A Review of Data Security and Privacy Issues over SaaS

Pradeep Kumar Tiwari
Computer Science and Engineering
Manipal University
Jaipur, India
pradeep.tiwari@muj.manipal.edu

Sandeep Joshi
Computer Science and Engineering
Manipal University
Jaipur, India
sandeep.joshi@jaipur.manipal.edu

***Abstract*— Cloud computing is an emerging computing technology over internet. Cloud service providers provide best use and utilization of resources by service models. Cloud computing cost and service make very popular among cloud user. Data security and privacy is main issue because of its dependence on cloud provider. SaaS service model provides many features but it still has some lack of security mechanism. In This paper we are discussing about lack of security mechanism and possible solution's which are already available. This paper would be helpful for elaborate study of SaaS security, vulnerabilities and security threats.**

Keywords*— *Security, SAML (Security Assertion Markup Language), SSL (Secure Socket Layer), TLS (Transport Layer Security).

I. INTRODUCTION

In new computing paradigm cloud computing is most popular and cost effective computing web service which provide three service models SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). Cloud computing offering cost effective world wide access processing and large scale data storage capabilities. The major cloud service providers are Google, Amazon AWS, Microsoft, salesforce.com, IBM and HP. Cloud computing provides internet based computing services so security concern is most important issue in Information Technology (IT) system. Security is not only major issue in cloud computing but also security in distributed computing, grid computing, scientific application, military, government, corporate systems and applications where we are using network based computing [17].

Cloud computing security can be specify in different categories like physical security, network security, IT system (system security), information (data security) and application security. Security responsibility ensure from both side client side and server side. Amzon AWS EC2 offering responsibility for security up to hypervisor, physical security, environmental security and virtualization security. Salesforce.com customer resource management (CRM) SaaS offering security responsibilities in physical and environmental security control. It also ensures the security control over on the infrastructure, application and data.

In all over worldwide many countries fallow rules and regulations for protecting the data and secure the information. These countries are Japan, Australia, New Zeland, Asia specific and many more they are using data protection laws. They are fallow privacy security guideline of the OECD (Organizations for Economic Cooperation and Development) and the APEC (Asia Pacific Economic Cooperation) and EEA (European Economic Area) [14].

Service provider provides several new security trends but they are still not providing full robust security mechanism. Data security is still major challenge to researcher. Researchers continuously doing research to secure data over the network but they are facing many major technical challenges to completely secure the cloud network and cloud storage [12], [17]. Protection of sensitive data and storage data during the transmission of information or accessing the data from cloud is widely using technology is cryptography [12], [13].In this paper we are broadly discussing protection of data over SaaS (Software as a Service). SaaS user can understand different security aspect in SaaS service.

SaaS (Software as a Service)- According to NIST (National Institute of Standards and Technology) Customers can access provider applications from cloud infrastructure with the help of interface. This interface may be the web browser (e.g. email, games). All services like management of infrastructure. Server, Storage, Operating System all are managed by cloud provider. Customers no need to worry about any management [53].SaaS service providers the capability of using applications over cloud. In outsourcing of information technology data moves over the internet. Security and privacy of data at the particular time when moving the data or application from one computing centre to another computing centre become critical. SaaS service providers are mainly held responsible for data security.

II. CHALLENGES IN SAAS SECURITY

In SaaS model clients are totally depend on the service providers. Cloud clients don't know the technical security issues and security measurement which are necessary for data security. Service providers give the assurance, client data always be secure during multi-tenancy live migration and isolation no one cannot see the other user's data. Most

978-1-4799-3975-6/14/$31.00 ©2014 IEEE

impotent to client to know right security measures and availability of data in secure way when he need [4], [44]. Service providers provide the new update version of software then exist new one. Service provider is not only focusing the portability of the application but also enhancing the security mechanism with data integrity [44],[54]. The SaaS software vendor may host the application on its own private server or deploy it on a cloud computing infra-structure service provided by a third-party provider (e.g. Amazon, Google, etc.) [4]. Moving of data and application in an external cloud environment create the breach and extend security risk. This risk may be or may not be generated bt service provider staff or other clients who are using SaaS service [46].

