Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Data Security in Cloud Computing - Issues and Solutions to SaaS

B. BalaMurugan, D. Kamalraj
Department of Comp Sci. & Applications,
Rajiv Gandhi Arts & Science College, Puducherry,
India

M. Sugumaran
Department of Comp Sci. & Engineering,
Pondicherry Engineering College, Puducherry,
India

Abstract—Cloud computing is a more flexible, cost effective and proven delivery platform for providing business or consumer services over the Internet. Cloud computing supports distributed service oriented architecture, multi-users and multi-domain administrative infrastructure. So, it is more prone to security threats and vulnerabilities. At present, a major concern in cloud adoption is its security and privacy. Security and privacy issues are of great concern to cloud service providers who are actually hosting the services. In most cases, the provider must guarantee that their infrastructure is secure and clients' data and applications are safe, by implementing security policies and mechanisms. The security issues are organized into several general categories: trust, architecture, identity management, software isolation, data protection, availability reliability, ownership, data backup, data portability and conversion, multi platform support and intellectual property. This paper contains some of the techniques that were implemented to protect such data. A review was taken on different solutions of security issues towards the implementation of cloud computing.

Keywords— Cloud computing, data security, virtualization, data privacy

I. INTRODUCTION

The information technology environment has evolved from client-server, internet, virtualization, cloud computing to mainframes computers. Cloud computing provides a shared pool of configurable resources (e.g., processing, network, software, information and storage) on demand, as a scalable and elastic service, through a networked infrastructure, on a measured (pay-per-use or subscription) basis, which needs minimal management effort. This is based on service level agreements between the service provider and consumers, and often utilizes virtualization resources [16]. Cloud Computing services and products are based on an infrastructure of four core layers, namely, hardware (physical parts, i.e., servers and the network components), software (i.e., operating systems), virtualization resources (enabling pooling and sharing of computing resources) and applications (i.e., Salesforce.com and Google Apps). In this paper, the discussion about cloud computing is in four different sections. The first section is about the services of cloud computing and the different deployment models used to implement cloud computing. The second section is about how data are stored in cloud, and while, storing the data in cloud many issues arises. These issues are also discussed in this section. The third section is about the key data security concept, now these concepts helps in designing data security in cloud computing. The fourth section is about different solution, that are followed to implement data security in cloud computing. Finally in this paper, it is to conclude about the various discussion and implementation data security towards SaaS in Cloud computing

II. CLOUD COMPUTING SERVICES AND MODELS

The service developer creates, publishes and monitors the cloud based applications and services for use by both the cloud consumer and cloud provider. The Cloud services are in different way such as SaaS (Software as Services), PaaS (Platform as Services), IaaS (Infrastructure as Services), etc. The following are the three most widely used service models of cloud computing. [6], [7], [37], [41]. These cloud services implements in the different layer of web application as different cloud services such as in the following figure-1. [6], [8], [22], [36], [35], [37], [41], [45]. Software as a Service. (SaaS): It is also referred to as software available on demand; it is based on multi-tenant architecture. Software likes word processor, CRM (Customer Relation Management), etc., or application services like schedule, calendar, etc. are provided in the cloud computing using the interconnectivity of the internet to do manipulation on data [7], [22], [36], [37], [43].

Platform-as-a-Service (PaaS): This layer of cloud provides computing platform and solution stack as service. Platform-as-a-Service provides the user with the freedom of application design, application development, testing, deployment and hosting [7], [22], [36], [37], [43]. Infrastructure-as-a-Service (IaaS): Infrastructure as a service delivers a platform virtualization environment as a service. The client uses the third party infrastructure services to support its operations including hardware, storage, servers and networking components [36], [37], [22].

