**A Review of Security Issues and Algorithms in Cloud Computing**

Manpreet kaur

Research Fellow, Chandigarh Group of College, Landran

Mohali,Punjab

Cutemani.shergill@gmail.com

Hardeep Singh

Asst professor, Chandigarh Group of college, Landran

Mohali,Punjab

Cgccoe.cse.hardeep@gmail.com

***Abstract:*** Cloud computing is an prominent model which has become today’s scorching research area due to its ability to reduce the costs associated with computing. In present scenario, it is most alluring and fascinating technology which is offering the services to its users on demand over the internet. There are number of users used cloud to store their personal data, so that data storage security is required on the storage media. The major concern of cloud environment is security during upload the data on cloud server. Cloud security is an evolving sub domain computer security, network security and more broadly, information security. Encryption is an technology for protecting sensitive data. There is a combination of public key and private key encryption to hide the sensitive data of users and cipher text retrieval. This research paper discuss the security issues and feasibility of applying encryption algorithms for data security and privacy in cloud storage.

***Keywords:*** Cloud computing, cloud data storage, cloud data security, Deployment models, Service models, cloud security challenges, privacy, Encryption Algorithms.

1. **INTRODUCTION**

The term “Cloud Computing” is the computing services in Information Technology like infrastructure, platforms, or applications could be arranged and used through the internet. Infrastructure upon which cloud is built upon is a large scaled distributed infrastructure in which shared pool of resources are generally virtualized, and services which are offered are distributed to clients in terms of virtual machines, deployment environment, or software. Hence it can be easily concluded that according to the requirements and current workloads, the services of cloud could be scaled dynamically. As many resources are used, they are measured and then the payment is made on the basis of consumption of those resources.

According to the definition of[15], cloud computing is “it is a significant distributed computing model that is directed by financial prudence of balance, in which stake of isolate, fundamental, loading, podium in which a facilities are supplied as per the request of exterior foreign clients through the internet”. There are some examples of cloud services like webmail, online file and business applications. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud storage [20] specifies the storage on cloud with almost inexpensive storage and backup option for small enterprise. The actual storage location may be on single storage environment or replicated to multiple server storage based on importance of data. The mechanism [20] model of cloud storage consists of four layers: storage layer which stores the data, basic management layer which ensures security and stability of cloud storage itself, application interface layer which provides application service platform, and access layer which provides the access platform. The basic cloud storage environment represented as below:

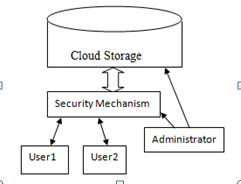


Figure 1: Cloud Storage Environment

1. **Cloud Services Models**

Cloud computing offers three fundamental service models that is [27] Infrastructure as a service, Platform as a service and Software as a service:

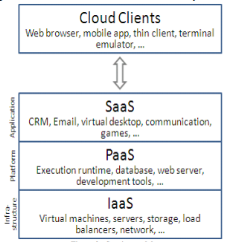


Figure: Service models

**Cloud Infrastructure as a service(IaaS):** In this composition of [24] implemented environment for their system a supplier must be supply a different computing resources which include loading, processing unit. Client has flexile to achieve and switches a software multilated to be implemented and vary between different applications like operating system etc.

**Cloud Platform as a service (PaaS):** This software supplies client with the ability to establish and extended [37] applications that are mainly positioned on equipment and programming languages promoted by the suppliers. In this the client has no containment over the different organization but has containment over the extended applications. Examples of this class of services include Google App Engine, Windows Azure Platform and rack space.

**Types of PaaS**: There are different types of PaaS such as

* Application Delivers only Environments
* Standalone Developments Environments
* Open Platform & Open Service
* Add on Development Possibility

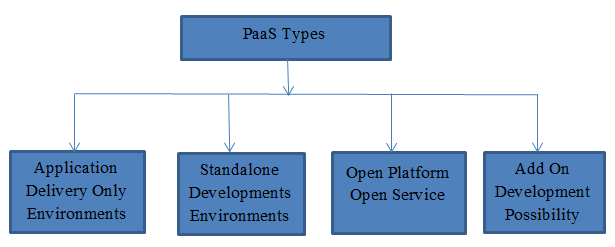


Figure 2: PaaS Types

**Cloud Software as a service (SaaS):** This software supplies the ability to usage the appliances which implemented on cloud organization. With the usage of standard [30] interfaces like web browser or online(e-mail) client, these appliances are obtainable. SaaS appliances are obtained from different devices like mobile, workstation from anywhere at any time.

