International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-1 E-ISSN: 2347-2693

Analyzing Various Existing Security Techniques to Secure Data Access in Cloud Environment

Rachna Jain[1*], Sushila Madan[2] and Bindu Garg[3]

[1*] Computer Science Department, Banasthali vidyapith University, Banasthali, Rajasthan, India
[2] Computer Science Department, Delhi University, Delhi, India
[3] Computer Science Department, IP University, Delhi, India

www.ijcaonline.org

Received: Dec/23/2014 Revised: Jan/4/2015 Accepted: Jan/24/2015 Published: Jan/31/2015

***Abstract*—** Cloud computing is the key powerhouse in numerous organizations due to shifting of their data to the cloud environment. The use of cloud computing has been increased rapidly in various organizations as it provides multiple benefits in terms of low cost and accessibility of data. There are different types of issues have been observed in cloud computing environment that need to be addressed. In the past, International Data Corporation (IDC) conducted a survey of 263 IT executives to gauge their opinion about the usage of IT cloud services in companies. As a result, Security was ranked first and observed utmost issue of cloud computing. So nowadays, protection of data in cloud is a big deal. Organizations mislay control over the data as soon as data moves to the cloud. Thus, protection needed to secure data is directly proportional to the value of the data.The first level of security where cryptography can help cloud computing is secure storage .There are already some cloud providers that have started providing secure storage services but offering different levels of protection.The major handicap of secure storage is that we cannot outsource the processing of this data without decrypting it before or without revealing the keys used for encryption. In this paper, various techniques to secure data access in cloud environment has been analyzed and during analysis it is observed that security need to be addressed for securing transaction in such a way that transaction should be encrypted and not be decrypted during access. Moreover, access should be provided to the users as per their access rights. Security can be enhanced by use of multi cloud as single cloud that become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud.

***Keywords*—**Cloud Computing,Single Cloud,Multi Cloud,Homomorphic Encryption,HELIB

I. INTRODUCTION

Cloud computing is becoming pertinent technology due to its style of computing where user can use applications and software on the Internet that stores and protect the data while providing a service[1].As a result, the technology of cloud computing has recently emerged as a new paradigm for hosting and delivering services over the Internet. Additionally, Cloud computing is being attractive to business owners as it eliminates the imminent plan for provisioning of resources. Moreover, it allows the enterprises to commence even from small scale. Furthermore, this technique increases number of resources purely on the basis of mounting in service demand. At present, cloud computing is defined by numerous organizations in their own way such as National Institute for Standards and Technology (NIST) [2] describes the Cloud computing as **"**a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction**"**. Berkeley [3] defined cloud computing as **"**to include application software delivered as services over the Internet and the hardware and systems software in the data centers that facilitate these services**"**. It is observed from aforesaid definitions that key characteristics of cloud computing include the illusion of infinite hardware resources, the elimination of up-front commitment and ability to pay for required resources.

Based on type of service provided to users cloud delivery models are exhibited as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). In IaaS user can avail computing services, data storage and networking infrastructure facilities. In other form, it can be described as delivery of computing infrastructure as a service. Examples of IaaS providers include Amazon EC2 [4], GoGrid [5] and Flexiscale [6]. PaaS is the delivery and deployment of computer applications over the internet with the consideration that all the parties needed in the development process are already obtained [7]. In PaaS user can utilize service provider's resources to run custom applications. Also, PaaS act as a development environment on which other higher level of services can be formulated. Examples of PaaS providers include Google App Engine [8], Microsoft Windows Azure

Corresponding Author: *rachnabtec@gmail.com*

© 2015, IJCSE All Rights Reserved

[9] and Force.com [10].In software as a Service,an application is hosted by the service provider and accessed via the World Wide Web by the client [11]. SaaS offers complete application as a service on demand. It also ensures that entire applications are hosted on internet and users can use them as per requirement. It eliminates the need to install and run applications on customer local computer. Examples of SaaS providers include Salesforce.com [10], Rackspace [12] and SAP Business ByDesign [13].