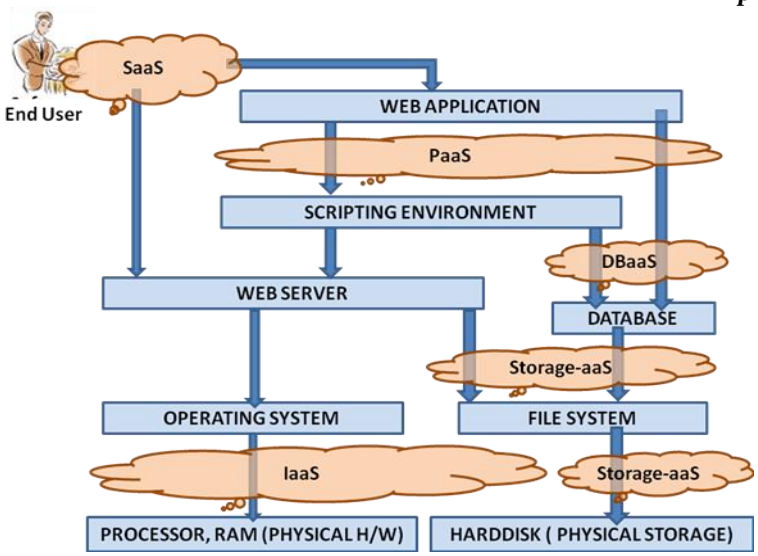

Fig -1 Different Cloud Service - Web Application

A. Cloud Deployment Models

There are four types of cloud deployment models that are widely used as public cloud, private cloud, hybrid cloud and community cloud [41]. Public: It is referred as external cloud or multi-tenant cloud computing model. This model represents an openly accessible cloud computing and in this environment, cloud computing can be accessed by the general public users. A customer can access resources and pay for the operating resources only. Public cloud computing can host individual services as well as a collection of services [11], [32]. Private: It is also known as the internal cloud or on-premise cloud. A private cloud provides limited access to its resources and services to consumers that belong to the same organization that owns the cloud. In other words, the infrastructure is managed and operated for one organization only so that a consistent level of control over security, privacy, and governance can be maintained [11], [32].

Hybrid: A hybrid cloud is a combination of public and private cloud. It provides benefits of multiple deployment models. It enables the enterprise to manage steady-state workload in the private cloud, and if the workload increases, it asks the public cloud for intensive computing resources, and then returns, if it is no longer needed [11], [32].

Community: This deployment model shares resources with many organizations in a community that shares common concerns (like security, governance, compliance, etc). It typically refers to special-purpose cloud computing environments shared and managed by a number of related organizations participating in a common domain or vertical market [11], [32], [42].

III. DATA SECURITY ISSUES IN THE CLOUD

Cloud computing implements three services such as SaaS, PaaS and PaaS to the end-user. In these services models different levels of security are provided in cloud computing environment. Efficient security technology in cloud computing is required to have proper secured cloud computing and to speedup cloud implementation. The consumers of service as infrastructure require inspecting confidentiality and security issues while implementing cloud. The SaaS model reduces the implementation cost for the customer's usage and to improve the efficiency of the cloud computing. In this work, it is about to discuss the SaaS security issues while implementing cloud. The security element in SaaS service model such data security, data integrity, identity management, data location, data availability, etc., as to be considered for better data security in cloud computing.

A. Data Security & Data Protection

Once the client hosts data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data [19], [35], [36].

B. Data Integrity

By providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to explain what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place, compliance issues. It may be necessary to have exact records as to what data was placed in a public cloud, when it occurred, what virtual memories (VMs) and storage it resided on, and where it was processed. When such data integrity requirements exist, the origin and custody of data or information must be maintained in order to prevent tampering or to prevent the exposure of data beyond the agreed territories (either between different servers or different networks) [3], [10], [36].

C. Data Location and Relocation

Cloud computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the cloud, they may want to know location where the data are stored safely. They may also wish to specify a preferred location (e.g. data in India). This requires a contractual agreement, between the cloud provider and the consumer that data should stay in a particular location or reside on a given known server [8]. Also, cloud providers should take responsibility to ensure the security of

systems (including data) and provide robust authentication to safeguard customers' information. Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decided by the cloud provider. However, it is often moved from one place to another place in-order to secure the data in cloud. Cloud providers have contracts with each other which are called as SLA (Service Level Agreement) and they use each others' resources [3], [8].

D. Data Availability

Customer data is normally stored in chunk on different servers often residing in different locations or in different clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult. So it is important for the provider to proper data availability to the authorized user [6], [35].