The main security problems in SaaS

A. Data Security and Backup

SaaS vendor should be ensure to his client, sensitive data always be on regular backup mode with the facility of quick recovery in case of any kind of disaster (intensely or accidently). Provider also uses strong security mechanism like encryption to protect the stored backup data to prevent fraud illicitly or accidental theft of sensitive information [4]. The data protection Act defines the area of sensitive data. Sensitive data can define by either client or service provider or both can decide. If data is sensitive that time apply the Act of prohibition with legal law. Laws of protection data many times very useful but many times they are not effective because laws change after international boundaries [2], [14]. ENSIA (European Network and Information Security Agency) is responsible for achieving network and information security with the three main object, policy and organization, technical and legal issues [39]. NIST define the type of services rather than implement solution and doing work understand of cloud internal operations and threats.

When a loss occurs that necessitates the recovery of operative data, the time period required for it is a key parameter. When data is loss that time it ensures that only loss data is recovered or all data is recovered. The actually meaning of data recovery is recovery of the entire data file [2].Currently the main problem in data protection is cryptography management failures. Management of key and interchange of key between user and service provider. Only few methods are practically effective still need many works over data security via cryptography [46], [50].

Service provider includes the robust encryption features and authorization system to control the unauthorized access of data. Security of data issue is above all [9]. A number of storage systems are available for storing data share data from common storage system. NAS (Network Attach Storage), SAN (Storage Area Network), Object Storage technologies are available used to store data. [5].

The users want his data separately encrypted and vendors give backup of his sensitive information this information not be theft and tampered by unauthorized person. Client wants separate treatment to his information while service uses by multi users at a time [7].

B. Data Integrity

Data integration means protecting the data from unauthorized access, deletion, and modification from the intruder and gives assurance to secure data transmission from source to destination. Service Provider must ensure that data will transmit in a secure system and data always remain actual [1], [40]. Data is always identically managed and maintain during integration operation such as synchronization of data between on location and SaaS system [1].

Data transaction system must follow ACID (Atomicity, Consistency, Isolation and Durability) properties to ensure data integrity. Most of the data base uses ACID properties to secure data transaction and maintain data integrity. Each SaaS application have different level of data availability it also depend in SLA (Service Level Agreement)[4]. Many standards and authorizations are available to managing data integrity and security with web service such as WS-Transaction and WS-reliability [9][10]. SaaS solution uses open, standard based APIs link to on-site system. This makes integrations simple, fast, and cost-effective [8].

Zetta is a system that is mainly focused on data integrity for Cloud services it provides similar idea to RAID system. Zetta provides Zetta system which considering on the data integrity in on demand storage system with assurance of data integrity and back up of data in any critical circumstances. Zetta Corporation mainly dedicated to data integrity in on demand service [19], [20], [21].

C. Data Locality

The most common compliance issue facing by the organization is data location. Clients want to know detail where his database is actually stored and which security mechanism, safe guard method and certification method is using to protect the data and where data relocate. Once information crosses the national borders then difficult to protect the data because rules and regulations of data protection change according to local rule of country where the data locate [46][51],[52].

Amazon has its EC2 in multi-locations, and currently one in USA and the other in Europe. Google App Engine locates in many countries (i.e., it has 36 data centres across the world), such as USA, China, and so on [19]. Ask to service providers if they committed to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers [41].

D. Data Segregation

Data of multiple users will locate at the same server location so interferences of among the clients are. Multi user environment breaches give the chance to intruder to hijacking data during the application access or accessing the client code to the SaaS system [4].

SaaS provider should ensure separate segregation of data physical level and application level. SaaS service must be

intelligent enough to isolate the data from different users. In the case of Amazon, the S3 APIs provide both bucket-level and object-level access controls [44].

