. INTRODUCTION

Cloud computing has been intended as the next generation paradigm in information Technology. From this cloud computing environment, both resources and applications are provided through the Internet as a service on demand. Cloud environment is comprised of software and hardware resources in the data centers that run different services over the internet or network to satisfy the user's needs and it depends on sharing resources instead of having local servers to handle application for a certain individual or organization [1] [2]. Since there is no infrastructure investment requires, shrink or expand the resources based on on-demand and the payment based on usage, it becomes popular among different technology aspects. The numerous cloud enterprise system looks for these advantages to be used in various applications. The service of the cloud makes it possible to access the data at anytime from anywhere. Cloud computing utilize the networks of a huge group of servers naturally brings a low rate data processing with specialized connection. Therefore, cloud computing has an interesting new model of IT service provisioning and support driven by productivity and economic benefits.

Cloud computing can be separated into two subsections such as the cloud and the user. In most scenarios, the individual user is connected to the cloud environment through the internet. This process is also possible for an organization to connect the private cloud via the internet. Therefore, both subsections are alike other than the utilization of the public and private cloud or the network [3] [4]. The cloud computing has the normal functions such as, the user requests to the cloud and the cloud response to the user [5]. The elasticity and multi-tenancy are two key features of the cloud environment (i.e.) sharing the same service instance, among the various tenants and elasticity enables a service based on the present cloud service demand. Characteristics of this service is to improve the service availability and resource utilization. Cloud services are divided into three service models such as

Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS), Software-as-a-service (SaaS). Each service has various implementations as shown in Figure 1, which complicates progress of standard security model for each cloud service.

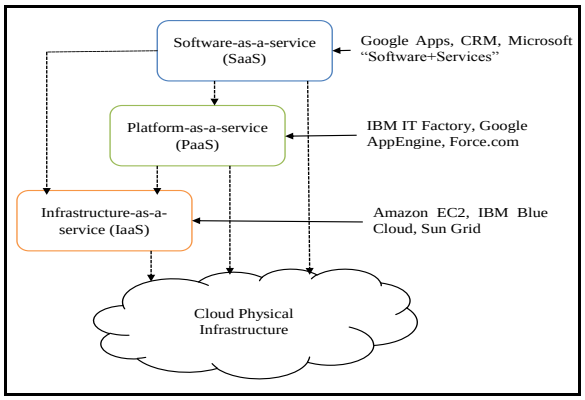

Figure -1: Cloud Service Model

Although the security is needed for cloud storage which differ with various users and applications, the users share the same three objectives such as availability, integrity and confidentiality. Different types of tools have been generated to accomplish these objectives, such as access control, authentication, audition, digital signature and encryption. This proposed work aims at providing a detailed study of current data security mechanisms for cloud storage and direction in attaining each security objectives.

2. SECURITY ISSUES, CHALLENGES, and METHODS

In cloud different types of security issues and challenges are available. Following part is discussed about few security issues, threats and challenges of cloud computing and their mitigation.Secure cloud architecture as shown in figure 2.

