International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Security Solutions Paradigm in Cloud Computing

Subhash Chandra Pandey[1], Abhishek Bhatt[2]

Computer Science & Engineering Department, Birla Institute of Technology, Ranchi -Allahabad Campus
B-7, Industrial Area, Naini, Allahabad (UP), India

Abstract: ***Cloud computing refers to the delivery of computing resources over the Internet and it encompasses five important attributes. These are networks, servers, storage, applications and services. Cloud is a model where services are provided to the user through cloud service provider (CSP) on pay per use basis. At present, it is a matter of great concern in cloud computing that how to make assurance in accepting, sharing applications, hardware, etc., in an environment where we don`t know who is answerable for securing our data There are many aspects pertaining to security such as data integrity, data confidentiality, and data privacy. These security components can affect the performance of cloud environment. The cloud computing technology has opened many new horizons to different corporations and IT companies in developed countries. However, different issues related to cloud computing have yet to need further more pragmatic approach.***

Keywords: Cloud computing, Infrastructure as a Service, Platform as a Service, Security issues, Software as a Service

1. Introduction

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be hastily provisioned and released with nominal management effort or service provider interaction"[1].

The main characteristic of cloud computing is that the vicinity of physical resources and devices being accessed are generally not known to the end user. Further, cloud computing offers a wide range of services to the network users e.g., applications, storage, various operations and remote printing, etc. [2]. Indeed, cloud computing is the blending of development and acceptance of existing technologies and paradigms and its objective is to let the users to take benefit from all these technologies and that too without having much of knowledge or expertise about each one of them [3]. In [4], cloud computing is viewed like having an infinite credit line. In fact, cloud computing represents the paradigm in which computing infrastructure is viewed as a ''Cloud'' from which business organizations and individuals can access different applications anytime and from anywhere in the world on demand [6]. Moreover, cloud computing can be visualized as a pragmatic and gigantic structure which incorporates the quality of minimizing the costs by improving and developing functionality and economic outcome and thus results in increased collaboration, pace, and scalability up to a substantial degree [7-8]. The term "cloud" was coined with Internet in 1994 [9]. Further, this term became famous in 2006 when Amazon introduced the Elastic Compute Cloud (EC2) [10]. In early 2008, Open-Nebula was introduced as the first open-source software for deploying private and hybrid clouds, as well as for the union of clouds [11]. Eucalyptus turned out to be the first open-source amazon web service- application program interface (AWS-API) compatible platform for deploying private clouds in early 2008. Furthermore, by middle of 2008, Gartner redefined the cloud computing as:

"...to treat the relation of consumers of IT services, those who use them and those who sell them". [12]

In addition, these initial cloud computing paradigms facilitate the users to access different sets of