The cloud provider should provide highly secured encryption schemes and tested by skilled specialists [41]. Sometimes users' data running in single physical machine with the many VM instances at this time SaaS provider give the proper user authorization and administrative task with secure way. Data should be transfer and store in controlled approach. Providers fallow the available protocol standard and security standard for secure data transmission. Best suited cryptography system with the practical approach fallow by the service provider to make a trust relation with the SaaS users [46],[50].

E. Data Access

The SaaS model alwayes be flexible enough to incorporate the specific policies put forward by the organization [4].

Kan Yang and Bo Zhang give the data access idea with security mechanism this proposed solution is calls DAC-MACS (Data Access Control for Multi-Authority Cloud Storage). Both are proposed effective and safe data access control policy in multi-tenancy and multi-authority cloud storage environment. Both researchers proposed multi-authority CP-ABE decryption scheme by using token based decryption method [32]

F. Data Avilability

The SaaS service providers ensure that data will be available 24*7 days without any interruption. Cloud architecture need to adopt effective load balancing mechanism during the processing of data. Architectural and infrastructural changes are required to achieve scalability and accessibility of data with effective response time [7].

Amazon AWS API hosted the retail site amzon.in. Amazon provides the retail services to multiple customers and same time provide multiple features with multi-tenant environment [4].

G. Data Confidentiality Issue

Confidentiality refers to the security of intended and unintended illegal access of information. Users have rights to know information will be secure form theft. May be another client change the security setting illicitly or maliciously. SaaS service provider provides robust security mechanism. This security mechanism should be certified by third party [44][45]. ECPA (Electronic Communication Privacy Act) Act of 1986 provides protection against illegal access of electronic mail or other information of users. ECPA gives the many privacy protection law to security and confidentiality of user data [4].

H. Authentication

In SaaS service, application service is hosted outside of the corporate firewall. Many times users use the application service but other use the same account with the already verified account. SaaS customer must remove or disable account of his employee who left the company and provide new user ID password for new joined employee [4]. SAML (Security Assertion Markup Language) and WS (Web Service) Federation are widely used with SAML being more popular .The alternative to SAML and WS Federation is a SSO (Single Sign On) solution that is deployed via a secured VPN (Virtual Private Network) tunnel. The widely used SAML standard is often used in versions 1.1 and 2.2 .Where possible SAML 2.0 should be supported because various proprietary upgrades have been integrated into this standard, enabling the addressing of a broad base of deployment scenarios [5].

I. Authorization

Authorization is the mechanism which is determines the level of an accessed particular user. Service provider should have secure resources to check authorization of the user and validate him by a secure mechanism with controlled manner [40]. The access control should be managed according to role of users. Authorization for access data secure in different level basis on clients hierarchy access policy and policy is reviewed on specific time period. In general, the least privilege model should be used, with users and CSP (Content Security Policy) administrators only possessing the rights that they require to achieve their tasks [5].

In February 2011, OMB responded in several issues, which references the proper establishment of a shared assessment and authorization process for cloud computing [35]. WS Federation provides a special type of STS (Security Token Service) that makes authorization decision. Digital identities may be the identical authorization mechanism to identify the authorized person this identity may based on an e-mail address or machine's unique IP address. A digital signature may be the also a good authorization technique to indentify the actual user this cryptography mechanism is a best suited method for authorization. [55].

J. Network Security

Network is a medium to access SaaS services from cloud system. Network attract to hacker with his vulnerabilities and its open the window to intruder to attack on cloud services to theft the information from cloud storage [19].