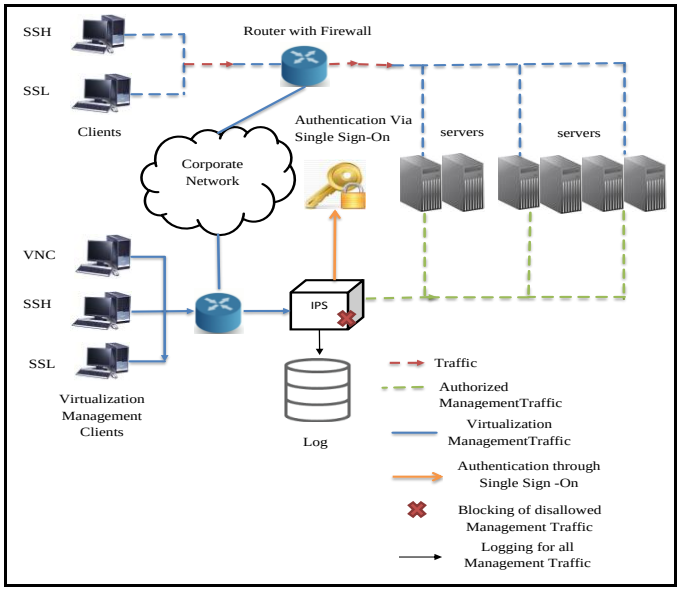

Figure -2: Secure Cloud Architecture

Normally the cloud users will have different types of logins, but it will direct to the authentication problem. The Single Sign On provides the user level authentication. To increase the data availability by using dynamic cloud storage servers within the cloud infrastructure. A proper intrusion prevention and detection components are implemented with virtual firewall and IPS should be installed to protect the cloud network. Additionally, the single management console is used for protecting the cloud network. The virtual management clients are Virtual Network Computing (VNC), Secure Shell (SSH) protocol, Secure Sockets Layer (SSL) protocol.

2.1 VM Attacks

Cloud computing architecture is separated into two different sections such as Front end and Back end. The Front and Back ends are connected through the network. The Front end side is the client or user and the cloud provider is on the back end. The front ends comprises the client's computer and needed to access the cloud architecture. On the back end of the cloud computing includes different virtual machines (VM's) [6], computer, data storage system and servers that generate the cloud computing services [7].

Cloud computing is relied upon VM technology. The Hypervisor, Sphere, VMware are used for Cloud implementation. The cloud developers required to take care of cloud attacks when the implementation is done and also take care by utilizing Intrusion Prevention System (IPS) and Intrusion Detection Systems (IDS) [8]. The IPS and IDS issues can solve by using suitable firewall.

2.2 Loss of Governance

The Loss Of Governance problem relied upon to losing security and administrative controls in cloud computing. It comprises transferring data to the cloud, it refers to losing control over location, redundancy and file system [9]. Service-level agreement (SLA) may not have guaranteed on cloud provider zone [10]. There is no proper SLA that is standard SLA's are not present in the cloud. Thus, the loss of governance problem was found.

2.3 Lack -In

Lack of security policy process could lead to vendor lock-in problem. This process would require to term the requirements for the cloud providers to certify they are able to assure that data migrated from the legacy provider [11]. But, the cloud user cannot transfer data from one service provider to another service provider. So to overcome this Application Programming Interface (API's) should be utilized, this should be identical. So anybody can utilize it on the cloud.

2.4 Data Loss or Leakage

Data loss or leakage, which means a data loss that occur in any device. Data loss happens when data may be logically or physically detached from the organization or user either unintentionally or intentionally [12].When the confidential information, for example, patient or customer data, design specifications or source code, intellectual property, price lists, trade secrets, budgets and forecasts are leaking out[13]. It is a negative impact on the cloud business environment. By protecting and encrypting the integrity of cloud data at the time transit is needed. Additionally, analysis of data encryption and production at both runtime and design should be done. In [14] introduced a novel UniversalSerial Bus (USB) memory bus for moving data safety in a cloud environment [15].

Table 1 shows the different types of cloud security category and the table 2 show the different types of Cloud Security Issues and Classifications

Table-1: Cloud Security Categories

NO	Category	Description
1	Security Standards	Defines the standards needed to take precautionary measures in the cloud computing so as to prevent attacks. It directs the policies of cloud computing for security without compromising reliability and performance.
2	Network	Consist of network attacks such as Denial of Service (DoS), Connection Availability, internet protocol vulnerabilities, DDoS,flooding attack, *etc.*
3	Access Control	Access control and Authentication and. It captures the issues that affect the privacy of user information and data storage.
4	Cloud Infrastructure	Attacks that are strict to the cloud infrastructure (IaaS, PaaS and SaaS) such privileged insiders and tampered binaries
5	Data	Data related security issues, including integrity, data migration, confidentiality, and data warehousing.