Depending on the purpose of setting up cloud and level of access to resources, there are four cloud deployment models: Public, Private, Community and Hybrid. Public cloud primarily owned by large scale organizations. The services offered by this cloud can be made available for the general public or a broad industry group while private cloud is owned solely by one organization and can be made available for a particular group. Public cloud raises concerns about the data privacy security since the computing infrastructure (computers, network and storage) is contained remotely outside the firewall of the company [14]. Private cloud reduces security risks as everything is managed inside the enterprise firewall allowing a fair used of the applications and the network bandwidth [15].Community cloud is deployed by one company and used by the others or provided by a third party over the Internet [16]. It can be shared and managed by the particular organization and supported by the specific community that has similar type of requirements. Hybrid cloud is composed of two or more clouds (private, public and community). In a hybrid cloud, some part of the service infrastructure runs in private clouds while the remaining part runs in public clouds.

Cloud computing is very dynamic concept and relatively has good number of benefits for its users. Today, businesses also need to keep up with the existing technology to provide real business solution due to advancement in cloud technology and increasing number of cloud users. Also, massive developments and implementations of cloud computing services indicate that the cloud computing services market is likely to reach between $150 billion in 2014 [17-18] and $222.5 billion in 2015 [19]. It seems that everyone is in the cloud when we see public clouds and private clouds or hybrid scenario. The existing cloud services are comprehensive to cover every domain such as Healthcare providers, eCommerce, data storage, etc. There are numerous advantages of cloud computing such as flexibility, elasticity and cost-effectiveness. Neverthless, there are frequent risks in cloud computing environment. Since data from various users and business organizations lie together in a cloud environment, breaching into the cloud environment will potentially attack the data of all the users. So functionality analysis and security analysis of existing techniques to secure data access in cloud environment becomes the desiarability of this era. Section 1 is current.Section 2 gives Related Works. Section 3 compares functionality of existing models. Section 4 provides the security analysis of the existing models .Section 5 concludes this paper.

II. RELATED WORK

Every organization transfers its data on the cloud utilizes the storage service provided by the cloud provider. Therefore, there is arising need to protect the data against the unauthorized access, modification or denial of services etc. The Security of data includes Availability, Confidentiality and Integrity. Confidentiality of data in cloud is accomplished by cryptography. The prime aim of cryptography is to take care of data from invaders. In today's time, cryptography is amalgamation of three types of algorithms i.e. (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Further, both symmetric and asymmetric-key algorithms can be used to encrypt data at cloud storage. Some popular Symmetric-key algorithms used in cloud computing are Data Encryption Standard (DES), Triple- Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish algorithms. The most common asymmetric-key algorithms for cloud are RSA, Diffie-Helman Key Exchange, Elliptical curve cryptography and IBE. SHA1 and MD5 are the examples for hash algorithms.

Xing Zhou et al. [20 implemented RSA algorithm to encrypt the data to provide security so that solely the concerned user can access it.In this model User data is encrypted first and then it gets stored in the Cloud. User places a request for the data to the Cloud provider as and when it requires. Cloud provider authenticates the user and delivers the data. The high risk on RSA encryption scheme evolved when the cryptanalysis attacks were successfully identified, where a 768 bit key can be easily broken down. RSA provides digital signatures which cannot be repudiated.

Eman M.Mohamed et al. [21] proposed that Amazon EC2 provider must use AES to ensure the most security in user data. They gave three advices to the Amazon EC2 cloud user, the first when you are not interested in higher security of the data and are interested about the performance of the algorithm then blowfish, DES or AES are used. The second advice is that when you are interested in higher security of the data then AES is used which is the highest security algorithm. Finally the third advice, AES is suitable to Amazon EC2 which it is the most secured and also takes less time to encrypt. Practically, it eliminates the possibility of weak and semi-weak keys in AES, which is an existing drawback of DES. AES is faster in both hardware and software. AES is more secure (as it is less susceptible to cryptanalysis). It needs more processing and requires more rounds of communication as compare to DES.