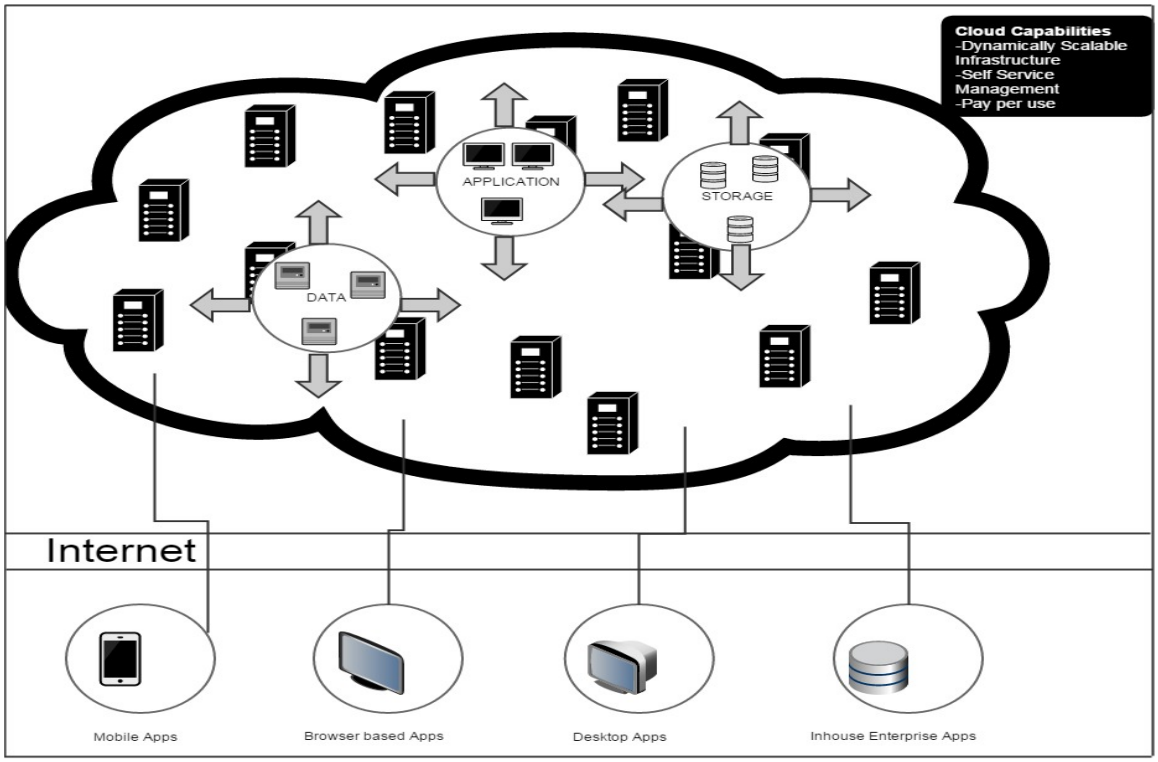

Figure 1: Conceptual view of cloud computing [16].

information technology services, including the Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS) layers [15-17]. Google Apps can be considered as an example of cloud computing from where we can access software or application using a browser and it can be utilized on thousands of computers via the Internet [18]. Fig.1 shows a conceptual view of cloud computing.

Perhaps security related issues are the most important concern in the field of cloud computing [8, 19]. It is obvious that insufficient security services can render the cloud system non-trustworthy. For example, managing personal information or data of consumers in a public network requires a high degree of security [8]. consistent care [20]. However, from the point of view of ease and cost of use the cloud computing is considerably beneficial.

Indeed, the customers' data and required computations must be confidential from both the cloud provider and other customers who are using the service [21]. In order to maintain this confidentiality the data are kept at remote location which is owned by others but it can create problem for the data owner in case of system failure of the service provider [22]. It is well known fact that data integrity and integrity of data storage is equally important and necessary requirement of the cloud computing. That's why integrity monitoring of data plays significant role in clouding computing to make it less prone to data corruption and crash [23].

Moreover, in cloud computing data security, data integrity, and data leakage all are major issues and for all these issues cryptographic solutions are available. There are different algorithms to get the data security in cloud computing e.g., Rivest, Shamir and Adleman (RSA) algorithm, Advanced Encryption Standard (AES) algorithm, Data Encryption Standard (DES) algorithm, International Data Encryption Standard (IDEA) algorithm etc. [26].

That's why, to make the cloud computing viable it is of the utmost importance to incorporate the feature of trust and fix the security flaws. In this paper, security issues in cloud technology have been reviewed. Further, different security solutions as well as algorithms are also elucidated.

2. Cloud Computing Models

The cloud computing environment consists of multiple types of clouds based on their deployment and usage. Following sub-sections present two important models of the cloud computing. These are the deployment and delivery model.

a) Deployment Models of Cloud Computing

There are different versions of the deployment models. Different categories of clouds used in deployment model are given below.