Table -2: Cloud Security Issues and Classifications

NO	Category	Issues
1	Security Standards	Absence of legal aspects (Service level agreement) Absence of security standards Compliance risks Trust Absence of auditing
2	Network	Network security configurations Appropriate installation of network firewalls Internet Dependence Internet protocol vulnerabilities

3	Access	Malicious insiders Service and Account and hijacking Privileged user access Browser Security Authentication mechanism
4	Cloud Infrastructure	Quality of service (QoS) Sharing technical flaws Insecure interface of API Multi-tenancy Reliability of Providers Server Location and Backup Security Misconfiguration
5	Data	Data location Data loss and leakage Data redundancy Data privacy Data protection Data recovery Data availability

3. DATAINTEGRITY AND DATA CONFIDENTIALITY

Data integrity and data confidentiality denote to the belongings that cloud data have not been destroyed or altered in an unauthorized way[35].The data outsourced and stored in the cloud environment because of the users do not have the sufficient physical storage for their data. But validating the exactness of the cloud storage data is a promising subject for cloud storage security.In order to get the cloud data integrity and data confidentiality in a cloud environment, in this survey intakes the concept of existing data integrity and data confidentiality. Different types of data integrity and data confidentiality based cloud security concept was implemented in the cloud storage as follows.Discuss different challenges faced by data encryption and access control mechanisms, in addition to, recent improvements to meet those difficulties of data confidentiality defense in cloud computing.

The author in [17] discusses the model based on Multi Agent Systems (MAS) architecture of cloud and the encoding mechanism of the data to improve the integrity of data centers. Multi Agent Systems (MAS) develop architecture for data integrity, which is available in the data centers and the data encoding is used to provide security. The system provides a better security for cloud storage located at different places, which is connected via high speed networks.

In the cloud there is no assurance that data stored in the cloud are secured or by using Third Party Auditor (TPA). So as to overcome this integrity of data issue, the user must be able to utilize the support of a TPA and it has tested the integrity of the data. This process is difficult to cloud owners. Thus, in [18] the author provides the integrity of data and proof that data whichsecuringthe storage by using a cryptographic key.

In cloud technology the cloud based services and service providers are progressed and caused in a new business trend. For upcoming computing techniques cloud has developed a conceptual and infrastructural procedure. The global computing infrastructure is frequently leads to the cloud based architecture. If the security is not strong and reliable, the flexibility and the merits that cloud computing deal with had some integrity. The author [19] represents a review of cloud computing concepts and the security issues which inherit inside the environment of cloud computing and cloud infrastructure. It is necessary to use the merits of cloud based computing by organizing it in expanded form and the security of a cloud based computing handles with involvement. The various cloud based services and the geographically isolated cloud service providers and the sensitive information of various process are being stored in remote servers and the cloud servers store the surplus process in the situation where the possibilities of the location is unprotected

Cloud computing is one of the IT services which provides a lease based network to the customers and to satisfy the requirements [20]. Cloud computing have some advantages like scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing helps the organization with an advanced business model to accepts the IT service without any investment. But the organizations are hesitating to accept the offer due to the lack of security and the challenges on it. Security is the main drawback of the cloud computing. It is annoying to transfer the important data from one organization to another. So the users need to understand the risk of security in cloud computing. This paper represents the detailed description of the security and the challenges

converging on the cloud computing types and service delivery types.

Cloud computing is developed in decades for the research of virtualization, distributed computing, utility computing, networking, web and software services. Cloud computing denotes a service oriented architecture which is used to reduce the measure of information technology to the end-user, flexible reduction of cost, provides required service and so on. The author [21] discuss the method of cloud computing in addressing the issues, related research topics and a necessity of cloud.

The cloud computing is an gradually well computing technique which has been derived from grid computing, parallel computing, virtualization technology, utility computing and other computing technologies. The main characteristics of the cloud computing are large scale computation, data storage, virtualization, high reliability and low cost. The security issues of cloud computing may prevent the hasty growth of cloud computing. This main aim of this paper [22] is to initiate the cloud computing systems and analyze the cloud computing security issues based on the cloud computing concepts and characters. The core security problem of the cloud computing technology is data privacy and the service availability. Many traditional and new technologies and strategies have to be used to protect the cloud computing system, the single security method cannot elucidate.