© 2015, IJCSE All Rights Reserved

Dubey et al. [22] in 2012 applied RSA and MD 5 algorithm for the encryption of cloud data. RSA algorithm is used for the encryption of data to be uploaded on cloud and private key is used by admin to decrypt the data. For updation of data administrator requests for a secure key to the user and user sends a secure key with a message digest tag for updation of data.

Prashant Rewagad et al. [23] in 2013 presented a method that utilize digital signature and Diffie Hellman key exchange blended with AES encryption algorithm in order to protect the confidentiality of data stored in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit has no use without user's private key, that is confined only to the legitimate user. In this protocol sender and receiver will set up a secret key to their symmetric key system by using an insecure channel. The problem in Diffie-Hellman key exchange arises when an attacker is capable of computing the random number generated by the client machine and he then compute the secret key from the random generated in order to break the scheme.

Alowolodu et al. [24] in 2013 proposed Elliptic Curve Cryptography scheme that acted as a secure tool to model a secured platform for the Cloud Application. Elliptical Curve Cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller and more efficient cryptographic keys. This model presented key strength as an important factor that is the difficulty in breaking the key and retrieving the plain text. ECC takes less time to encrypt the Data than others and also, will ensure the fast retrieval of Data.
Radhika G et al. [25] in 2013 implemented SHA1 and MD5 algorithms and deploying information into cloud in a secure way. It is proved from the obtained result, that Cryptography algorithms gives protection to the stored data in Cloud. The acronym for SHA is Secure Hash Algorithm. The purpose of SHA1 is authentication not encryption. In SHA1, the user gives an arbitrary size of input & it produces a fixed size of hash function and the size of hash function for SHA1 is 160 bits. The acronym for MD5 is Message Digest. MD5 is one way of hash function. MD5 algorithm takes an input of arbitrary length and produces a message digest i.e., 128 bits long. The size of hash function for MD5 is 128 bits.

Hongwei Li et al. [26] proposed a Hierarchical Architecture for Cloud Computing (HACC). The presented method inherited attractive properties from IBC such as certificate-free and small key sizes. This potentially offered a more lightweight key management approach. Based on the Hierarchical Architecture for Cloud Computing (HACC), it gave Identity-Based Encryption (IBE) and Identity-Based Signature (IBS) for cloud computing. They designed an Authentication Protocol which is more efficient and lightweight the node at each level of the hierarchy can give the access right to its subordinates. Based on the level of the user node the access rights to the users are issued and there by securing the data from unauthorized users.

Privacy homomorphism was introduced in [27]. Ideally, one should be able to transmit encrypted information to the server, process the encrypted data on the server and retrieve processed data from the server. This ideal situation, for long renown as the "Holly Grail of Cryptography", has finally got a brake through in 2009 by Craig Gentry in his Ph.D. thesis [28]. According to them any operation can be reduced to the basic addition and multiplication operations on bit level.

Craig Gentry et al. [29] showed that **"**fully homomorphic encryption can, in principle, be constructed which was put forth by Rivest Adleman and Dertouzos [RAD78] in 1978. According to this, an encrypted data can be processed without decrypting. Thus, we can get the cloud to perform a computation for us while revealing nothing of the input or output. It is quite complex and far from usable in practice. So the question of finding simpler, more efficient constructions as well as based on more traditional remained open.

Marten van Dijk et al. [30] presented a second fully homomorphic encryption scheme which uses many tools of Gentry's construction, but it does not require ideal lattices. **"**They illustrated that somewhat homomorphic component of Gentry's ideal lattice-based scheme can be replaced with a very simple homomorphic scheme by using just integers. The scheme is therefore conceptually simpler than Gentry's ideal lattice scheme, but has similar properties with regards to homomorphic operations and efficiency**"**.