E. Identity Management

Each user uses his identity for accessing a cloud service. Thus, the provider should provide an identity management system for providing authentication and authorization. This is an important issue for both provider as well as user in a cloud computing environment [43]. But while providing authentication and authorization, an independent IdM stack, credential synchronization, federated IdM has to be implemented [12], [34]. Identity management and sign-on process are implemented towards identity of data in cloud computing [9], [36].

IV. KEY DATA SECURITY TECHNOLOGIES

In cloud computing, data is stored in the third party storage. Those organization who adopt cloud computing in the world, have carried out gradually the research of cloud computing security technology, to improve the security standards of cloud computing, and ensure that organization data and personal data security. Existing security technology more reflected in the following aspects in the research field and current implementation in the industries

- Data privacy protection:
- Proof of existence and usability of data:
- Trusted access control
- Retrieve and process of cipher text
- Cloud resource access control
- Trusted Cloud computing

A. Data privacy protection

Data privacy protection can make an anonymous data search engine, the two interactive sides can search the data from the other side and obtain the data they need. At the same time, the search contents are not known to the counter party, and irrelevant content will not be obtained during the search [8]. Data privacy protection is concerned with every phase of data life cycle in cloud computing. Roy [17] put centralized information flow control (CIFC) and differential privacy protection technology into the data generation and calculation stages. Privacy protection system which was named airavat, that can prevent disclosure of private data during map reduce, and can remove the key from the calculation results automatically [17]. In the data storage and using stages, Mowbray [25] proposed a client-based privacy management tool. It provided a user-centric trust model to help users to control the sensitive information stored and used in the cloud [12], [24], [25], [34].

B. Proof of existence and usability of data

Users cannot verify the correctness of data after download, as large-scale data tend to produce huge communication cost. Therefore, users have a high confidence level to determine whether the integrity of remote data, through some kind of knowledge proof protocol or probabilistic analysis tools in the case of retrieving very little data. While accessing the data in between user and the provider, much mitigation are processed in cloud [22]. Typical work includes the following: Provable Data Irretrievability (PDR) method that user-oriented independent verification, Provable data possess (PDP) method that publicly verifiable. PDI method that was proposed by NEC laboratory improves the processing speed and expands the scale of verification object of PDR method. PDI method also supports PDP. These methods greatly improve the data security of cloud computing [8], [14], [27].

C. Trusted Access Control

As service provider of cloud computing the implementation of user-defined access control policy cannot be trusted, the researchers concerned about how to access and control the data objects by non-traditional means of access control in the cloud computing model. The access control policy which received most attention is based on cryptographic methods. Include the following access control policy based on levels of key generation and distribution, attribute-based encryption algorithm, proxy re-encryption-based method, and methods that access control tree is embedded in the user key or cipher text, etc. Privileges revoked are an important issue of cryptographic-based access control policy. A basic solution is that a key is generated for set time duration. The key gets expiry after time duration and then the user updates a private key from the authority in a time intervals. [8], [20]. To obtain privacy preserving in trust negotiations in cloud computing, it has propose by two techniques based on the notions of substitution and generalization. This formulates the trust negotiation requirements in terms of disclosure policies is often restrictive. In this sense, the problem of trust negotiation requirements expressed as property-based policies. These relationships can be used by a credential requestor to motive about which policies should be uses in a trust negotiation to implement cloud computing [2].

D. Retrieve and process of cipher text

To enhance data security, you can turn the data into cipher text. But, many features lose when data was turned into cipher text. These lead most data analysis methods to failure [18], [35]. There are two typical methods to retrieve the

cipher text. First, there is a safety index-based approach which checks the existence of key words by establishing a secure cipher text key words indexing. Second, there is a cipher text scanning-based approach which confirms the existence of key words and count up the number of them by matching each word in the cipher text [21], [23], [24], [28].

E. Cloud resource access control

In the cloud computing, each cloud application belongs to different security management domain which manages local resources and users. Certification services are necessary to be set up at the domain boundary when users access to the shared resources across domains. It provides a unified certification and management of users' identity. Each domain has its own access control policy when users access to resources across multiple domains. Therefore, we must develop a public access control policy that both sides agree to share and protect the resources. Meanwhile, the synthesis of support policy is needed. Synthetic strategy not only ensures the safety of the new strategy, but also cannot go against the original access control policies of each domain, such as autonomy principle and safety principle [24].