Cloud computing technology is used to raise the capability deprived of investing in new infrastructure, licensing new software or training new personnel. Cloud computing prolongs the surviving capability of information technology. It rapidly develops over the IT industries by being an auspicious business concept. The companies and the individuals are more concern about the security of the data stored in the cloud. The development of the cloud is increasingly popular even though the industries are still unwilling to deploy their data's in cloud [23]. The complication in data privacy and data protection were reducing the development of cloud computing and security is the main issue which dominates the growth of cloud. The introduction of the advance model is not satisfied with the requirement functionalities of current models in cloud computing. The new model is introduced to overcome the drawbacks of the existing model; it should not collapse various important features of the current model. The security of the existing technologies is posed by the cloud architecture when organized in a cloud environment. In this new environment, the cloud service users have to be cautious in knowing the risk factors. The author [24] proposes a survey of threats that presented in various cloud security risks. It represents the service delivery of cloud computing system and security issues.

Standard encryption methods are utilized to encrypt the data during processing, storage and transmission in the cloud. There are different types of algorithm are used such as Identity Based Encryption [35] [36],Key Policy Attribute Based Encryption [37] Ciphertext-Policy Attribute Based Encryption [38], Hierarchical Attribute-Based Encryption [39],hierarchical identity based encryption [40]. These encryption systems supporting"fine-grained access control over attributes" and "full delegation" respectively.The Different types of encryption schemes are compared and analyzed based on different parameters shown in table 3.

Table- 3: Different Types Of Security Schemes

Schemes	IBE	KP-ABE	CP-ABE	HABE	HIBE
Data confidentiality	Yes	Yes	Yes	Yes	Yes
Data Access control	Better than KP-ABE	Low	Average	Good	Lower than CP-ABE
Scalability	Yes	No	No	Yes	Yes
Data integrity	No	No	Yes	Yes	No
User revocation	Yes	Yes	Yes	Yes	Yes
Collusion resistance	Yes	Yes	Yes	Yes	Yes
Computation overhead	Lower than KP-ABE	High	Average	Low	High
Storage overhead	High	High	Average	Low	High

4. DATA AVAILABILITY AND DATA PRIVACY

As a various security measure, the data privacy and availability in cloud storage signifies to that the data are usable and accessible when authorized users needs them from any security machine at any time in the cloud. In an earlier stage of cloud computing, cloud data availability was more concern because the lack of reliable infrastructure and mature.Different types of data availability and data privacy based cloud security concept was implemented in the cloud storage as follows. Discuss different challenges faced by data encryption and access control mechanisms based on data availability and data privacy, in addition to, recent improvements to meet those difficulties of data availability and data privacy defense in cloud computing.

Cloud computing brings the new issue in the creating a reliable and secure data access and storage,it facility over unreliable or insecure service providers. Data storage integrity is one of the challenging tasks in the cloud. Thus, in [25] author proposes a novel approach for overcome this data integrity issue by using remote data integrity checking protocol, which is based on RSA and HLA signature with the support of public verification. This public verification creates the protocol very flexible. Since the user can direct the data prossession to check the TPA.

The computation world has been changed from centralized into distributed system and now it changes back to the virtual centralization which is known as cloud computing. The empire of the computation has been changed to the location of data and process. A client/customer can hold and control the data and the process of his/her computer in one hand. On the other hand, the client or the customer is unaware of where the process has been made and where the data's are store because, the service and the data maintenance were provided by some purveyor. From this we understand the client has no control on it. The internet is used as the communication media for the cloud computing. The purveyor has to provide some assurance in a service level agreement (SLA) about the security of cloud [26]. The Organization uses the cloud computing to examine the security and privacy issues for their business applications. The security of the cloud is still not reliable, so the purveyor has to provide various services like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a service (IaaS). Each service relies on its own security issues. So the SLA has to be provided based on every single service and explain the security policies which are implemented in their business. This paper helps the organization to know the issues of the cloud services and the security issues that have to be intimate in SLA.

Cloud computing empowers ubiquitous, user oriented, on-demand system access to a shared pool of configurable computing resources that can be quickly provisioned and discharged with limited management effort or service provider interaction. In cloud computing, creating a hook is completely surrounded by a combination of warm and cold air, likewise cloud computing gets an analogy which has an exact obstacle with the appropriate services of security and privacy issues. The author identifies the main issues which have a long-term process of the security and privacy issues.