1) *Public cloud:* The public cloud is entirely used by common civic. Moreover, a public cloud encompasses an organization with reference to a cloud infrastructure which is shared via the Internet with other organizations and members of public community.
2) *Private cloud:* This cloud may be accessed by the organization itself or by a third party. Examples of private cloud technologies are Eucalyptus, Elastra, and VMware etc. [28].
3) *Community cloud:* This cloud is communally shared by many organizations comprising similar security requirements and also they need to store or process data of related sensitivity.
4) *Hybrid cloud:* The combination of cloud deployment models is known as hybrid cloud. Here, each cloud could

be independently managed while applications and data would be permitted to move across the hybrid cloud.

b) Delivery Models of Cloud Computing

Delivery model of cloud computing are mainly of the three types. These are SaaS, PaaS, and IaaS. Brief descriptions of these models are given below.

1) *Software as a service (SaaS):* Software-as-a Service allows organizations to get into business functionality at a very low cost usually less than paying for licensed applications due to the fact that SaaS charges are built on a monthly basis [28]. SaaS is a software dissemination method which gives right to access the software and its functions tenuously as a web-based service [30]. In this service, the user can take benefit of all the applications. There is no need to install or maintain any additional software for using this service. According to some recent reports, SaaS is a rapidly rising market that predicts ongoing double digit growth [31].
2) *Platform as a service (PaaS):* In PaaS, the user has an option of deploying the owned functional programs on the infra-structure of cloud [32]. PaaS is the service that offers the users to deploy user-designed or obtained applications on the cloud infrastructure [33]. In this cloud model, the cloud supplier provides a computing platform, logically comprising operating system, database, programming language implementation environment and web servers [34].
3) *Infrastructure as a service (IaaS):* This model uses virtualization software and thus enables multiple customers to work. These multiple customers are referred as "multiple tenants". The end user avails these offered services based on their needs and pay for what they have used [33]. However, the client has control over the operational system, storage area, and the established programs. Furthermore, an artificial server is entirely available for the user in IaaS [32]. These three delivery models are shown in Fig.2.

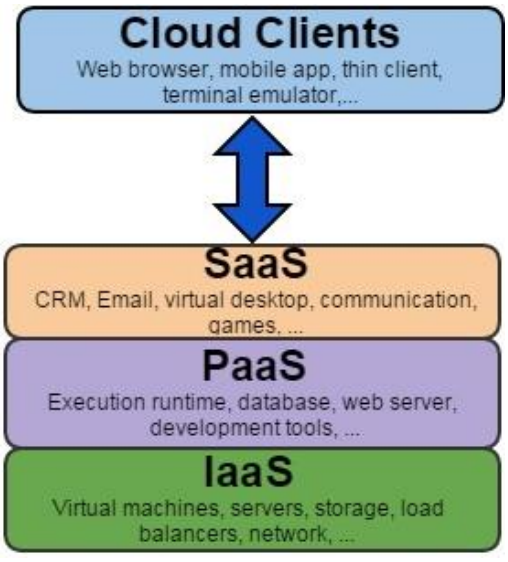

Figure 2: Hierarchical layout SaaS, PaaS, and IaaS with cloud clients

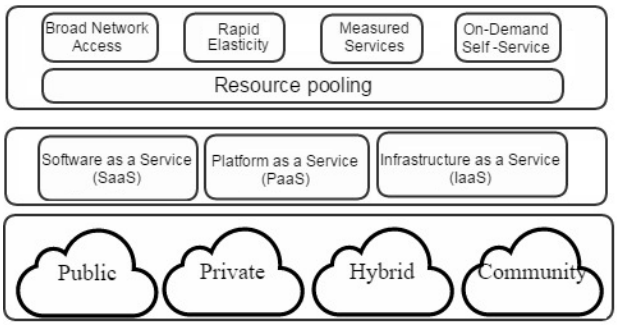

Figure 3: NIST cloud definition frame work [7]

3. Security Issue in Cloud Computing

Cloud computing exercises three delivery models and these three models can render several types of services to the end user. These service models also consign a different level of security constraints in the cloud environment. IaaS is the foundation of all cloud services, with PaaS built upon it and SaaS in turn built upon it [36-37]. If the cloud service provider takes under consideration only the security at the bottom of security architecture, the clients become more liable for implementing and supervising the security capabilities [38].