F. Trusted Cloud computing

The trusted cloud computing was used in cloud computing to provide reliable cloud service has become a hot topic in the field of cloud security research. The trusted cloud computing platform which was named as TCCP in implementing cloud computing. Based on TCCP, IaaS service providers can offer their subscribers a closed execution environment, to ensure the confidentiality of the guest virtual machine running. In addition, it allows users to test whether the service provided by IaaS is secured before starting the virtual machine [34]. While the trusted data in cloud considered that trusted cloud computing can provide trusted software and hardware as well as trusted mechanism by implementing different algorithms, to prove their own behavior can be used to solve outsourcing data confidentiality and integrity. A reliable software token is developed. This token was bound with a security authentication module in order for the outsourcing sensitive (encrypted) data to perform various function operations under the condition not to disclose any information [33].

V. SOLUTIONS FOR DATA SECURITY IN CLOUD

Cloud computing data security refers to the set of procedures, processes and standards designed to provide information security of data in a cloud computing environment. Cloud computing data security addresses both physical and logical security issues across all the different service models. It also addresses how data security of these services are delivered (public, private or hybrid delivery model). While data of the customer need to be secured in cloud, both the data backup and data recovery methods should be efficient. The data recovery and backup process has various successful techniques. The techniques are lagging behind some critical issues like implementation of complexity, low cost, security and time related issues. These issues are proposed different and smart remote data backup algorithm and data recovery techniques.

The cloud provider should provide a proper strong encryption technique to protect the data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users for data safety [31]. The cloud seeker should be assured that data hosted on the cloud will be confidential. Towards data security, anonymity based technique for data privacy is implemented [12], [36]. Data security of cloud can be implemented in cloud computing by digital signature and encryption with elliptic curve cryptography [38], [40]. Client based privacy manager are implemented to data integrity, confidentiality and availability. While implementing data location and data segregation policy ranking based approach was used in cloud computing. Data hiding approaches are used in long-term viability of data in cloud. Fog computing implementation is for data security. CPABE (Cipher text policy attribute encryption is a mechanism for protecting the confidentiality of storing data and transmitting data information in external storage is required. Traditionally, encryption is viewed as a method for a user to share data to a targeted user or device [5]. These encryptions mechanism can also used in cloud computing to protect our data in external storage [8], [5], [18], [29], [41].

Ensuring data storage security in cloud computing is an important aspect of Quality of Service (QoS). An effective and flexible distribution verification protocol is required to address data storage security in cloud computing. This protocol rely on erasure code for the availability, reliability of data and utilize token pre-computation using Sobol Sequence [30] to verify the integrity of erasure coded data rather than pseudorandom data in implementing the cloud services. The cloud provider provides more security to user data stored in cloud computing. This analysis by Syam [30] is more secure than existing system against Byzantine Failure, unauthorized data modification attacks, and even cloud server colluding attacks.

The cloud services provided are facing different attacker to attack by SaaS, PaaS and IaaS. The data are gathered at one place in data centers in cloud computing, the DDOS attacks such as HTTP and XML in this environment is dangerous and provides harmful effects. These attacks can be resolved and detected by securing cloud from DDOS attacks using intrusion detection system in virtual machine [27]. This method solves the problem by a SOAP request makes the communication between the client and the service provider. Through the Service Oriented Trace back Architecture the SOAP request is send to the cloud. This architecture of service oriented trace back mark is present which contain proxy within it. This proxy marks the incoming packets with source message identification to identify the real client. The SOAP message is travelled via XDetector to monitors and filters the DDoS attacks such as HTTP and XML DDoS attack. Finally the filtered real client message is securely transferred to the cloud service provider [27], [43], [28].

The technique implied in PCS is convenient for data recovery totally based on parity recovery service. For data recovery, it generates a virtual disk in user system for data backup, make parity groups across virtual disk, and store parity data of parity group in cloud. It uses the Exclusive–OR for creating parity information. However, it is unable to control the implementation complexities [47].

