# SECURITY ON BCCP THROUGH AES ENCRYPTION TECHNIQUE

**Narjeet Singh[1], Gaurav Raj[2]**

*Department of Computer Science and Technology, Lovely Professional University, Phagwara, Punjab*
***narjeetsingh7@gmail.com, er.gaurav.raj@gmail.com***

## Abstract

*Cloud is a virtualized server pool which can provide the different computing resources of their clients. Users of the system need only be concerned with the computing service being asked for. In contrast Cloud computing environments are likely to suffer from a number of known and unknown vulnerabilities and also enabling attackers to use computing and storage services unauthorized or distorted information (attack against cloud customer's data). It define that the most important issues in the cloud computing field is data security and privacy. Various mechanisms are available for achieving security by leveraging the capabilities of cryptographic techniques; it supports technologies for managing the data encryption and decryption algorithms. Encrypt sensitive data before placing it in the cloud. In this paper draws implications in data security and also presents various requirements covering the data security issues present in current cloud computing environments. In this paper, we present a framework to ensure data security in cloud computing is to enhance security as well as secure the privacy of the owner's data using AES within the cloud computing environment.*

.

***Keywords:*** *Cloud Computing; Cryptographic; Security; Broker Cloud Communication Paradigm (BCCP ;)*

---------------------------------------------------------------------***---------------------------------------------------------------------

## 1. INTRODUCTION

The data and the services provided reside in massively scalable data centers and can be ubiquitously accessed from any connected device all over the world. Most of the large companies have promoted their own cloud computing platforms and infrastructure for customers to deploy their web applications on these platforms.

The cloud is virtual computation resources that can manage it, usually for some large-scale server clusters, including processing server, storage server and network resources. The Cloud Computing will concentrate all computation resources, and can be managed automatically through the software without intervene. Users need not to be worried for tedious jobs like cost optimisation and network and data management. He can concentrate on his own business. This is favourable to innovation and to reduce the cost. Cloud computing has different means to different people. For Cloud computing, the common characteristics are to share on-demand and scalability of highly available with reliable pooled computing resources. It provide secure access to metered services from nearly anywhere, and dislocation of data from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud computing remains a work in progress. In Cloud computing, figure 1 shows a virtual pool of resources such as storage, CPU, networks and memory to fulfil the user's resource requirement and provides on demand (pay per use) hardware and software without barriers. It can be named as dynamic computing because it provides resources when required. Cloud Computing manages the pool of resources without human intervention and dynamically through software and hardware.

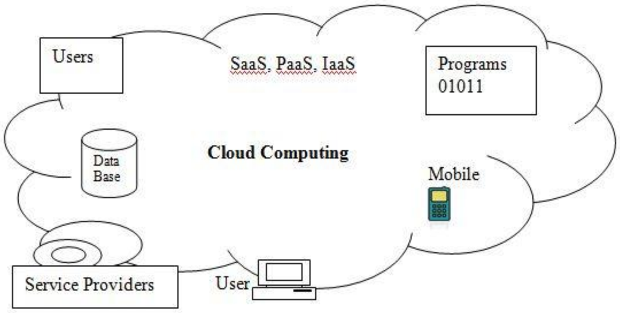


Figure 1: Cloud Services: Virtual pool [1].

Cloud computing can much improve the availability of IT resources and owns many advantages over other computing techniques. Cloud Computing is likely to have the same impact on software that foundries have had on the hardware industry. Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data-centres that provide those services. The services themselves have long been referred to as Software as a Service (SaaS), so we use that term. The data-centre hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the public, we call it a Public Cloud, the service being sold is Utility Computing. Current examples of public Utility Computing include AmazonWeb Services, Google AppEngine, Microsoft Azure, Gogrid and Rackspace. For example, it can provide self-help services without need any manual interactions with service providers and all the resources on the cloud are transparent to the users, that is users can dynamically lease physical or virtual resources and do not need to know the exact places of the resources existed. Besides, all the resources on cloud computing platform can be quickly and elastically deployed. Last but not least, as users can use the IT infrastructure with Pay per Use and On-Demand mode, this would be much benefit them and much save the cost [11] to buy the physical resources that may be not in use. Figure 2 to represents non- exhaustive view on the main aspects forming a cloud system [2].