Fully homomorphic encryption scheme has been implemented by the IBM research team conducted by S. Halevi and V. Shoup using ideas that can be found in [31], [32], and [33]. The implementation is called Homomorphic-Encryption Library (HELib) and can be found at:https://github.com/shaih/HElib.This software library implements the RLWE homomorphic encryption scheme, along with many optimizations to make homomorphic evaluation runs faster. HElib is written in C++ and uses the NTL mathematical library.The main issue in this context is the question if fully homomorphic encryption schemes are efficient enough to be practical for cloud computing. Craig Gentry estimated in an article [34] that performing a Google search with encrypted keywords would multiply the necessary computing time by around 1 trillion. A more scientific analysis of Gentry's fully homomorphic encryption system was done in [35], but Gentry's estimation should make clear that the performance penalty of this scheme is a big way to use it in practice.

© 2015, IJCSE All Rights Reserved

In [36], Lauter, Baehrig and Vaikuntanathan provided few concrete applications of homomorphic encryption and argued that there are many functions which could be useful for privacy preserving cloud services, which can be computed by many additions and a small number of multiplications on cipher-texts. For example, averages require no multiplications, standard deviation requires one multiplication, and predictive analysis such as logistical regression requires few multiplications.

Smart et al. [37] in 2009 presented a specialization of Gentry's scheme that yielded a smaller cipher text size. We present a fully homomorphic encryption scheme which has both relatively small key and ciphertext size. Our construction follows that of Gentry by producing a fully homomorphic scheme from a "somewhat" homomorphic scheme. For the somewhat homomorphic scheme the public and private keys consist of two large integers (one of which is shared by both the public and private key) and the ciphertext consists of one large integer. As such, our scheme has smaller message expansion and key size than Gentry's original scheme. In addition, our proposal allows efficient fully homomorphic encryption over any field of characteristic two.

Cramer, R et al. [38] introduced a new approach to multiparty computation (MPC) basing it on homomorphic threshold crypto-systems. They showed that given keys for any sufficiently efficient system of this type, general MPC protocols for n parties can be devised which are secure against an active adversary that corrupts any minority of the parties. The total number of bits broadcast is O (nk|C|), where k is the security parameter and |C| is the size of a (Boolean) circuit computing the function to be securely evaluated. An earlier proposal by Franklin and Haber with the same complexity was only secure for passive adversaries, while all earlier protocols with active security had complexity at least quadratic in n.They have given two examples of threshold cryptosystems that can support the construction and lead to the claimed complexities.

III. FUNCTIONALITY ANALYSIS OF EXISTING TECHNIQUES

Security of the data on cloud relies on trusted computing and cryptography. Cloud computing technology used multiple encryption techniques to get rid of different type of attacks. However security fails at some places. Hence Cloud computing is become a challenge and has supreme importance as many flaws and Security risks are yet to be identified.Few of the flaws and security risks faced by the cloud computing users are mentioned as:

i) Major encryption techniques are based on Symmetric and Asymmetric Encryption algorithms. Symmetric key encryption is highly vulnerable to attacks like brute force, cryptanalysis and system based attacks. Cloud computing providers prefer to use Asymmetric key encryption schemes for the betterment of the client data security.

ii) The security issue lies at a place where Cloud Server owners / attackers may compromise keys from Cloud Servers & process desired request and generate false positive results. Existing encryption schemes does not provide solution for security of shared keys.

iii) One of the main security based concern is where a customer may feel that server side personnel can re-use or misuse the credentials of their customers.

iv)Data providers need to list all the access levels and issue the authorization privileges accordingly, so that only intended users use the critical data.

v) Existing encryption schemes deals with single cloud that become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud.

vi)The major handicap of existing secure storage is that they do not allow the processing of data without decrypting it before or without revealing the keys used for encryption.