HSDRT was also an efficient technique for the movable clients in cloud environment. This technique fails to manage the low cost for the implementation of the recovery and also unable to control the data duplication. The HSDRT is an innovative file back-up concept, which makes use of an effective ultra-widely distributed data transfer mechanism and a high-speed encryption technology. This proposed system follows two sequences one is backup sequence and second is recovery sequence. There are some limitations in this model and therefore, this model is somehow unable to declare as perfect solution for back-up and recovery [9].

In Linux, Box model [15] is having very simple concept of data back-up and recovery with very low cost. However, in this model protection level is very low. It also makes the process of migration from one cloud service provider to other very easy. This solution eliminates consumer's dependency on the ISP (Internet Service Provider) and its associated backup cost. It incorporates an application on Linux box that will perform backup of the cloud onto local drives. The data transmission will be secured and encrypted. A consumer can backup not only the data but sync the entire virtual machine which somehow waste the bandwidth because every time when backup takes place it will do back-up of entire virtual machine [15].

A smart remote data backup algorithm called as Seed Block Algorithm (SBA) [25]. This algorithm is twofold; first it help the users to collect information from any remote location in the absence of network connectivity and second to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason. The time related issues are also being solved by proposed SBA such that it will take minimum time for the recovery process. SBA also focuses on the security concept for the back-up files stored at remote server, without using any of the existing encryption techniques.

A different approach has discussed about the quandary of safeguarding privacy in trust consultation [47]. This approach initiates the notion of privacy preserving discovery, with a set that does not include attributes or credentials, or combinations of these, which may negotiate privacy. To obtain privacy preserving disclosure sets, it has proposed two techniques based on the notions of substitution and generalization in order data privacy in cloud.

In cloud computing, VGuard framework with efficient protocol that allows a cloud policy owner and a cloud request owner to collaboratively determine, whether the request satisfies the policy without the policy owner knowing the request and the request owner knowing the policy [1]. The basic idea of VGuard is to first convert a firewall policy to non-overlapping numerical rules and then use Xhash to check whether a request matches a rule. Comparing with the Cross-Domain Cooperative Firewall (CDCF) framework, which represents the state-of-the-art, VGuard is not only more secure but also orders of magnitude more efficient [1].

Therefore with these techniques and solution data in the cloud computing stored securely and retrieved, from the external storage. Although each one of the backup solution and retrieved data in cloud computing is unable to achieve all the issues of remote data back-up server. The advantages and disadvantages of all these techniques are described. Due to the high applicability of backup and retrieved process in the cloud providers and clients, the role of a remote data back – up server is very important and great challenges to the research.

VI. CONCLUSION

Cloud data security encompasses a broad range of security constraints from an end-user and cloud provider's perspective, where the end-user will primarily will be concerned with the provider's data security policy, how and where their data is stored and who has access to the data. For a cloud provider, on the other hand, cloud computing data security issues can range from the physical security of the infrastructure and the access control mechanism of cloud assets, to the execution and maintenance of security policy. Cloud security is important because it is probably the biggest reason why organizations fear the cloud. To overcome these fear data security is implemented in different ways to protect the data. In cloud computing, these issues towards data security and those techniques to overcome these issues will implement cloud computing as an efficient technology for the customer's data.

References

[1] Alex X. Liu and Fei Chen, (2011) Privacy Preserving Collaborative Enforcement of Firewall Policies in Virtual Private Networks, IEEE Transactions on Parallel and Distributed Systems 22:5, 887-895.

[2] Anna C. Squicciarini, Elisa Bertino, Elena and Indrakshi Ray, (2006) Achieving Privacy in Trust Negotiations with an Ontology-Based Approach, IEEE Transactions on Dependable and Secure Computing, 3: 1, 13-30.

[3] Balachandra, P.V. Ramakrishna and A.Rakshit (2009), Cloud Security Issues, IEEE International Conference on Services Computing, 517-520.

[4] Bhaskar Prasad Rimal, Eunmi Choi and Ian Lumd (2009), Taxonomy and Survey of Cloud Computing Services, Fifth International Joint Conference on INC, IMS and IDC, 44-51.