SaaS service provider must implement strict regulation for data protection from any type of manipulation, theft and illicit access of data. Only cryptography is best suited mechanism for user authorization but it should be certified by security service providers [2]. Service provider provide robust encryption technique such as SSL (Secure Socket Layer) and TLS (Transport Layer Security) techniques for data access and data security over the network [7]. Amazon web service provide strong security mechanism over the traditional network security issue for example MITM (Man in the Middle) attacks, IP spoofing, Port scanning, packet sniffing etc. Amazon S3 provides maximum possible security services. Process via SSL encrypted endpoint ensures that data is transferring by secure way. It ensures that data are passing in

secure way [4]. User can connect to an AWS access point via HTTP or HTTPS using SSL mechanism to protect against data theft, tampering and message forgery [11]. Security measures provide secure IDS/IPS firewall protection to protect to spyware, malware, versus and Trojan attack [5].

K. Virtualization

Virtualization is a concept and component of cloud. It do the work as middleware between server and users and give the features of server virtualization, multi-tenancy, data isolation and resources managements. Real time challenges, multi-tenancy, load balancing and live migration make the effective to virtualization but these are also gives attack threats to attacker like VM escape, VM hopping and sniffing/Spoofing of virtual network [54]. These benefits give vulnerabilities and security threats to hackers to do the attack over VM middleware for accessing data and resource or destroy services features.

Enforcement of security mechanism in virtual machine is difficult task. In virtualized environment, many instances run simultaneously. Multiple guests can run different application and different operating system on a single host computer and provide isolation between the different users access. Virtualization allows users to create copy, share, migrate, and roll back virtual machines, which may allow them to run a variety of applications [36], [37], [38].

The other issue is the control of administrator on host and guest operating systems. Current VMMs (Virtual Machine Monitor) do not offer perfect isolation of machine and data[4]. Xen an open source x86 VMM, incorporates a modified Linux kernel to implement a privilege partition for input/output operations and KVM (Kernel-based Virtual Machine) another source effort transforms a Linux kernel into a VMM [46,47,48,49]. Multi tenancy is difficult to manage in virtual machine. Resources and information share between multiuser that time attacker can access the information .It is also challenging to AWS EC2 network how can handle multiple user account domain name ,service type and assigning multiple IP address to indentify to all as an individually [11] .

*v*IDS/*v*IPS (Virtual Instruction Detection System and Virtual Protection System) protects virtual environment through collect and analyse processing information between network to host after that detect the malware and spyware code from the processed information. *v*IDS/*v*IPS monitor and analyse the virtual network configuration , network loop holes and ensure the security policies to protect the information and gives assurance of unbreakable security policy with secure transaction [29].

Hamid Banirostam , Alireza Hedayati proposed a TCCI (Trusted Cloud Computing Infrastructure) to ensure confidentiality and accuracy of computing which is assigned to access software services in secured virtualized environment [31]. Research on virtualization management and security of virtualized environment is still in progress, researchers are doing continuously work for enhancing performances and security.

L. Encryption

Data process in secure way cloud providers use the cryptography method. When the data transport on the network that time cloud provider should use cryptographic method and product for secure transmission of data. The cryptographic key management is complex in cloud computing environment and at present no appropriate tools are available for key management [5]. SSL technique is using by SaaS service provider for making the encrypt connection between application and user data base instance. RDS creates an SSL certificate and install the certificate on the DB instance when instance is provisioned for MySQL and SQL Server [11]. During the sharing of data in multi-tenant environment need to be highly scalable encryption mechanism to protect resources and data [15]. Encryption methodology have key major aspect to solve the problem (a) an efficient secure comparison mechanism (b) an efficient encryption delegation mechanism (c) an efficient decryption delegation mechanism (d) computation over encrypted/authenticated data [17], [18].

Purushothama B R and B B Amberker proposed five algorithms for data security Algorithm 1: Setup, Algorithm 2: Pre-processing and Outsource, Algorithm 3: Query Pre-processing and Querying Phase, Algorithm 4: Query Processing and Response Phase, Algorithm 5: Query Post processing and Result Phase. These provide an improved query processing scheme over encrypted data [30].

Kan Yang, Xiaohua Jia,, Kui Ren, Bo Zhang data access idea with security mechanism this proposed solution is calls DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme for multi-authority cloud storage systems. They also proposed construct a new multi-authority CP-ABE (Ciphertex Policy Attribute-based Encryption) scheme with efficient decryption [32].