In fact, enterprise security concerns are emerged as the prime issue for the adoption of SaaS applications in the cloud [39].It is very challenging to assure the security of corporate data as they utilizes three services (SaaS, PaaS, IaaS) because each has its own security issues [41].

In short; IaaS and other allied services have enabled start-ups and other businesses to focus on their core proficiencies without troubling much about the provisioning and infrastructure management [37].

PaaS has the only disadvantage that, the advantages itself can be obliging for a hacker to control the PaaS cloud infrastructure for malware command and manage to go behind IaaS applications [43]. Fig. 2 shows the hierarchical layout of SaaS, PaaS, and IaaS with cloud clients.

a) Security Issues in SaaS

So it becomes complicated for the users to make sure that accurate security measures are being followed and it is also critical to believe that the application would be available when needed [44]. The following key security elements should be carefully considered as an integral part of the SaaS application development and deployment process:

- Data Security
- Availability
- Authentication and authorization
- Network Security
- Backup
- Data Breaches
- Data Integrity
- Web application security

1) *Data security:* Data security is one of the chief and most cited issues in SaaS delivery model. Moreover, extra security checks are needed to prevent the breaches occurring due to security susceptibilities in the application or through malevolent employees [45]. This

technology requires proper security principles and mechanisms to eradicate the malevolent users. Indeed, in SaaS model most cloud users are constantly anxious regarding their confidential data because it might be used for other malign purposes or transferred to other cloud service providers [46]. The issue of data storage protection in mobile cloud computing is discussed in [47].

2) *Availability:* It should be the major goal of the SaaS application providers to ensure that the systems are in running status and ventures are available with services almost all the time [37]. Moreover, flexibility in hardware or software breakdown, as well as the insolence of service strafe should be built in a bottom up manner within the application [48].
3) *Authentication and authorization:* For working with a safe cloud environment the authentication and authorization applications for venture environments may perhaps need to be altered.

Table 1: A comparison of HMAC, TPA and SIMS security solutions for Cloud Computing

Parameters→ Solutions Proposed↓	Year	Technique	Cost	Security	Speed	Advantage	Disadvantage	Remarks
Use of Hash Message Authentication Codes (HMAC)	1996	Combining a key with a Hash function	Minimises the cost	Directly related to the underlying hash function used.	one-half CPU cycle per byte (cpb) on 64-bit architectures	1. Can be used without the need for SSL. 2. Key pairs can be deleted. 3. Guarantees the authenticity. 4. An admin can generate any number of key pairs.	1. Not a lot of consistency. 2. Few and inconsistent server side implementations. 3. A single character difference can result to different value.	Advantageous in Security.
Third Party Auditor(TPA)	2008	HMAC	Reduces computation cost	Depends on storage correctness verifier.	18 clock cycles per byte	1. Public audit ability. 2. Storage correctness. 3. Privacy-preserving. 4. Batch auditing. 5. Lightweight.	If anyone deletes record then this method can no longer work.	Transparent yet cost-effective method.
Secure index management scheme(SIMS)	2004	Proxy Re-encryption	Provides cost efficiency	Pairing makes it difficult for a vicious third party to decode communication contents.	Single pairing and hash calculation provides quick search speed.	1. Confidentiality. 2. Search speed. 3. Traffic efficiency. 4. Calculation efficiency. 5. Sharing efficiency among users.	When the proxy and any delegate in the system collude, they can decrypt everyone else's messages.	Delegators' private key can be recovered.

properties of discrete logarithm problem and secure one-way hash function [49].