The cloud computing gathers a big attention on infrastructure architecture, software delivery and development models. Cloud computing inherits the model of grid computing, utility computing and autonomic computing and encompasses it into a distributed architecture. The rapid development of the cloud concerns on a complex problems to identify the success of information systems, information security and communication. This paper is presented based on two processes, 1) to identify the unique security requirements based on the justification of cloud security. 2) To eliminate the potential threat by accepting the viable solution. This paper [27] introduces a trusted third party which risks with assuring specific security characteristics inside a cloud environment. The proposed system of cloud computing is cryptography, which particularly deals with SSO and LDAP, to confirm the authentication, integrity and privacy of data and communication.

Cloud computing has developed diversely with the versatile cloud services, so in order to share the data within a friend circle, the cloud computing environment is an efficient platform. But still it is inefficient concerning

with security. The features like Key freshness, Key authentication and the Key confidentiality are to be considered when the cloud utilizes the dynamic group key scheme to share the data. The Key Generation Center (KGC) that have the Dynamic Group key protocol distribute the keys to the members of the group and avoid the members who are not in the group. By using this process the above mentioned features are achieved. Because the cloud environment is not efficient in providing privacy, the access control has been a promising task ever. Hence, in this paper [28], a modification in the usual short group signature scheme is done in order to achieve the strongest access control. This proposed scheme provides the strongest data access and avoid the member list verification.

Numerous businesses are depending on the cloud computing that has the radical improvement in recent years. This is because of its smart features, namely low cost, flexibility, scalability and fast start-up. The cloud provides many services like rendering hardware and software to observe the security and various issues regarding the security. So it is necessary to use some algorithm to share the private data securely in the cloud [29]. The nodes in the cloud are assigned with an ID number and it is from 1 to N, this is the anonymous ID assignment technique. It improves the data stored in the cloud and becomes difficult for secure sharing. The ID assignment is done using the central authority. The proposed approach is evaluated along with the existing system and it is based on the Newton's identities and Sturm's theorem.

In [30] author suggested a third party auditing mechanism to authenticate the integrity of data. This process may help to access the whole data and this method guarantee the remote data integrity. But there are some issues like some process do not support the dynamic data or public audibility. Thus, this paper discuss all the aspects of current mechanism and also third party contribution which decides both dynamic and audibility data operations. In [31] it proposes some ideas under a Dynamic Multi-Replica Provable Data Possession scheme (DMR-PDP) that avoids the CSP from duplicitous; DMR-PDP also supports efficient dynamic operations like block insertion, modification and deletion on data duplications over cloud servers.

Cloud computing technology is one of the information systems which offered the service to the users on the web as rented base. The organization provides some services to scale-up and scale-down for their internal fundamentals [32]. Usually the purveyor makes the arrangement to provide cloud services. There are some major advantages in cloud computing like flexibility, efficiency, scalability, integration and cost reduction. The organization can deploy their application or run their operation through an advanced virtual space provided by the cloud computing technology. The organizations are hesitating to invest in cloud computing for the disregard of its services. This paper is used to review so many security issues and the tasks are discussed.

The cloud computing is known for its success and popularity which represents the new business and computing model. The cloud service provides features on on-demand services such as storage and bandwidth resources. The cloud computing is depending upon many technologies, business and medias. Cloud computing has a conflict in security from a long term and the main obstacles to the extensive use of cloud computing. The author [33] proposes briefly about the security concern which particularly exists on the cloud computing technique. The basic cloud concepts and the cloud security issues have been discussed. The cloud terminology was discussed in the case study of Amazon web services. The discussion of the current process and the future evolution has been made.

5. CONCLUSION

Cloud computing is a developing and auspicious way for data storage and data transmission. Security and privacy becomes the most significant issues against the radical growth of cloud computing. The data storage minimization and reduction in processing cost is essential for the any business, because data and information exploration is very significant for making decisions. So the business organization expects a strong trustworthiness between the business owners and the cloud service providers to transfer their data to the cloud. Numerous approaches and

techniques have been proposed for the same problem such as data security and protection in the cloud. But these techniques and approaches have to be more efficient and powerful, so that some necessary improvements have to be done with the portion of cloud computing, that the cloud service consumers should accept. In this paper, various approaches and techniques focusing on the data privacy and security on the data storage in the cloud are discussed where the trustworthiness between the consumers and the cloud service providers are made.