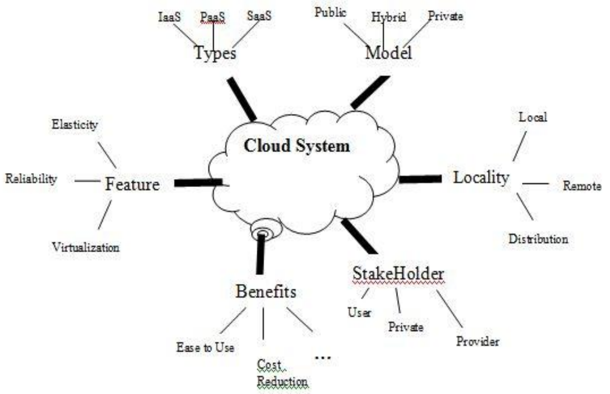


Figure 2: View on the main aspect forming a cloud system [2].

### (A). Cloud computing services

Cloud computing services are divided into three classes, according to the abstraction level of the capability provided and the service model of providers, namely: (1) Infrastructure as a Service, (2) Platform as a Service, and (3) Software as a Service. In this Figure 3 depicts the layered organization of cloud stack from physical infrastructure to applications [3].

| | | |
|---|---|---|
| SaaS | Web rowser | Cloud Applications<br>Social Network, Office Suit, Video Processing |
| PaaS | Cloud Development Environment | Cloud Platform<br>Programming Language , Framework, Structured Data |
| IaaS | Virtual Infrastructure Manager | Cloud Infrastructure<br>Computing Servers, Data Storage, Firewall, Load Balancer |

Figure 3: Cloud Computing Services [3]

***(1) SaaS (Software as a Service)***

Applications reside on the top of the cloud stack. Services provided by this layer can be accessed by end users through Web portals. It stands for Software as a Service. Service provider provides software services in the cloud. Users access software as a services as software and do his work without installing the same in the local machine. Google Apps provides such services to create documents and spreadsheets online without installing any document or spreadsheet application. Salesforce.com also provides software as a service [3].

***(2) PaaS (Platform as a Service)***

A cloud platform offers an environment on which developers create and deploy applications and do not necessarily need to know how many processors or how much memory that applications will be using. Platform as a Service allows users to use cloud computing for developing any application using development kit provided by cloud computing. Users are not required to install development kit on local machine, he can use installed software or development kit in cloud computing to develop any program. Oracle involves in providing platform as a Service [3]. There are Salient features of platform as services.

- Empowers developers to deploy, deliver and manage their applications. They can build applications, upload (deploy) the same into the cloud platform and simply run and test them.
- Developers can also leverage additional benefits like authentication and data access provided by the platform.
- While creating this kind of cloud computing platform, a vendor “builds a cloud platform first and then develops applications that run on it” or “develops a hostable application and then plugs it into the cloud”.

***(3) IaaS (Infrastructure as a Service)***

Offering virtualized resources (computation, storage, and communication) on demand is known as Infrastructure as a Service (IaaS). Infrastructure services are considered to be the bottom layer of cloud computing systems. Infrastructure as a Service enables us to install and execute the software. Here, users can gain access to virtualized server. IaaS targets operating systems, hardware, CPUs and embedded systems, networks and storage. This enables a homogenous virtualized environment where specific software will be installed and executed. Amazon provides infrastructure as a service [3].
There are Salient features of Infrastructure as a Service.

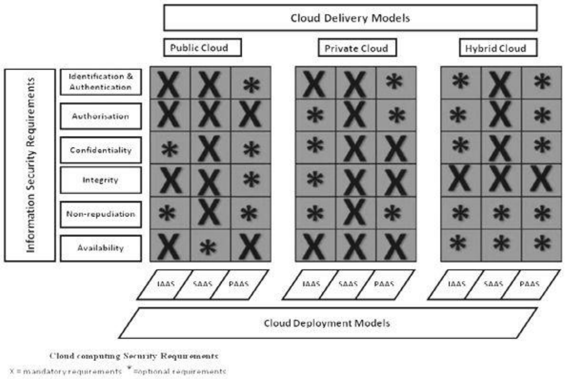
- Provides access to shared resources on need basis, without revealing details like location and hardware to clients.
- Provides details like server images on demand, storage, queuing, and information about other resources, among others.
- Vendors who provide this type of service enable cloud platforms and cloud applications. Some may even leverage

others within the space to provide competitive viability as well.

- Offers full control of server infrastructure, not limited specifically to applications, instances and containers.