IV. SECURITY ANALYSIS OF EXISTING TECHNIQUE

According to Data Breach study of 2013, published by Ponemon and Symantec the Institute, the cost of the average consolidated data breach incident augmented from US$130 to US$136. However, this number can vary according to the country, where German (US$199) and US (US$188) companies have experienced much higher costs. Eight breaches in 2013 exposed more than 10 million identities and targeted attacks increased according to data collected and analysed by Symantec's security experts. The 2011 Internet Security Threat Report named the year 2011 as the Year of the Data Breachs and 2013 can best be described as the Year of the Mega Breach. The total number of breaches in 2013 was 62 percent greater than in 2012 with 253 total breaches. It was also larger than the 208 breaches in 2011. But even a 62 percent increase does not truly reflect the scale of the breaches in 2013. Eight of the breaches in 2013 exposed more than 10 million identities each. In 2012 only one breach exposed over 10 million identities. In 2011, only five were of that size. In total over 552 million identities were breached in 2013, putting consumer's personal information (credit cards, passwords, address details etc.) at risk.

During the analysis it is observed that all existing algorithms can easily decrypt the data by any encryption bypass attacks. Since, some basic encryption bypass attacks cannot be prevented such as Dictionary and Brute force are not prevented. Moreover, stated algorithms even do not provide total security to data, encryption keys at client side,

© 2015, IJCSE All Rights Reserved

Authentication at server side and Cloud Server side. Furthermore, these algorithms are dealing with single cloud and dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud.Besides, existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. The major handicap of existing secure storage is that they do not allow the processing of data without decrypting it before or without revealing the keys used for encryption. The above studies also do not provide facility for data provider to list all the access levels and issue the authorization privileges accordingly, so that only intended users can use the critical data to achieve data authentication.

The existing cloud security solution does not address various critical threats to cloud security and they do not provide a viable solution that eliminates various potential threats. So security needs to be addressed for securing transaction in such a way that transaction should be encrypted and not be decrypted during access.Moreover, access should be provided to the users as per their access rights. Security can be enhanced by use of multi cloud as single cloud that become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. The successful implementation of this technique can ensures the clients that their valuable data travelling over the network and stored on server side is encrypted & safe.

v. CONCLUSION

This paper contains a complete discussion of the cloud computing, service models, deployment models and cryptography techniques that have been used in cloud. It is observed from the functionality and security analysis that the cloud computing technology is not reliable for the users to use it without any worries.So there is a need of efficient framework to secure data access in cloud environment that can overcome all possible critical threats to cloud security.So that the benefits of cloud computing can be reached its maximum heights and propel in the direction it is designed for.

REFERENCES

[1] Introduction to cloud computing architecture [online]. Sun Microsystems USA: Santa Clara:Sun Microsystems 2009.URL:http://http://www.scribd.com/doc/17274860/Introduction-to-Cloud-Computing-Architecture, Accessed 08 June 2010.

[2] Peter Mell, and Tim Grance, Draft NIST Working Definition of Cloud Computing, 2009: from http://csrc.nist.gov/groups/SNS/cloud-computing/

[3] Michael Armbrust et al. Above the Clouds: A Berkeley View of Cloud Computing Technical report EECS-2009-28,UCBerkeley,http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html, Feb 2009.

[4] Amazon Elastic Computing Cloud, aws.amazon.com/ec2

[5] Cloud Hosting, CLoud Computing and Hybrid Infrastructure from GoGrid, http://www.gogrid.com

[6] FlexiScale Cloud Comp and Hosting, www.flexiscale.com

[7] Cloud computing [online].Cloud computing Asia: 2010.URL:http://www.cloudcomputinglive.com/asia/platform-as-a-service.html, Accessed December 08,2010.

[8] Google App Engine, URL http://code.google.com/appengine

[9] Windows Azure, www.microsoft.com/azure

[10] Salesforce CRM, http://www.salesforce.com/platform

[11] What is Saas and What are its advantages?[online]. Metaquote Software corp:2008-2011.URL:http://www.teamwox.com/en/teamwox/tutorials/71,Accessed September 15, 2010.

[12] Dedicated Server, Managed Hosting, Web Hosting by Rackspace Hosting, http://www.rackspace.com

[13] SAP Business ByDesign, www.sap.com/sme/solutions/

[14] Laying the ground work for Public cloud and Private Cloud [online]. Dell inc: 15 June2010.URL: http://whitepapers.businessweek.com/data/memberRegister.do,Accessed July 06,2010.