**Cloud Network as a service (NaaS):** NaaS provides the capability to use the network services and inter-cloud network [37] connectivity services. Improvement of possession allocation services include in view of network and computing resources. These type of services involved extensible, enhanced virtual private network.

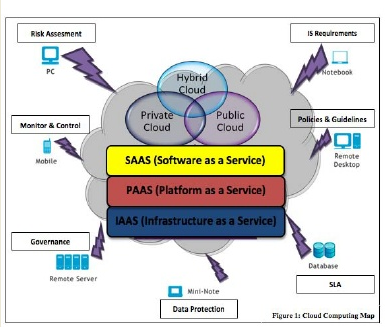


Figure 3: Cloud Computing map [6]

1. **Cloud Deployment Models**

**Public Cloud:** Public [25] cloud describes the conventional meaning of cloud computing that is accessible, effective ways and means, which are accessible on internet from a minor party, which detached assets and charges its clients on the basis of utility. Cloud organization is possessed and accomplish by a supplier who suggest its retune to public domain. E.g. Google, Amazon, Microsoft offers cloud services via Internet. There are different benefits of public cloud model. The following figure shows some of those benefits:

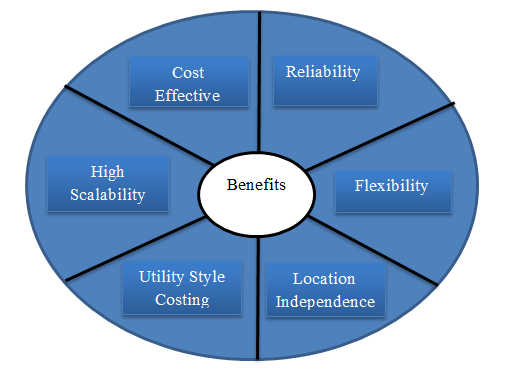


Figure 4: Benefits of Public Cloud

**Private Cloud:** Private cloud is a term used to donate a proprietary [11] computing architecture provisioned services on corporate networks. Big enterprises usually used this type of cloud computing to permit their private network and information Centre administrators to effectively become in-house ‘service providers’ catering to customers within the corporation. Cloud organization is establishing for a particular aggregation and managed by a third party under a service level agreement. Only single organization preferred to operate via corporate cloud. There are advantages (benefits) of internal cloud model. The diagram given below depicts a few of these advantages (benefits):

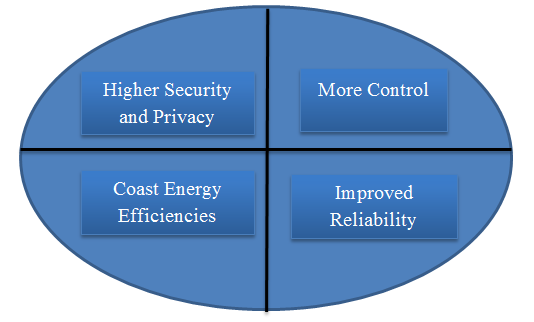


Figure 5: Benefits of Private Cloud

**Hybrid Cloud:** A hybrid cloud comprises assets from both corporate [37] and public providers will definitely become the demanded choice for enterprises. The hybrid cloud is a combination of both corporate cloud and public cloud.. For example, for general computing enterprise could selects to make usage of external services, and its own data Centre’s comprises it own data Centre’s. Hybrid cloud model has number of advantages (benefits).The diagram given below reveals some of those advantages (benefits):

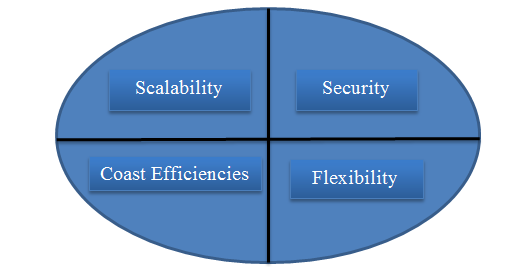


Figure 6: Benefits of Hybrid Cloud

1. **Cloud Computing Characteristics**

**On Demand self-service:** A cloud might individually attain computing possibilities, as per the use of different servers, network storing, as on request, without communicating with cloud provider.