4) *Network security:* In fact SaaS application treats the vulnerable data attained from the enterprises and stores these data at the SaaS merchant end. The network security encompasses the use of strong network traffic encryption techniques such as the Transport Layer Security (TLS) technique and Secure Socket Layer (SSL) technique [51]. The network layer offers substantial fortification against the customary network security issues e.g., IP spoofing which is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an internet protocol (IP) address indicating that the message is the encoded end-points are accessible from both the Internet as well as from the Amazon EC2 and it assure that the data is transmitted steadily within AWS and from sources outside of AWS [52].
5) *Backup:* The SaaS vendor desires to make sure that all amenable enterprise data is retreated consistently for elegant improvement of quick recovery in case of desolation. The users need to separately encode their data and backups so that it may not be retrieved by any unapproved users [48].
6) *Data breaches:* It is fact that the data from different users and organizations resides together in a cloud environment. The chance of breaching into the cloud surroundings will

Table 2: Acomparison of PDP, POR and DIFC security solutions for cloud computing

Parameters→ Solutions Proposed↓	Year	Technique	Cost	Security	Speed	Advantage	Disadvantage	Remarks
Provable Data Possession(PDP)	2007	RSA-based homo-morphic authenticators.	Reduces I/O and storage costs.	Depends on spot checking and homo-morphic verifiable tags.	4.5 times as *fast* as MHT-SC.	Ensure possession of data files on un-trusted storage.	May leak user data information to the auditor when used directly.	Public audit ability demands the linear combination of sampled blocks which are exposed to the external auditor.
Proof of Retrievability (POR)	2007	Efficient audit protocol	Requires high resource cost.	The sentinels are generated independently of	High transmission cost.	The archive needs to access only a small portion of the file	Computationally cumbersome to encrypt data file	Best suited for storing encrypted files.

				the bit string.		unlike in the key-hash scheme.	especially when data to be encrypted is large.	
Decentralized Information Flow Control (DIFC)	1997	Labels (owner set and reader set).	Considerable cost of ensuring that a program does not violate security.	Protects privacy much more directly than access control.	Minimal cost to overall performance.	Clear rules for the legal propagation of data through a program, and the ability to localize security policy decisions.	Excessive restrictive -ness and the computational overhead.	It is not a widely accepted technique

However, the chances of data breach results in virtualization vulnerability [54].

7) *Data integrity*: Data integrity is one of the most solemn components in any system. Data integrity is easily attained in a discrete system with a single database. Data integrity in such a system is managed via database transactions [55]. Most of the databases support atomicity, consistency, isolation and durability (ACID) transactions and can preserve data integrity. One method for confirming the integrity of a set of data is based on hash values. A hash value is retrieved by abbreviating a set of data into a single unique value by way of a pre-demarcated algorithm [56].

8) *Web applications security:* SaaS application development may imply various types of software components and frameworks. These tools can lessen time-to-market and the cost of renovating a traditional software product or building

9) *Security Issues in PaaS:* In PaaS, the application provider may facilitate the people to build applications on top of the platform. However, any security issue underneath the application level such as host and network invasion prevention will still be an anxiety for the application provider and the application provider has to provide strong assertions that the data rests inaccessible in-between the applications [58]. Consequently, it inclines to be more extensible than SaaS at the cost of customer-ready features. This arrangement outspreads the security features and proficiencies especially where the innate capabilities are less complete. However, this arrangement is more flexible to provide additional security to different layers [58].

Algorithms → Factors↓	DES	AES	RSA	ECC	Blowfish
Developed	1977	2000	1982	1985	1993
Contributor	IBM 75	Rijman , Joan	Rivest, Shamir 78	Neal Koblitz, Victor S. Miller	Bruce Schneier
Key Length	56-bits	128,192, and 256	128,192, and 256	135 bits	32-448
Block Size	64-bits	128 bits	Variant	Variant	64
Security Rate	Proved Inadequate	Excellent	Good	Less	Considered Secure
Execution Time	Slow	More fast	Slowest	Fastest	Fast

10) *Security Issues in IaaS:* Although in theory virtual machines might be able to address these issues but in practice there are plenty of security problems [59]. Further, in order to achieve extreme trust and security the cloud resources require application of numerous other techniques [60].