## 2. RELATED WORK

Cloud computing environments are likely to suffer from a number of known vulnerabilities, enabling attackers to either obtain computing services for free (attack against cloud providers), steal information from cloud users (attack against cloud customers data) [4]. Cloud networking will not change the fact that vulnerabilities will continue to exist and that attackers will continue to exploit them. In the world of computing, security and privacy issues are a major concern and cloud computing is no exception to these issues. We provide a mechanism for achieving maximum security by leveraging the capabilities of cryptographic. Further we enhance the security of the encrypted data by distributing the data within the cloud. Privacy and security of data has always been a question and cloud computing is no exception to this. We believe that security and privacy of user data must be defined by broker. We provide architecture and guidelines to increase the security as well as the privacy of the owner data. We isolate the process of encryption and decryption from the cloud to a broker service that are trusted by both cloud provider and consumer. For maximizing the security of user data, we segment and encrypt the user data using a secured co-processor [4]. Cloud storage is built on the network computing environment. There are many benefits to move data into the cloud [5]. For example, users do not have to care about the complexities of direct hardware management. But since users stored their data in the cloud, it means that they will lose the control of them and more and more worries will come out about the data security. Data security is always an important aspect of quality of service and it is also a key issue in cloud computing. Cloud storage is used by a large number of individuals and enterprises. All data stored on their hard drive is not cared by user and no one knows where exactly data saved. Most of the data will be stored in a network computing system on top of the cloud, data security has become of great concern to the user. The same cloud system may exist in different types of customers, enterprises, individuals. Different users require different level of data security, and the ability to pay is different too, so the cloud computing system should prepare different levels of data security for different users. It does also embody the concept of cloud computing on-demand services [5]. In Figure 4 the information security requirements coupled with the Cloud computing deployment model and delivery models has been adapted [6]. In Figure 4, the different cloud delivery models and deployment models are matched up against the information security requirements with an “X” denoting mandatory requirements and an asterisk (*) denoting optional requirements. However future work is needed in investigating the optimal balance required in securing Cloud computing. Figure 4 should be viewed in context as a guideline in assessing the security level. Each of the security requirements will be highlighted below in context of Cloud computing [6].



| Information Security Requirements | Public Cloud | | | Private Cloud | | | Hybrid Cloud | | |
|---|---|---|---|---|---|---|---|---|---|
| | IAAS | SAAS | PAAS | IAAS | SAAS | PAAS | IAAS | SAAS | PAAS |
| Identification & Authentication | X | X | * | X | X | * | * | X | * |
| Authorisation | X | X | X | * | X | * | * | X | * |
| Confidentiality | * | X | * | * | X | X | * | X | * |
| Integrity | X | X | * | * | X | X | X | X | X |
| Non-repudiation | * | X | * | * | X | * | * | * | * |
| Availability | X | * | X | X | X | X | * | * | * |

Cloud Delivery Models
Cloud Deployment Models
Cloud computing Security Requirements
X = mandatory requirements * =optional requirements

Figure 4: Cloud computing Security Requirement [6]

In the ISO 7498-2 standard [6], produced by The International Standards Organization (ISO), Information Security should cover a number of suggested themes. Therefore by exploring the information security requirements at each of the various cloud deployment and delivery models set out by the ISO, vendors and organizations can become confident in promoting a highly protected safe and sound cloud framework.

### (A). Security Issues

In Cloud computing there are a number of main issues, which include issues of privacy, security, reliability and liability etc. But the most important between them is security and how cloud provider assures it. Number of security issues in cloud computing which are mentioned below.

### *(1) Problem Related to passive Attacks*

In passive attacks in cloud , the attacker only watches the transmission of cloud data’s and does not try to modify data packets or don’t do anything that user may realize that someone's watching him [7].

### *(2) Data location*

When clients use the cloud, they probably won't know exactly where their data are existing. Distributed data storage is a usual manner of cloud providers that can cause lack of control and this is not good for customers who have their data in local machine before moving from local to cloud [8].

### *(3) Privacy*

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users personal data may be scattered in various virtual data centre rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users [9].

### *(4) Data Integrity*

Data integrity in the Cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users). As data is the base for providing Cloud Computing services, such as Data as a Services, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task [8].

### *(5) Recovery*

If a cloud provider broke or some problems cause failure in cloud sever what will happen to users' data? Can cloud provider restore data completely? Moreover clients prefer don't get permission to third-party companies to control their data. This issue can cause an impasse in security [7].

### *(6) Freedom*

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring [9].

### *(7) Problem Related to Man in the Middle Attack*

In the man-in-the-middle attack (MITM) or bucket-brigade attack, or sometimes Janus attack, is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances [7].

### *(8) Long-term Viability*

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company. Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application [9].

### *(9) Security*

Your data more secure on your local hard driver or on high security servers in the cloud. Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security [12]. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can enter by force virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees accidentally exposing data on the Internet, with nearly 16 percent due to insider theft [7].