**Broad Network Access:** Services are delivered across the Internet within a standard mechanism and access to the services is possible through assorted customer tools.

**Resource pooling:** A multitudinous model is employed to serve different types of clients by making pools of different computing resources, as per the request of customers these have different resources which can be assigned and reassigned dynamically.

**Rapid Elasticity:** Capabilities might be elastically provisioned or rapidly released. From customers view, the provided possibilities come out to be limitless and must have the capability to purchase in any quantity at any time.

**Measured Services:** The provision procured by different clients is measurable. The use of asset will be directed, estimated, and accused for contributor and asset.

1. **Cloud Security challenges**

There are some key security [6] challenges are:

**Authentication:** Throughout the internet data stored by cloud user is available to all unauthorized people. Henceforth the certified user and assistance cloud must have inter-changeability administration entity.

**Access Control:** To check and promote only legalized users, cloud must have right access control policies. Such services must be adjustable, well planned, and their allocation is overseeing conveniently. The approach governor provision must be integrated on the basis of Service Level Agreement (SLA).

**Policy Integration:** There are many cloud providers such as Amazon, Google which are accessed by end users. Minimum number of conflicts between their policies because they user their own policies and approaches.

**Service Management:** In this different cloud providers such as Amazon, Google, comprise together to build a new composed services to meet their customers need. At this stage there should be procure divider to get the easiest localized services.

**Trust Management:** The trust management approach must be developed as cloud environment is service provider and it should include trust negotiation factor between both parties such as user and provider. For example, to release their services provider must have little bit trust on user and users have same trust on provider.

1. **Security Feature in Cloud Computing**

Cloud computing security architecture is reveal in figure . Cloud provider is concerned with cloud orchestration and cloud service management. Cloud auditor assesses the data in the cloud environment. Cloud broker has different services such as intermediation, aggregation and arbitrage. So cloud consumer, cloud provider and cloud broker act as a major role in cloud security.

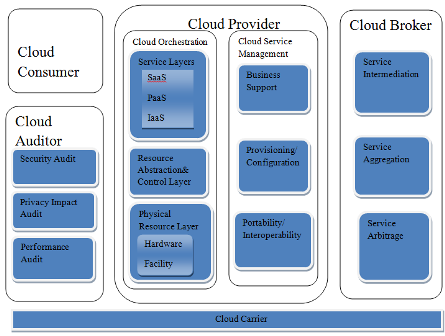


Figure 7: cloud computing security

There are several main challenges for building a secure band trustworthy cloud system:

**Outsourcing:** Outsourcing brings down both capital expenditure and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services. In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive data is out of the owner’s control.

**Massive data and intense computation:** Cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored, it is impractical to hash the entire data set. To this end, new strategies and protocols are expected.

1. **Security Issues**

The security of corporate data in the cloud is difficult, as they provide different services like Network as a service (NaaS), Platform as a service (PaaS), Software as a service (SaaS), Infrastructure as a service (IaaS). Each service has their own security issues [4]

**Data Security:** Data Security refers as a confidentiality, integrity and availability. These are the major issues for cloud vendors. Confidentiality is defined as a privacy of data. Confidentiality are designed to prevent the sensitive information from unauthorized or wrong people. In this stores the encryption key data from enterprise C, stored at encrypted format in enterprise D. that data must be secure from the employees of enterprise D. Integrity is defined as the correctness of data, there is no common policies exist for approved data exchanges. Availability is defined as data is available on time.

**Regulatory Complaince:** Customers are eventually accountable when the security and completeness of their own data is taken by a service provider. Traditional service providers more prone to outsource surveys and security certification. Cloud computing providers reject to endure the scrutiny as signaling so these customers can only make usage of paltry operations [16].