[15] CloudComputing UseCases White Paper [online]. SA(shared alike): July 2,2010. URL: http://www.scribd.com/doc/18172802/Cloud-Computing-Use-Cases-Whitepaper, Accessed July 21,2010.

[16] A community approach to cloud computing [online]. Orange Business Services:July-August 2010.URL:http://www.orangebusiness.com/en/mnc2/footer/news/enterprise_briefing/summer2010/cloud-computing.jsp ,Accessed July 23, 2010

[17] Deloitte. Executive Forum - Cloud Computing: risks, mitigation strategies, and the role of Internal Audit. Available: http://www.deloitte.com

[18] C. Pettey and B. Tudor. *Gartner says worldwide cloud services market to surpass $68 billion in 2010* Available: http://www.gartner.com/it/page.jsp?id=1389313

[19] *Cloud Computing Services - New Market Report Published*.Available:http://www.companiesandmarkets.com/r.ashx?id=41AETZYHJ289173&prk=ecb8413c602cb89051067456b636c7b9 , Press Office. (2010, 31 August 2010).

[20] Xing Zhou, Xiaofei Tang, Research and Implementation of RSA Algorithm for Encryption and Decryption, Department of Computer Science and Technology Harbin, china,2011.

[21] Eman M.Mohamed, Hatem S. Abdelkader, Sherif EI-Etriby ―Enhanced Data Security Model for Cloud Computing‖, The 8th International Conference on Informatics and Systems (INFOS2012) - 14-16 May Cloud and Mobile Computing Track.

[22] Dubey, Ashutosh Kumar, M. Namdev, and Shiv Shakti Shrivastava. "Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment",*Software Engineering (CONSEG), 2012 CSI Sixth International Conference on* IEEE, 2012.

[23] Prashant Rewagad, yogita pawar," Use of Digital Signature with Diffie Hellman Key Exchange and AES

© 2015, IJCSE All Rights Reserved

Encryption Algorithm to Enhance Data Security in Cloud Computing", CSNT '13 Proceedings of the 2013 International Conference on Communication Systems and Network Technologies IEEE computer society Washington,DC, Page No. (437-439),USA2013.

[24] Alowolodu, Ogundele, "Elliptic Curve Cryptography for Securing Cloud Computing Applications", International Journal of Computer Applications, Vol.- 66, No. -23, March 2013.

[25] Radhika G, K.V.V. Satyanarayana, Tejaswi A," Efficient Framework for Deploying Information in Cloud Virtual Datacenters with Cryptography Algorithms", International Journal of Computer Trends and Technology- volume-4,Issue-3,2013.

[26] Hongwei Li1, Yuanshun Dai1, 2, Bo Yang1," Identity-Based Cryptography for Cloud Security" http://eprint.iacr.org/2011/169.pdf.

[27] R. Rivest, L. Adleman and M. Dertouzos, "On Data Banks And Privacy Homomorphisms", Foundations of Secure Computation, Page No. (169–180),1978.

[28] C. Gentry, "A Fully Homomorphic Encryption Scheme", PhD Thesis, Stanford University, http://crypto.stanford.edu/craig, 2009.

[29] C. Gentry. , " Fully homomorphic encryption using ideallattices", In Proc. of STOC, ACM, Page No(169-178)., 2009

[30] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, "FullyHomomorphic Encryption Over the Integers", Advances in Cryptology, Eurocrypt 2010, Lecture Notes in Computer Science, Page No. (24–43), 2010.

[31] Z. Brakerski, C. Gentry and V. Vaikuntanathan, "Fully Homomorphic Encryption without Bootstrapping", Innovations in Theoretical Computer Science Conference, Page No. (309–325), 2012.

[32] C. Gentry, S. Halevi and N. Smart, "Homomorphic Evaluation Of The AES Circuit", Advances in Cryptology, Crypto 2012, Lecture Notes in Computer Science, Page No.(850–867), 2012.