Sahai and Waters introduced the first ABE scheme (Attribute-based Encryption) [32], [33], Kan Yang, Xiaohua Jia,gives analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model. Our attribute revocation method can efficiently achieve both forward security and backward security [34].

Cryptography methodology is one the most method to secure data transportation but still it has some lack of security mechanism. It not gives 100% assurance of data security. Many work already done in the filled of cryptography and key management technique but still now need lots of work in cryptography methodology [30]. Cloud storage providers don't give the security information to his client to maintain his reputation in cloud market. Security such as forgery attack, replace attack and data leakage are problem in data security. Cloud storage system should be inbuilt with SSL and TCCP service [55].

III. CURRENT SOLUTION SCHEME PROVIDERS, ACT AND CERTIFICATE

Cloud Cube Model also highlights the challenges of understanding and mapping cloud models to control frameworks and standards such as ISO/IEC 27002, which provides "a series of guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization [14]." CSA is an organization led by a coalition of industry practitioners, corporations, associations and other stake holders [15], [16], NIST also issued a draft publication on cloud computing, SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, which addresses the security concerns associated with data center operations and the division of responsibilities among providers and customers [35]. IBM developed a fully homomorphic encryption scheme in June 2009. This scheme allows data to be processed without being decrypted [42], [43].

IV. CONCLUSION

SaaS service model is application based computing concept that gives several benefits with less cost. This is most popular service among all cloud services. SaaS service model growth is moving ahead day by day but it has many security issues. Cloud provider provides some security solution with certificate and many organizations are working for security issue. In this paper aims to signify different security problem in SaaS service. This paper represents the traditional and new security problem and current available solutions. Privacy concern should be change time to time as user requirement. Investigating the problem of data security, integrity, and data segregation, data location, virtualization and encryption method and current available solutions are mentioned in this paper. Paper helps to understand security problem and present solution to researchers. Robust data security solution is not available in SaaS service researcher are continuously doing research in this field. SaaS technology is still developing because there are many security issues need to resolve. Some methods, certification and organization are doing work actively but these are not enough to secure data.

REFERENCES

[1] David S. Linthicum, "Approaching SaaS Integration with Data Integration Best Practices and Technology,",White Paper 2009.

[2] Paul Meinl , "Software as a Service – Correct Conclusion of Contracts 2nd enhanced edition, IT Cluster Vienna | Cloud Computing Group,".

[3] "Security and SaaS , WHITE PAPER by webandflow" 2013

[4] Subashini, Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of Network and* Computer Application 34.1(2011):1-11., www.elsevier.com/locate/jnca.

[5] "Security Recommendations for Cloud Computing Providers," White Paper, Federal office of information security.

[6] " Seven Criteria for Evaluating Security-as-a-Service (SaaS) Solutions, A Websense,"White Paper .

[7] " Securing SaaS Applications: A Cloud Security Perspective for Application Providers, "Leo TechnoSoft Pvt Ltd.

[8] "Smart Questions For Your Saas Vendor," A SAManage eBook,

[9] Kumar, Prashant, and Lokesh Kumar. "Security Threats to Cloud Computing."International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) Volume 2, No. 1, December 2013,

[10] Subashini, Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of Network and Computer Applications Vol 34, pp. 1-11, 2011.

[11] "Amazon web service: Overview of Security Process," November,http://aws.amazon.com/security.

[12] PENG, Yong, Wei ZHAO, Feng XIE, Zhong-hua DAI, Yang GAO, and Dong-qing CHEN. "Secure cloud storage based on cryptographic techniques." *The Journal of China Universities of Posts and TelecommunicationsVol* 19, pp. 182-189. 2012.