**Data Locations:** When users use, they probably won’t know exactly where their data will hosted and which location it will stored in. In fact, they might not even know what country it will be stored in. Service providers need to be asked whether they will accomplish to storing and alter data in particular arbitration, and on the basis of their customers will s make a fair accomplishment to follow local privacy requirement [14].

**Privileged user access:** Outside the resource data that is processed contains an indigeneous risk, as deploy services, avoid the mortal, consistent and human resource manage IT shops works on the house programs.

**Trust Issue:** Trust is also a major issue in cloud computing. Trust can be in between human to machine, machine to human, human to human, machine to human. Trust is revolving around assurance and confidence. In cloud computing, user stores their data on cloud storage because of trust on cloud. For example people use Gmail server, Yahoo server because they trust on provider.

**Data Recovery:** It is defined as the process of restoring data that has been lost, corrupted or accident.

1. **Security Algorithms**

**MD5 Encoding Algorithm:** The main reason to describe the basics [18] of MD5 and how it works is that because in present scenario the world of cryptography is huge and very difficult. MD stands for Message Digest. It explains a mathematical function that can take place on a variable length string. The numeral 5 simply reveals that MD5 was the beneficiary to MD4. MD5 is crucial a checksum that is usage to confirm the accuracy of a string. It is one of its most common usages. There is a one working example. Let’s say, any client have clemency a few program, application or a software that any client demands to openly distribute in community, this is all better and well but what if any individual was to humour with clients appliances with malignant intent? For instance what if they combined malware onto client application, how would individuals know? SO, if any individual had taken MD5 checksum of any client original data and made this information public, only then customer downloaded software and could check their downloaded information and check that the MD5 checksum matches clients informations. If it does then great! If not then it means your program has been tampered with.

**How does it work?** – In this user explain that if it is new to cryptographer then this can get complicated! Essentially the input string is divided into 512 it blocks, if the string is not divisible by 512 only then it is cushioned. Furthermore, the output for an MD5 hash is always a 128 bit file. The activity to work this is divided into four 32 bit words that is W, X, Y, Z. Moreover, each of these words performs 16 operations making 64 in sum. These are also known as rounds. The application perform on each 512 bit block then applications are non-linear functions, for modular combination and left rotations. At last, output is then a 128bit Hex string.

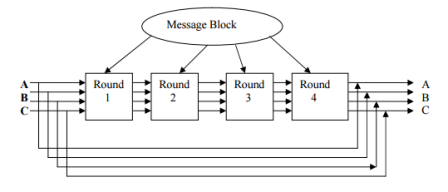


Figure 8: MD5 main loop

**Diffie Hellman Key Exchange Algorithm:** Diffie Hellman was the first key algorithm ever invented, in 1976. Diffie Hellman key agreement protocol is [27]:

Exponential key agreement

Allows two users to exchange a secret key

Requires no prior secrets

Real-time over an untrusted network

Definition of Diffie Hellman: Let n be a prime number and p be an integer. The Diffie Hellman Problem (DHP) is the problem of computing the value of (mod n) from the known values of (mod n) and (mod n). The setup of Diffie Hellman algorithm

* Suppose we have two parties Master and Slave, they want to communicate to each other.
* They do not want the eavesdropper to know their message.
* Alice and Bob agree upon and make public two numbers n and p, where n is a prime number and p is a primitive root mod n. Anyone has access to these numbers.
* Public exchange of values.
* Masters sends M to slave==M
* S= Slave sends S to Master

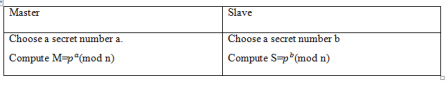


Table1: Private Computations

* Master compute the number.
* Bob compute the number

Here Master and Slave have the same key that is K=(mod n).

In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to exchange data, both agree on a symmetric key. Symmetric Key is used for encryption or decryption the messages. Diffie Hellman algorithm is used for only key agreement or key exchange, but it does not used for encryption or decryption. Before starting the communication, secure channel is established [27]. Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established.

Figure 12, shows that Master and Slave wants to communicate with each other. To start communication both parties need to establish secure channel. To establish secure channel, two random prime numbers p and n are selected, both devices are agreed on these two numbers. Selected p and n are the public numbers. Both parties, say device 1 become master and device 2 become slave, both master and slave select their private numbers a’ and ‘b’ respectively. Master and slave use their public and private number and calculated their private keys [26].