4. Current Security Solutions

In Hash Message Authentication Code (HMAC) process, a secret key and hash algorithm such as secure hash algorithm (SHA) is used to generate the message authentication code. The HMAC function was firstly made available by Bellare et al. in 1996 and it comprises of analysis and a proof of the function's security [62]. Further, in 2002 it is assimilated in "Federal of Information Processing Standards" *(*FIPS) and "National Institute of Standards and Technology" (NIST) [62, 63]. Fig. 3 shows a cloud framework as defined by the NIST. Moreover, any hash algorithm such as MD5, SHA-1, SHA-256 etc., can be used with HMAC. The table 1 shows the comparison of HMAC, TPA and SIMS security solutions for cloud computing.

It eliminates the involvement of the client while the data is being stored in the cloud [65].

In this method, the public adaptability is attained by using provable data possession (PDP) and it ensures possession of data files on non-trusted storages [68]. The PDP technique utilizes the RSA-based authenticators for auditing the outsourced data and it recommends the random sampling of few blocks of the file. However, in this method the public audit-ability hassles the linear combination of sampled blocks exposed to the external auditor [68].

Further, this hash is stored along with the secret key. Thereafter, to verify the accuracy of

Table 3: Comparison of DES, AES, RSA, ECC, and BLOWFISH algorithms on the basis of different parameters

The table 2 displays the comparison of PDP, POR and DIFC security solutions for Cloud Computing and table 3 compares the DES, AES, RSA, ECC, and BLOWFISH algorithms on the basis of different parameters.

5. Conclusions

This paper reviews the different approaches for cloud data security and also encompasses different techniques and

algorithms pertaining to the domain of cloud computing. The proof of retrievable (POR) method uses a keyed hash function. In this method, before documenting the data file in cloud storage, the verifier calculates the cryptographic hash by means of keyed hash function. The network layer offers substantial fortification against the customary network security issues e.g., IP spoofing which is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an internet protocol (IP) address indicating that the message. Further, the application provider may facilitate the people to build applications on top of the platform.