[13] Tang, Yang, Patrick PC Lee, John CS Lui, and Radia Perlman. "FADE: Secure overlay cloud storage with file assured deletion." In *Security and Privacy in Communication Networks*, pp. 380-397. Springer Berlin Heidelberg, Security Guidance for Critical Areas Of Focus In Cloud Computing V3.0, Cloud Security Alliance,2010

[14] Gonzalez Nelson, Miers Charles , Redıgolo Fernando , Simplıcio Marcos, Carvalho Tereza , Naslund Mats , and Pourzandi Makan ,2012. A quantitative analysis of current security concerns and solutions for cloud computing ,A Journal of Cloud Computing: Advances, Systems andApplications2012,1:11

[15] "CSA , About. https://cloudsecurityalliance.org/about" 2011.

[16] " Security for Cloud Computing, Report to the National Science Foundation Directorate for Computer and Information Science and Engineering (CISE)," Arlington, Virginia , March 15-16, 2012.

[17] Ma D.,"Cryptographic Approach for Delegation and Authorization in Cloud Computing, " Presentation at NSF Workshop on Security for Cloud Computing, March 14-16, 2012.

[18] Zhou, Minqi, Rong Zhang, Wei Xie, Weining Qian, and Aoying Zhou. "Security and privacy in cloud computing: A survey." In Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on, pp. 105-112. IEEE, 2010.

[19] Zetta, "Zetta: Enterprise cloud storage on demand,"http://www.zetta.net/, 2008.

[20] Chen, Peter M., Edward K. Lee, Garth A. Gibson, Randy H. Katz, and David A. Patterson. "RAID: High-performance, reliable secondary storage." ACM Computing Surveys (CSUR) vol. 26, no. 2, pp. 145–185, 1994.

[21] Burnside, Russell S. "Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies The," Rutgers Computer & Tech. LJ,vol. 13, p. 451, 1987.

[22] Cao, F., H. K. Huang, and X. Q. Zhou. "Medical image security in a HIPAA mandated PACS environment." Computerized Medical Imaging and Graphics27, Vol no. 2, pp 185-196,2003.

[23] Act, Fair Credit Reporting. "Fair Credit Reporting Act." Flood Disaster Protection Act and Financial Institute, 2009.

[24] EPIC.org,"Video Privacy Protection Act," http://epic.org/privacy/vppa/.

[25] Akhigbe, Aigbe, and Ann Marie Whyte. "The Gramm-Leach-Bliley Act Of 1999: Risk Implications For The Financial Services Industry."Journal of Financial Research , vol. 27, no. 3, pp. 435–446, 2004.

[26] Mahmood, Zaigham. "Data location and security issues in cloud computing." InEmerging Intelligent Data and Web Technologies (EIDWT), International Conference on, pp. 49-54. IEEE, 2011

[27] "Google Apps Service Level Agreement, " www.google.com/apps/intl/en/terms/sla.html , November 2010.

[28] Luo, Shengmei, Zhaoji Lin, Xiaohua Chen, Zhuolin Yang, and Jianyong Chen. "Virtualization security for cloud computing service." In Cloud and Service Computing (CSC), 2011 International Conference on, pp. 174-179. IEEE, 2011.

[29] Purushothama, B. R., and B. B. Amberker. "Efficient Query Processing on Outsourced Encrypted Data in Cloud with Privacy Preservation." In Cloud and Services Computing (ISCOS), International Symposium on, pp. 88-95. IEEE, 2012.

[30] Banirostam, Hamid, Alireza Hedayati, Ahmad Khadem Zadeh, and Elham Shamsinezhad. "A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure." In Computer Modelling and

Simulation (UKSim), UKSim 15th International Conference on, pp. 717-721. IEEE, 2013.

[31] Yang, Kan, Xiaohua Jia, Kui Ren, and Bo Zhang. "Dac-macs: Effective data access control for multi-authority cloud storage systems." In INFOCOM, 2013 Proceedings IEEE, pp. 2895-2903. IEEE, 2013.