From M, slave computes:

K2=mod n

If both master and slave calculate same values of K1 and K2, then secure channel is established between them. The combination of KI and K2 becomes the shared symmetric key between master and slave.

To encrypt the messages, they used the public key or shared key (k) of both parties. For decryption of messages private key of both parties which is randomly chosen by the users i.e. ‘a’ and ‘b’ are used [28].

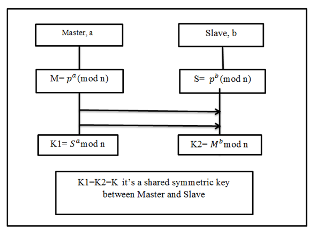


Figure 9: Diffie hellman key exchange

**Advanced Encryption Algorithm:** This algorithm was established [37] by Joan Daemen and vincient Rijmen, in 1998. These were two Belgian cryptographers. AES is a secret key encryption algorithm which operates on a fixed block size of 128 bits, but different key lengths that is 128, 192 and 256 bits. The sum of recurrence of conversion bulbous that disciple the input called plain text into the final output called the cipher text.

The sum of period of recurrence are as follows:

10 cycles of repetition for 128 bits.

12 cycles of repetition for 192 bits.

14 cycles of repetition for 256 bits.

Each round consists of several processing steps. A bent of converse bulbous are enforced to deportation cipher text into the plain text by using encryption key.

The basic steps of AES algorithm are stated as:

Key Expansions

Initial Round

Rounds

Final Round

Key Generation

**Key Expansions**: In this round keys are derived from cipher keys. AES requires a separate 128 bits keys plus one more key.

**Initial Round:** In this add round key is used which is explained further:

**Add Round key:** In this individual eight bits of the capacity is connected with block of the round key using bit wise XOR.

**Rounds:** In this three different steps are used that is sub-bytes, shift rows and mix columns.

* **Sub-bytes:** A non-linear substitutions steps where each byte is reinstate with one more on the basis of look up table.
* **Shift Rows:** A transaction stride in which individual line of the case is transfer cyclically a certain number of steps.
* **Mix Columns:** A mixing procedure which proceed on the file of the case, mixing the four bytes in individual file.
* **Add Round key:** In this individual eight bits of the file is mixed with block of the round key using bit wise XOR.

**Final Round:** In this all steps are same as round except mix columns.

**Key Generation:** This module handles key generation by the cryptographic module at client side. The assistant develop unique keys for clients once they accurate themselves with the assistant. The key is develop with the usage of AES key developer category. This key is transmission to the cloud customer via the e-mail which get and save a duplicate for it for decrypting purpose..

**RSA:** It is an algorithm [40] for public key cryptography, involves a private key. For encrypting messages public key is used which can be known to everyone. All those messages can be only decrypted by using private key which can be encrypted by public key. Client information include encryption prior to saved, client authentication procedures prior to save or retrieval and building privacy channels for information transmission.

**Limitations:** There are following some limitations of RSA algorithm:

* Using small primes.
* Using primes that are very close.
* Messages is an observable power.
* Two people using the same N receiving the same message.
* Sending the same message to e or more people with the same e (Hastad’s attack).

1. **Conclusion & Future work**

Cloud computing is latest technology that is being widely used all over the world. If company takes the decision to round the cloud then they loses control over the information. The extent of preservation required to private information is directly proportional to the value of information. Privacy of the Cloud relies on trusted computing and cryptography. Number of cloud platforms are available now in educational as well as in enterprises circle

In this paper, we have discussed the issues related to data location, storage, security, availability and integrity. Establishing trust is the way to overcome these security issues as it establishes entities relationship quickly and safely. These issues mentioned above will be the research hotspot of cloud computing. Security algorithms are defined for advanced encryption and decryption. These algorithms can be implemented in future to enhance security over a network. In future, we will extend our research by providing algorithms implementations. There is no doubt that cloud computing has bright future.

1. **References**

1) Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, *“Cloud security issues*” In Services Computing, 2009. IEEE International Conference on, page 517520, 2009

2) Boldreva A., Chenette N., Lee Y, O’neill A. (2009), *“Order-preserving Symmetric encryption”,* Advances in Cryptology-EUROCRYPT 2009 Springer, Berlin/Heidelberg, pp. 224-241.