REFERENCES

[1]SwapnaLia Anil, Roshni Thanka, "A Survey on Security of Data outsourcing in Cloud",International Journal of Scientific and Research Publications, Vol. 3, Issue 2, 2013.

[2] Salve Bhagyashri, Prof. Y.B.Gurav, "A Survey on Privacy-Preserving Techniques for Secure Cloud Storage",International Journal of Computer Science and Mobile Computing,Vol. 3, Issue. 2, PP.675 – 680, 2014.

[3] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu, "Data Security and Privacy in Cloud Computing",International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages, 2014

[4] Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull, "Security Issues with Possible Solutions in Cloud Computing-A Survey",International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol.2, Issue 2, 2013.

[5] B.Tejaswi, L.V.Reddy, M.Leelavathi, "A Survey on Secure Storage Services in Cloud Computing", Global Journal of Computer Science and Technology Cloud & Distributed Volume 12 Issue, 0975-4172, 2012.

[6] Yinqian Zhang,Ari Juels, Michael K. Reiter, "Cross-VM side channels and their use to extract private keys",ACM conference on Computer and communications security,PP. 305-316,2012.

[7] BhruguSevak, "Security against Side Channel Attack in Cloud Computing",International Journal of Engineering and Advanced Technology (IJEAT), Vol-2, Issue-2, 2012.

[8] Aye Aye Thu, "Integrated Intrusion Detection and Prevention System with Honeypot on Cloud Computing Environment",International Journal of Computer Applications,Vol. 67– No.4, 2013.

[9] VinayakShukla,ShobhitSrivastava, Nidheesh Sharma, "Cloud Computing: Security Issues and Solutions",International Journal of Emerging Trends & Technology in Computer Science,Vol.3, Issue 5, 2014.

[10]Mitchell Cochran,Paul D. Witman, "Governance And Service Level Agreement Issues In A Cloud Computing Environment",Journal of Information Technology Management, Vol. XXII, Number 2, 2011.

[11] Grispos, G., Glisson, W.B., and Storer, T., "Cloud Security Challenges: Investigating Policies, Standards, and Guidelines in a Fortune 500 Organization", 21st European Conference on Information Systems, 5-8, 2013.

[12]BijayalaxmiPurohit,PawanPrakash Singh, "Data leakage analysis on cloud computing",International Journal of Engineering Research and Applications,Vol. 3, Issue 3, 2013.

[13]V. Shobana, M. Shanmugasundaram, "Data Leakage Detection Using Cloud Computing",International Journal of Emerging Technology and Advanced Engineering, Vol.3, Special Issue 1, 2013.

[14]Manas M N, Nagalakshmi C K, Shobha G, "Cloud Computing Security Issues And Methods to Overcome",International Journal of Advanced Research in Computer and Communication Engineering,Vol. 3, Issue 4, 2014.

[15] Tomoyoshi Takebayashi, Hiroshi Tsuda, TakayukiHasebe, RyusukeMasuoka, "Data Loss Prevention Technologies", FUJITSU Sci. Tech, vol.46, No.1, PP 47-55, 2010.

[16] Allen Oommen Joseph, Jaspher W. Kathrine, Rohit Vijayan, "Cloud Security Mechanisms for Data Protection: A

Survey", International Journal of Multimedia and Ubiquitous Engineering
Vol.9, No.9, pp.81-90, 2014.

[17]SatyakshmaRawat,RichaChowdhary,AbhayBansal, "Data Integrity of Cloud Data Storages (CDSs) in Cloud",International Journal of Advanced Research in Computer Science and Software Engineering,Vol.3, Issue 3, 2013.

[18]Saranya Eswaran, Sunitha Abburu, "Identifying Data Integrity in the Cloud Storage",International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, 2012.

[19] Monjur Ahmed and Mohammad Ashraf Hossain," Cloud Computing And Security Issues In The Cloud", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, 2014.

[20] Kuyoro S. O., Ibikunle F., Awodele O.," Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Vol.3, Issue 5, 2011

[21] Mladen A. Vouk,"Cloud Computing – Issues,Research and Implementations", Journal of Computing and Information Technology (CIT), 4, pp.235–246, 2008.