[33] N. Smart and F. Vercauteren, "Fully Homomorphic SIMD Operations", Designs, Codes and Cryptography, 2012.

[34] C. Gentry, "Computing Arbitrary Functions Of Encrypted Data", Communications Of The ACM, Page No.(97–105), 2010.

[35] C. Gentry and S. Halevi, "Implementing Gentry's Fully-Homomorphic Encryption Scheme", Advances in Cryptology, EuroCrypt 2011, Lecture Notes in Computer Science, Page No.(129–148), 2011.

[36] M. Naehrig, K. Lauter and V. Vaikuntanathan, "Can Homomorphic Encryption Be Practical? ", ACM Workshop on Cloud Computing Security Workshop, Page No.(113–124), 2011.

[37] Smart, N. P., & Vercauteren, F. ," Fully homomorphic encryption with relatively small key and ciphertext sizes In *Public Key Cryptography–PKC"*, Springer Berlin Heidelberg, Page No(420-443),2010.

[38] Cramer, R., Damgård, I., & Nielsen, J. B. ,"*Multiparty computation from threshold homomorphic encryption",* Springer Berlin Heidelberg ,Page No(280-300),2001.

Rachna Jain , is currently working as an Assistant Professor in CSE Department of Bharati Vidyapeeth College of Engineering since Aug'2007. Prior to this she worked as a lecturer in N.C College of Engineering for one year .She completed her B.Tech (CSE) with honors from Kurukshetra University and ME (CTA) from Delhi University. She is Pursuing Phd from Banasthali Vidyapith. She has a total teaching experience of around 9 years. She is an active member of CSE Department and played an important role in various departmental and college level activities. She is also a co-coordinator of .Net In-house Summer Training programmed for second year students organized in the college every year. She is working closely in the areas of Speech, robotics, Network Security and Cloud Computing. She has also authored many papers, published in IEEE International Conferences, and International Journals of computer applications (IJCA),International Journal of Science Technology And management(IJSTM). She has also attended a number of workshops and faculty development programs inside and outside college.

Dr. Sushila Madan, is an Associate Professor at Lady Shri Ram College for Women, University of Delhi, Delhi. She is Ph.D. from Delhi University, M. Tech. (software systems) from BITS-PILANI and M. Sc. in Applied Mathematics from IIT Delhi. She has also submitted a project funded by UGC titled "Security Risk Management in E-Commerce".Dr. Madan has authored books on IT, Multimedia and web technology, Management Information and Control Systems, E-commerce and Essential PC tools. To her credit there are a number of research papers which have appeared in leading journals; some of which have been presented in conferences and included in conference proceedings; leading national level magazines and in-house journals of corporate sector. Moreover, white papers on the Internet are also available. Also she is a member of the Computer Society of India. biography appears here. Degrees achieved followed by current employment are listed, plus any major academic achievements. Do not specify email address here.

Dr.Bindu Garg, With 11+ years of experience in academia and Industry, she joined Bharati Vidyapeeth college of Engineering as Associate professor in August 2013. She completed her PhD in CSE from Jamia Millia Islamia, Central University at New Delhi under guidance of Prof. M.M Sufyan Beg and Prof. A.Q Ansari. She did her B.Tech (CSE) and M.Tech (CSE) with honors. Prior to Bharati Vidyapeeth, she worked as acclaimed faculty in India and abroad.

She was youngest to be awarded with Dr RAJENDRA PRASAD AWARD" by International Eminent Educationists Forum of India on 5th Sept 2008 to acknowledge meritorious achievements in the field of education, commitment of teaching and social work dedication. She was founder of NGO-YUKTI to serve weaker section of society. She is proficient in English, Hindi and French (DELF A1 Certified). She has attended multiple FDP's (Faculty development programs) and professional trainings. She has membership of many societies like: IEEE, CSI and ISTE. She is in review committee of numerous national & international conferences/journals.Her key research areas are: Soft Computing, Analysis & designing of algorithms and Time Series Prediction. she has 22 research publications in her credit.

 © 2015, IJCSE All Rights Reserved