3) Boneh D., Di G., Ostrovsky R., Persiano G. (2004), *“Public key encryption with keyword search”,* Advances in Cryptology-Eurocrypt, Springer, Berlin/Heidelberg, pp 506–522.

4) B.R kandukuri, R.Paturi V, and A.Rakshit, “cloud security issues”,2009 IEEE International Conference on Services Computing, sep. 21-25, 2009, Bangalore, India, pp. 517-520.

5) Campbell, Jeronimo, “Applied Virtualization Technology,” Hillsboro, Intel Press (ISBN 09764832-3-8), 2006, pp. 69-73.

6) Chandrahasan, R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam. "Research Challenges and Security Issues in Cloud Computing." *International Journal of Computational Intelligence and Information Security* 3.3 (2012): 42-48.

7) Chun-Ting Huang, Zhongyuan Qin, C.-C. Jay Kuo., “Multimedia Storage Security in Cloud Computing: an Overview” 978-1-457701434- 4/11/$26.00,IEEE,2011.

8) Cloud Security Alliance, “Top Threats to Cloud Computing v1.0,” Prepared by the Cloud Security Alliance, March 2010, pp. 1-14.

9) Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy Preserving Public Auditing for Data Storage Security in , cloud Computing”, 2010.

10) Cong Wang, Qian Wang, KuiRen and Wenjing Lou, “*Ensuring Data Storage Security in Cloud Computing”,* In Quality of Service, 2009. 17th International Workshop on, page 19, 2009.

C. Boulton, Oracle CEO Larry Ellison Spits on cloud computing Hype, in eWeek.com. 2009, 2009, pp. 11–14.

11) Dong Xin, et al.”achieving secure and efficient data collaboration in cloud computing. ”Quality of service, 2013 IEEE/ACM 21st  International symposium on.IEEE,2013.

12)Dr.R.Manicka Chezian and C.bagyalakshmi ”a survey on cloud data security Using encryption technique” in International journal of advanced research in computer engineering & technology , Volume 1, Issue 5, July 2012.

13) Er.Rimmy Chuchra,Lovely Professional University,Phagwara, India, *“Data Security in Cloud Computing”*, International Journal Nov.,2012.

14) Feng-Tse Lin, Teng-San Shih, “Cloud Computing: The Emerging Computing Technology,” ICIC Express Letters Part B: Applications (ISSN: 2185-2766), v1, September 2010, pp. 33-38.

15) Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud Computing and Grid Computing 360-Degree Compared CoRR. *abs/0901.0131*.

16) G. Hughes, D. Al-Jumeily & A. Hussain,” Supporting Cloud Computing Management through an Object Mapping Declarative Language”, 2010 Developments in E-systems engineering.

17) Hassan Takabi, James B. D. Joshi and Gail-JoonAhn**,** *“Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments”* Proceedings of the 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops, p.393-398, July 19-23, 2010.

18)Hossain, Md Alam, et al. "Cryptanalyzing of message digest Algorithms MD4 and MD5." *International Journal on Cryptography and Information Security (IJCIS)* 2.1 (2012): 1-13.

19) John Harauz, Lori M. Kaufman and Bruce Potter, ”Data security in the world of cloud computing” published by the IEEE computer and reliability societies in July/August 2009.

20)Jouni Mäenpää, “Cloud Computing with the Azure Platform,” TKK T-110.5190 Seminar on Internet Working, April 27, 2009.

21) Kant, Dr Chander, and Yogesh Sharma. "Enhanced Security Architecture for Cloud Data Security." *International Journal of Advanced Research in Computer Science and Software Engineering* 3.5 (2013): 571-575.

22) Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print.

23)Meiko Jensen, JlorgSchwenk, Nils Gruschka and Luigi Lo Iacono, *“On Technical Security Issues In Cloud Computing”,*IEEE International Conference on Cloud Computing,2009.