References

[1] Mell, Peter, and Tim Grance, The NIST definition of cloud computing, NIST Special Publication, vol.800, page.145, 2011.
[2] Brian, Olivier, Thomas Brunschwiler, Heinz Dill, Hanspeter Christ, Babak Falsafi, Markus Fischer, Stella Gatziu Grivas et al., Cloud computing. White Paper SATW, publish Swiss press Page 6, 2012.
[3] M. *Hamdaqa*, L. *Tahvildari*,, Cloud computing uncovered: a research landscape, Advances in computers, vol. 86, Elsevier, pp. 41-85, 2012.
[4] Satwant Kaur, Cloud computing is like having an infinite credit line, IETE technical review, vol. 30, issue 5, pp. 410-416, 2013.
[5] Sichao Wang, Are enterprises really ready to move into the cloud? From CSA, 2015.
[6] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Gener. Comput. Syst, vol. 25, pp. 599–616, 2009.
[7] H.Takabi, J.B.D. Joshi, G. Ahn ., Security and privacy challenges in cloud computing environments, IEEE security privacy magazine, vol 8, pp.24-31, 2010.
[8] Pring. Ben, Cloud computing: the next generation of outsourcing, Gartner Group, pp.1-10, 2010.
[9] The official Microsoft blog. Microsoft.2010-02-01.
[10] Parag Nemade, Vaibhav Jaybhaye, Neethu Menon, Smita Dange, Designing virtual labs using cloud computing, International journal of advanced computer technology, vol. 3, Issue-10, pp.11-44, 2014.
[11] Hon. W. Kuan, Christopher Millard, Ian Walden, Negotiating cloud contracts: Looking at clouds from both sides now, Stanford technology law review, vol.16, page.1, 2012.
[12] Fernandes D. A., Soares, L. F., Gomes J. V., Freire M. M., Inácio, P. R., Security issues in cloud environments: a survey, International Journal of information security, vol.13.2, pp.113-170, 2014.
[13] Ali Mazhar, Samee U. Khan, Athanasios V. Vasilakos, Security in cloud computing: Opportunities and challenges, Information sciences, vol.305, pp.357-383, 2015.
[14] Kulkarni Gurudatt, Cloud computing-software as Service, International Journal of cloud computing and services science, I J-Closer, vol.1.1, pp.11-16, 2012.
[15] M. Monsef, N. Gidado, Trust and privacy concern in the cloud, European Cup, IT security for the next generation, pp.1-15, 2011.
[16] Zhang, Qi, Lu Cheng, Raouf Boutaba, Cloud computing: state-of-the-art and research challenges, Journal of internet services and applications, vol.1.1, pp.7-18, 2010.
[17] Subashini, Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of network and computer applications, vol.34 (1) pp.1-11, 2011.
[18] Fernandes, Diogo D. A., Soares, L. F., Gomes J. V., Freire, M. M., Inácio, P. R., Security issues in cloud environments: a survey, International journal of information security, vol.13.2, pp.113-170., 2014.
[19] Velte Toby, Anthony Velte, Robert Elsenpeter, Cloud computing: a practical approach, McGraw-Hill, Inc., 2009.
[20] Nuno Santos, Krishna P. Gummadi, Rodrigo Rodrigues, Towards trusted cloud computing, Proceedings of the 2009 conference on hot topics in cloud computing, pp.3-3., 2009.
[21] Prasanth A., Bajpei M., Shrivastava V., Mishra R. G., Cloud computing: A survey of associated services, eBook published by HCTL, 2015.
[22] Chou, David C., Amy Y. Chou, Software as a service (SaaS) as an outsourcing model: An economic analysis. Proc. SWDSI'08, pp.386-391, 2007.
[23] Braubach L., Pokahr A., Jander K., Jadex cloud-an infrastructure for enterprise cloud applications, Multi agent system technologies, Springer Berlin Heidelberg, pp.3-15., 2011.
[24] Hashemi, Sajjad, Khalil Monfaredi, Mohammad Masdari, Using cloud computing for e-government: challenges and benefits, World academy of science, engineering and technology, International journal of computer, information science and engineering, vol. 7, no.9 pp. 447-454, 2013.
[25] Domzal J., Securing the cloud: Cloud computer security techniques and tactics (winkler) [book reviews]. Communications Magazine, IEEE, vol.49 (9) pp. 20-20, 2011.
[26] Boniface M., Nasser B., Papay J., Phillips S. C., Servin A., Yang X., Kyriazis D., Platform-as-a-service architecture for real-time quality of service management in clouds., Internet and web applications and services (ICIW), 5th International conference on IEEE, pp.155-160, 2010.
[27] Hashizume K., Rosado D. G., Fernández-Medina E., Fernandez E. B., An analysis of security issues for cloud computing, Journal of internet services and applications, 4(1), pp.1-13, 2013.
[28] Sen, Jaydip, Security and privacy issues in cloud computing, architectures and protocols for secure information technology infrastructures, pp.1-45, 2013.
[29] Tiwari Pradeep Kumar, Bharat Mishra, Cloud computing security issues, challenges and solution, International journal of emerging technology and advanced engineering , 2,8, pp.306-310, 2012.
[30] Chen D., Zhao H., Data security and privacy protection issues in cloud computing, Computer science and electronics engineering (ICCSEE), International Conference of IEEE, vol. 1, pp. 647-651, 2012.
[31] Jansen W., Grance T., Guidelines on security and privacy in public cloud computing, NIST special publication 800, page.144, 2011.