[5] Brent Waters (2011), Cipher text-Policy Attribute-Based Encryption: An Expressive, E-client, and Provably Secure Realization, 14th International Conference on Practice and Theory in Public Key Cryptography 2011.

[6] C.N. Hoefer and G. Karagiannis (2010), Taxonomy of cloud computing services, Proceedings of the 4th IEEE Workshop on Enabling the Future Service-Oriented Internet (EFSOI'10), 1345-1350.

[7] C.N. Höfer and G. Karagiannis (2011), "Cloud computing Services: Taxonomy and Comparison", J-Internet Server Applications, 81-94.

[8] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel and Muttukrishnan Rajarajan (2012), A Survey on Security issues and Solutions at different layers of Cloud computing, Springer Science Business Media,

[9] Chi-won Song, Sungmin Park, Dong-wook Kim and Sooyong Kang (2011), Parity Cloud Service: A Privacy-Protected Personal Data Recovery Service, Ttrust, security and Privacy in Computing and Communications (TrustCom) IEEE 10th International Conference.

[10] Christopher Jarabek (2011), A Review of Cloud Computing Security: Virtualization, Side-Channel Attacks, and Management.

[11] Nashaat el-Khameesy and Hossam Abdel Rahman (2012), A Proposed Model for Enhancing Data Storage Security in Cloud Computing System, Journal of Emerging Trends in Computing and Infom Sci 3:3 970-974.

[12] Arockiam, Parthasarathy and Monikandan S (2012), Privacy In Cloud Computing: A Survey, Proceeding of International Conference of Advanced Comp Sci & Information Technology (ACSIT 2012), 231-230.

[13] Fu Wen and Li Xiang (2011), The Study on Data Security in Cloud Computing based on Virtualization, IEEE Proceeding,

[14] G.Ateniese, R.Burns, R.Curtmola, J.Herring, L.Kissner, Z.Peterson and D.Song (2007), Provable Data Possession at Untrusted Stores, In Proceeding of the 14th ACM Conference on Computer and Communications Security (CCS'07). 598–609.

[15] Giuseppe Pirr´o, Paolo Trunfio , Domenico Talia, Paolo Missier and Carole Goble (2010), A Semantic-based System for Service Discovery in Distributed Infrastructures, 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing.

[16] HsinYi Tsai (2012), "Threat as a Service? Virtualization's impact on Cloud Security", IT Professionals 14:1 32-37.

[17] I.Roy, H. Ramadan, S. Setty, A. Kilzer, V. Shmatikov, and E. Witchel (2012), Airavat: Security and Privacy for MapReduce, Proceeding of the 7th USENIX Conference on networked System Designed and implementation (NSDI).

[18] K.S.Suresh and K.V.Prasad (2012), Security Issues and Security Algorithms in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering 2:10 110-114.

[19] Kaufman, L (2009), Data security in the world of cloud comp, Security & Privacy, IEEE proceedings 7:4 61-64.

[20] Leu FY, Lin JC, Li MC, Yang CT and Shih (2009), Integrating grid with intrusion detection, In Proceedings of the 19th international conference on advanced information networking and applications 1:1 304–309.

[21] Mandeep Kaur and Manish Mahajan (2013), Using encryption Algorithms to enhance the Data Security in Cloud computing, International Journal of Communication and Computer Technologies 12:3 56-59.

[22] Mariana Carroll, Alta vander Merwe and Paula Kotzé (2011), Secure Cloud Computing, Information Security South Africa (ISSA), 1-9.

[23] Md Kausar Alam and Sharmila Banu K (2013), An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds, International Journal of Scientific and Research Publications, 3:4.

[24] Mohit Marwaha and Rajeev Bedi (2013), "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science, 10:1, 366-370.

[25] Mowbray M and Pearson S (2013), A client-based privacy manager for cloud computing, In Proceedings of the fourth international ICST conference on communication system software and middleware, 1–8.

[26] Kruti Sharma and Prof. Kavita R Singh (2013), Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing, 2013 International Conference on Communication Systems and Network Technologies, 376-380, 2013.