24) M. Bloch, A. Hoyos-Gomez, How CIOs should think about business value,McKinsey on Business Technology 15 (Spring 2009) 28–37

M.A. Baish, J. Curtis, J. Applebaum, L. Bradley, F. Al-Rawaf, M. Greenwood, C.Saylor, J. Cuddihy, S. Udry, K. Bankston, M. Rotenberg, J. Richard, S. Aftergood, E.Fidell, C. Scherr, J. Radack, L. Pratt, T. Foster, D. Chaffee, C. Chodroff, G. Isaac, S.Buttar, M. Price, J. Bertin, M. McCluer, L. Gustius, K. Adair, N. Sonnett, R. Melberth,K. Guinane, W. Patten, A. Fuller, J. Bradshaw, M. Johnson, A. Canterbury, J. Musa, N.Singh, P. Murthy, D. Brook, C. Arrowood, M. Ostrolenk, M.A. Stein, J. Thukral, D.vonBreichenruchardt, R. Kassem, Liberty and Security: Recommendations for the Next Administration and Congress, The Constitution Project, 2008.

25)Nabendu Chaki, ”A Survey on Security issue in Cloud Computing ” in 6th International conference on Electrical Engineering/Electronics, Computer, Telecommunication and Information Technology, May 2009.

26)N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam, “An Implementation of RSA Algorithm in Google Cloud using Cloud SQL”, Research Journal of Applied Sciences, Engineering and Technology, 2012, ISSN: 2040-7467.

27) R. Agarwal, H. Lucas, The information systems identity crisis: focusing on highvisibility and high-impact research, MIS Quarterly 29 (3) (2005) 381–398.

28)Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg and Ivona Brandic, “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility,” Future Generation Computer System, 2009, pp. 599-616.

29)Ren K, Wang C, Wang Q (2012) Security challenges for the public cloud. IEEE Internet Comput 16(1):69–73.

30)R. Buyya, C.S. Yeo, S. Venugopal, Market-Oriented cloud computing: Vision, Hype,and Reality for Delivering IT Services as Computing Utilities, 10th IEEE International Conference on High Performance Computing and Communications,2008 (HPCC08), 2008.

31) "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. 2011. Retrieved 2011-05-04.

32)Tout, Sverdlik, and Lawver, “Cloud Computing and its Security in Higher Education,” In Proceedings of the Proc ISECON 2009.

33)Vaquero, Merino and Lindner, “A Break in the Clouds: Towards a Cloud Definition,” ACM SIGCOMM Computer Communication Review, v.39 n.1, January, 2009, pp. 50-55.

34) W. Zeng, Y. Zhao, K. Ou, and W. Song, "Research on cloud storage architecture and key technologies," in Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea, 2009, pp. 1044-1048.

35)Xia Z., Zhu Y., Sun X. and Chen L. (2014), "*Secure semantic expansion based search over encrypted cloud data supporting similarity ranking "*Journal of Cloud Computing”,Springer 3.1, pp. 1-11.

36) Yunqi Ye, Liangliang Xiao, I-Ling Yen, Farokh Bastani, “Secure, Dependable, and High Performance Cloud Storage”, 2010 29th IEEE International Symposium on Reliable

37)Bhoyar, Rahul, and Nitin Chopde. "Cloud Computing: Service models, Types, Database and Issues." *International Journal of Advanced Research in Computer Science and Software Engineering* 3.3 (2013): 695-701.

38)Pahal, Ritu, and Vikas Kumar. "Efficient Implementation of AES." *International Journal of Advanced Research in Computer Science and Software Engineering Volume* 3 (2013).

39))[www.academicroom.com/topics/cloud-computing](http://www.academicroom.com/topics/cloud-computing)

40)Zhou, Xin, and Xiaofei Tang. "Research and implementation of RSA algorithm for encryption and decryption." *Strategic Technology (IFOST), 2011 6th International Forum on*. Vol. 2. IEEE, 2011.

**BIOGRAPHY OF AUTHORS**

**Manpreet kaur** is pursuing Masters in computer science at Chandigarh Group of college (CGC-COE), Chandigarh. Her research interests include Cloud Computing and software Architecture.

**Hardeep Singh** completed masters in computer science & engineering from Baba Banda Singh Bahadur college, Fatehgarh sahib. His research interest are in the fields of software engineering, cloud computing, cyber administration.