[22] Wentao Liu, "Research on cloud computing security problem and strategy", IEEE publication, pp.1216-1219, 21-23, 2012.

[23] S. Subashini, V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, Vol. 34, No. 1, pp. 1-11, 2011.

[24]WenjunLuo, GuojingBai, "Ensuring the data integrity in cloud data storage",International Conference on Cloud Computing and Intelligence Systems (CCIS), IEEE,240 – 243,15-17, 2011.

[25]B. R. Kandukuri, V. R. Paturi, A. Rakshit, "Cloud Security Issues," IEEE International Conference on Services Computing, 21-25 pp. 517-520, 2009.

[26] Jansen, W.A.," Cloud Hooks: Security and Privacy Issues in Cloud Computing", pp.1-10, 4-7, IEEE ,2011.

[27] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems, Vol. 28, No. 3, pp. 583-592, 2012.

[28] Dharani.R and M.Narmatha, "Secured Data Sharing With Traceability in Cloud Environment", International Journal of Inventions in Computer Science and Engineering, Volume 1 Issue 8, ISSN: 2348 – 3431, pp. 1-9, 2014.

[29] M. Divya Meena, AR. Arunachalam and T. Nalini, "Confidential Data Sharing With Anonymous Id Assignment Using Central Authority", International Journal of Inventions in Computer Science and Engineering, Volume 1 Issue 2, ISSN: 2348 – 3431, 2014.

[30]GauravPachauri, Subhash Chand Gupta, "Ensuring Data Integrity In Cloud Data Storage" International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.

[31] Barsoum, A.F, Hasan, M.A., "Integrity Verification of Multiple Data Copies over Untrusted Cloud Servers", IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), IEEE, 829 - 834 2012.

[32] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, Vol. 1, Hangzhou, 23-25, pp. 647-651, 2012.

[33] Patrick Mosca1, Yanping Zhang1, Zhifeng Xiao2, Yun Wang," Cloud Security: Services, Risks, and a CaseStudy on Amazon Cloud Services", Int. J. Communications, Network and System Sciences, 7, 529-535, 2014.

[34]Anandita Singh Thakur,P. K. Gupta, "Framework to Improve Data Integrity in Multi Cloud Environment",International Journal of Computer Applications, Vol. 87 – No.10, 2014.

[35] Zhang, F.; Li, Q.; Xiong, H.,"Efficient revocable key-policy attribute based encryption with full security", IEEE 8th International Conference on Computational Intelligence and Security 477–481,2012.

[36]Taeho Jung, Xiang-Yang Li, Zhiguo Wan,Meng Wan, "Privacy Preserving Cloud Data Access With Multi-Authorities",arXiv:1206.2657,Vol.6, 2013.

[37]Changji Wang, Jianfa Lu "An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length",Volume 2013, Article ID 810969, 7 pages,2013.

[38]Yi-mu Ji, Jie Tan, Hai Liu, Yan-peng Sun, Jia-bang Kang, Zizhuo Kuang, Chuanxin Zhao, "A Privacy Protection Method Based on CP-ABE and KP-ABE for Cloud Computing",Journal Of Software, Vol. 9, No. 6, 2014.

[39] Sai Krishna Parsha, Mohd.Khaja Pasha, "Enhancing Data Access Security in Cloud Computing using Hierarchical Identity Based Encryption (HIBE)",International Journal of Scientific & Engineering Research, Vol. 3, Issue 5, 2012.

[40] Guojun Wanga, Qin Liua, b, Jie Wub, Minyi Guoc, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers",Computers & Security, Elsevier journal,Volume 30, Issue 5, Pages 320–331,2011.

BIOGRAPHIES

Prof. B. Rex Cyril is working as Assistant Professor and pursuing doctor of philosophy in Department of Computer Science, St. Joseph's College,(Autonomous),Tiruchirappalli, Tamil Nadu, India. He received his M.Phil degree from Prist University. He received his MSc degree from St. Joseph's College, Tiruchirappalli. His area of interest is Cloud Security Services.

Dr. S.Britto Ramesh Kumar is working as Assistant Professor in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India He has published many research articles in the National/International conferences and journals. His research interests include Cloud Computing, Data Mining, Web Web Mining, and Mobile Networks.