[32] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." In *Advances in Cryptology–EUROCRYPT 2005*, pp. 457-473. Springer Berlin Heidelberg, pp. 457–473, Springer 2005.

[33] Yang, Kan, and Xiaohua Jia. "Expressive, Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage." pp 1-1. IEEE 2013.

[34] Tran, Hai V. "Data Management Challenges in Cloud Computing." InComputational Science and Its Applications (ICCSA), 13th International Conference on, pp. 19-27. IEEE, 2013.

[35] Hashizume, Keiko, David G. Rosado, Eduardo Fernández-Medina, and Eduardo B. Fernandez. "An analysis of security issues for cloud computing."Journal of Internet Services and Applications 4, Vol 1, pp 1-13. 2013

[36] Jasti, Amarnath, Payal Shah, Rajeev Nagaraj, and Ravi Pendse. "Security in multi-tenancy cloud." In Security Technology (ICCST), IEEE International Carnahan Conference on, pp. 35-41. IEEE, 2010.

[37] Garfinkel, Tal, and Mendel Rosenblum. "When Virtual Is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments." InHotOS.pp 227–22944] 2005.

[38] Catteddu, Daniele," Cloud Computing: benefits, risks and recommendations for information security," Springer Berlin Heidelberg, 2010.

[39] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation Computer Systems, Vol 3, pp 583-592,2012.

[40] Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and Atanu Rakshit. "Cloud security issues." In Services Computing SCC'09. IEEE International Conference on, pp. 517-520. IEEE, 2009.

[41] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." In Computer Science and Electronics Engineering (ICCSEE), International Conference on, vol. 1, pp. 647-651. IEEE, 2012.

[42] Prince, Brian. "IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering." E-Week. com (2009).

[43] Sahoo, G., and S. Mehfuz. "Securing Software as a Service Model of Cloud Computing: Issues and Solutions." International Journal on Cloud Computing: Services & Architecture Vol.3, No.4, August 2013.

[44] Cloud Security Alliance. Security Guidance for critical areas of focus in cloud computing Version2.1.2009.

[45] Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloud computing." In System Sciences (HICSS),44th Hawaii International Conference on, pp. 1-10. IEEE, 2011.

[46] A.Karger,"I/O for Virtual Machine Monitors: Security and performance issue,"IEEE Security and privacy ,September/October 2008.

[47] Shah, Amit. "Kernel-based Virtualization with KVM." Linux Magazine 86, pp 37-39, 2008.

[48] Xen Architecture Overview ,Version 1.2,Xen Wiki Whitepaper February 13,2008,

[49] Greenberg, Andy. "IBM's blindfolded calculator." Forbes Magazine, July 13,2009.

[50] Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and Atanu Rakshit. "Cloud security issues." In Services Computing, SCC'09. IEEE International Conference on, pp. 517-520. IEEE, 2009.

[51] Badger, Lee, Tim Grance, Robert Patt-Corner, and Jeff Voas. Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology. CreateSpace Independent Publishing Platform, 2012.

[52] Brunette, Glenn, and Rich Mogull. "Security guidance for critical areas of focus in cloud computing v2. 1." Cloud Security Alliance pp 1-76,2009.

[53] Lockhart, Hal, Steve Andersen, J. Bohren, Y. Sverdlov, M. Hondo, H. Maruyama, A. Nadalin et al. "Web services federation language (WS-federation) version 1.1." International Business Machines Corp., URL: ht tp://www-128. ibm. com/developerworks/library/specification/ws-fed ,2007.

García-Valls, Marisol, Tommaso Cucinotta, and Chenyang Lu. "Challenges in real-time virtualization and predictable cloud computing." Journal of Systems Architecture Vol 60, no. 9, pp 726-740, 2014.

[55] Yu, Yong, Jianbing Ni, Man Ho Au, Hongyu Liu, Hua Wang, and Chunxiang Xu. "Improved security of a dynamic remote data possession checking protocol for cloud storage." Expert Systems with Applications 41, no. 17 (2014): 7789-7796.