[32] Kandukuri B.R, Paturi V.R, Rakshit A., Cloud security issues. IEEE international conference on services computing, pp.517–20., 2009.
[33] Blaze, M., Feigenbaum, J., loannidis, J., Angelos, D. and Keromytis ,The role of trust management in distributed systems security, secure internet programming, issues for mobile and distributed objects. Berlin. Springer-Verlag; pp.185–210., 1999.
[34] Al Zain M. A., Pardede E., Soh B., Thom J. A., Cloud computing security: from single to multi-clouds. System science (HICSS), 45th Hawaii international conference on IEEE, pp.5490-5499, 2012.
[35] Choudhary V., Software as a service: Implications for investment in software development, International conference on system sciences, page. 209, 2007.
[36] Kuyoro S.O., Ibikunle F. , Awodele O, Cloud computing security issues and challenges, International Journal of Computer Networks, vol. 3, issue 5, pp.11-14, 2011.
[37] T. Elahi, S. Pearson, Privacy assurance: Bridging the gap between preference and practice, trust, privacy and security in digital business, Springer Berlin, Heidelberg, vol. 4657, pp. 65-74, 2007.
[38] Liao I. E., Lee C. C., Hwang M. S., A password authentication scheme over insecure networks, Journal of computer and system sciences, vol. 72(4), pp.727-740, 2006.
[39] Yang G., Wong D. S., Wang, H., Deng X., Two-factor mutual authentication based on smart cards and passwords, Journal of computer and system sciences, vol.74, pp.1160-1172, 2008.
[40] Susarla, Anjana, Anitesh Barua, Andrew B. Whinston, Multitask agency, modular architecture, and task disaggregation in SaaS, Journal of management information systems, vol. 26 (4), pp.87-118, 2010.
[41] Fenn, Micheal, Jason Holmes, Jeffrey Nucciarone, A performance and cost analysis of the amazon elastic computer cloud (EC2), Cluster compute instance, pp.1-7, 2010.
[42] Chou Te-Shun, Security threats on cloud computing vulnerabilities, International journal of computer science and information technology, vol. 5 (3), pp.79-88, 2013.
[43] Tsai W. T., Zhong P., Multi-tenancy and Sub-tenancy architecture in software-as-a-service (SaaS), In service oriented system engineering (SOSE), 8th International symposium on IEEE, pp.128-139, 2014.
[44] Eswaran S., Abburu S., Identifying data integrity in the cloud storage, International journal of computer science issues (IJCSI), vol.9 (2), pp.403-408, 2012.
[45] Kaufman LM., Data security in the world of cloud computing, IEEE security and privacy magazine, vol.7 (4), pp.61–64, 2009.
[46] Lee K., Security threats in cloud computing environments. International journal of security and its applications, vol.6 (4), pp. 25-32, 2012.
[47] Sandikkaya, Mehmet Tahir, Ali Emre Harmanci, Security problems of platform-as-a-Service (PaaS): clouds and practical solutions to the problems, Proceedings of the IEEE 31st Symposium on reliable distributed systems, IEEE Computer Society, pp. 463-468, 2012.
[48] Attanasio C.R., Virtual machines and data security. Proceedings of the workshop on virtual computer systems. New York, NY, USA: ACM, pp.206–209, 1973.
[49] Juels A., Jr. Kaliski B.S, PORS: proofs of retrievability for large files, Proceedings of the 14th ACM conference on computer and communications security (CCS'07), pp.584–597, 2007.
[50] Richa Singh, Amit Kumar Sharma, A comparative study: various approaches for cloud data security, International journal of computer science and information technologies (IJCSIT), vol.5 (2), pp.1934-1937, 2014.
[51] Elovici Y., Waisenberg R., Shmueli E., Gudes E., A structure preserving database encryption scheme, SDM workshop on secure data management, pp. 54-68, 2004.
[52] Sun-Ho Lee, Im-Yeong Lee, Secure index management scheme on cloud storage environment, International journal of security and its applications, vol.9 (2), pp.75-82, 2012.
[53] Ateniese G., Burns R., Curtmola R., Herring J., Kissner L., Peterson, Z., Song D., Provable data possession at un-trusted stores, Proceedings of the 14th ACM conference on computer and communications security, pp.598-609, 2007.
[54] Shacham Hovav, Brent Waters, Compact proofs of retrievability, advances in cryptology-ASIACRYPT, Springer Berlin, Heidelberg, pp.90-107, 2008.