[27] Asha.D and R.Chitra (2013), Securing cloud from ddos attacks using intrusion detection system, IJREAT International Journal of Research in Engineering & Advanced Technology, 1:1, 20-28.

[28] Nagaraju Kilari and Dr. R.Sridaran, (2012), Survey on Security Threats for Cloud Computing, International Journal of Engineering Research & Technology.

[29] Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, Tereza Carvalho, Mats N¨aslund and Makan Pourzandi (2012), A quantitative analysis of current security concerns and solutions for cloud computing, Journal of Cloud Computing: Advances, Systems and Applications, 1:2 1-6.

[30] P. Syam Kumar, R.Subramanian and D.Thanizh Selvam (2010), Ensuring Data Storage Security in Cloud Computing using Sobol Sequence, Proc. of PDGC-2010, IEEE.

[31] Parsi Kalpana and Sudha Singaraju (2012), Data Security in Cloud Computing using RSA Algorithm, International Journal of Research in Computer and Communication technology, 1:4 1- 12.

[32] Prashant Srivastava and et al, " An architecture based on proactive model for security in cloud computing", IEEE-International Conference on Recent Trends in Information Technology, pp.661-666 2011.

[33] Priyanka Arora, Arun Singh and Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment" World of Computer Science and Information Technology Journal (WCSIT), Vol.2, pp.179-183, 2012.

[34] Rizwana Shaikh and M. Sasikumar, "Security Issues in Cloud Computing: A survey", International Journal of Computer Application, Vol.4, No.19 , pp.4-10, 2012.

[35] Sharma, Sonika Soni and Swati Sengar, "Security in Cloud Computing", National Conference on Security Issues in Network Technologies types and security issue and approaches to secure data in cloud, pp.1-6, 2012.

[36] Subashini and Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol. 34, No 1, pp. 1-9, 2010.

[37] Vaquero, Rodero-Merino, Caceres and Lindner, "A break in the clouds: towards a cloud definition", ACM SIGCOMM Computer Communication, Vol. 39, No.1, 2009.

[38] Veerraju Gampala, Srilakshmi Inuganti and Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE), Vol.2, No.3, 2012.

[39] Vijaykumar and Javaraiah Brocade, "Backup for Cloud and Disaster Recovery for Consumers and SMBs", IEEE 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS), pp.1-3, 2011.

[40] Vikas Kumar Swetha M.S, Muneshwara M.S. and Prof Prakash S, "Cloud Computing: Towards case study of Data Security Mechanism", International Journal of Advanced Technology & Engineering Research (IJATER), Vol.2, No.4, 2012.

[41] Wang Jun-jie and MuSen, "Security Issues and Countermeasures in Cloud Computing", IEEE International Conference on Grey Systems and Intelligent Services (GSIS), pp.483-846, 2011.

[42] Wang.C, Ren.K, Lou.W and Li.J, "Toward publicly auditable secure cloud data storage services", IEEE proceeding Network, Vol.24, No.4, pp. 19-24, 2010.

[43] Wayne A. Jansen, "Proceedings of the 44th Hawaii International Conference on System Sciences", pp.1-8, 2011.

[44] Xiangyang Luo, Lin Yang, Linru Ma, Shanming Chu and Hao Dai, "Virtualization Security Risks and Solutions of Cloud Computing Via Divide-Conquer Strategy", Third International Conference on Multimedia Information Networking and Security, pp. 637-641, 2011.

[45] Xue Jing and Zhang Jian-jun, "A Brief Survey on the Security Model of Cloud Computing", Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science, pp.475-478, 2010.

[46] Y.Ueno, N.Miyaho, and S.Suzuki, "Disaster Recovery Mechanism using Widely Distributed Networking and Secure Metadata Handling Technology", Proceedings of the 4th edition of the UPGRADE-CN workshop, pp. 45-48, 2009,

[47] Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki,Muzai Gakuendai, Inzai-shi, Chiba,Kazuo Ichihara, "Performance Evaluation of a Disaster Recovery System and Practical Network System Applications," Fifth International Conference on Systems and Networks Communications, pp.256-259, 2010.