## 3. SECURITY IMPLEMENTATION ON BCCP

### (A). Broker Cloud Communication Paradigm for Data Security

1. Owner asks for service to execute tasks
2. Broker asks for specification of task.
3. Owner submits task specification.
4. Broker send request to cloud Exchange to search available clouds.
5. Cloud Exchange send request to all connected cloud coordinators.
6. Cloud coordinator updates available DataCenter information of the cloud to cloud exchange.
7. Cloud Exchange gives information of available of all clouds and data centres to Broker.
8. Broker send request to owner for send data.
9. Owner sends data into encrypted formed to Broker.
   (a) Data Owner encrypted data through AES technique.
   (b) AES performed numbers of round to encrypted data.
10. Broker send data to cloud coordinator which already encrypted by owner

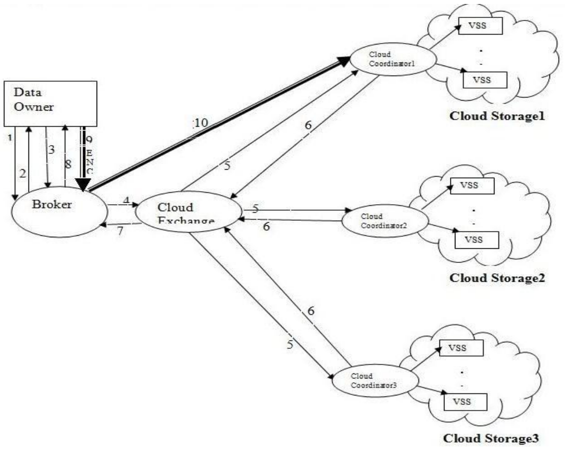


Figure 5: Broker Cloud Communication Paradigm for Data Security

ENC- Encrypted Data
VSS- Virtual Storage Server
→ Information Flow
→ Actual Data Transfer

### (B). Implementing AES Algorithm

Implement AES algorithm technique to secure Broker storage Cloud communication paradigm for Data security.

AES Algorithm Implementation
1. Data owner encrypted data through AES algorithm technique as follows

a. Initialize State XOR RoundKey are derived from the cipher key using
b. Initial Round
   i. AddRoundKey—each byte of the state is combined with the round key using bitwise xor
c. For each of the Nr-1 Round than
   i. SubBytes (State)
   ii. ShiftRow (State)
   iii. MixColumns (State)
   iv. Add RoundKey (State)
d. Last Round than
   SubBytes (State) ShiftRow (State)
   i. Add RoundKey (State)
   ii. Output as encrypted data generates.
   iii. Broker Send encrypted data to cloud coordinator.
   iv. Cloud coordinator is store the encrypted data to virtualized storage server.
   v.

## 4.IMPLEMENTATION RESULTS AND ANALYSIS

Paragraph content goes here. Paragraph content goes here In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

### (A). Analysis Result for Encryption algorithm AES and RSA

Performance of encryption algorithm is evaluated considering the following parameters.

- Computation Time
- Memory usage

The more CPU time is used in the encryption process, the higher is the load of the virtual machine's CPU. The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time. Comparisons analyses of the results of the selected different encryption scheme are performed. Experimental result for Encryption algorithm AES and RSA are shown in table 1, which shows the comparison of two algorithm AES and RSA using text file for five experiments. By analyzing the table 1, we noticed that time taken by RSA algorithm is much higher compare to the time taken by AES algorithm. Variation in memory usage is noticed.

| ***Data Type*** | ***Size (Kb)*** | ***AES*** | | **RSA** | |
|---|---|---|---|---|---|
| | | **Time** | **Memory** | **Time** | **Memory** |
| File 1 | 25 | 0.5 | 129040 | 1.2 | 135544 |
| File 2 | 57 | 0.7 | 129040 | 1.8 | 151984 |
| File 3 | 72 | 0.9 | 221656 | 2.4 | 231552 |
| File 4 | 95 | 0.9 | 222656 | 3.5 | 237215 |
| File 5 | 115 | 0.9 | 376184 | 5.1 | 402640 |
| File 6 | 130 | 1.0 | 406256 | 6.2 | 413731 |
| File 7 | 145 | 1.0 | 466312 | 6.6 | 470088 |
| File 8 | 162 | 1.2 | 471472 | 7.2 | 471078 |
| File 9 | 192 | 1.5 | 477000 | 8.1 | 481259 |
| **File 10** | 225 | 1.9 | 477156 | 9.7 | 483531 |

**Table 1:** Shows Time and Memory of AES and RSA

### (B) Comparisons of AES and RSA of Time and Memory

By analyzing Figure 6 shows execution time Taken for encryption on various size of text file using AES and RSA, it is noticed that RSA algorithm takes much longer time compare to time taken by AES.

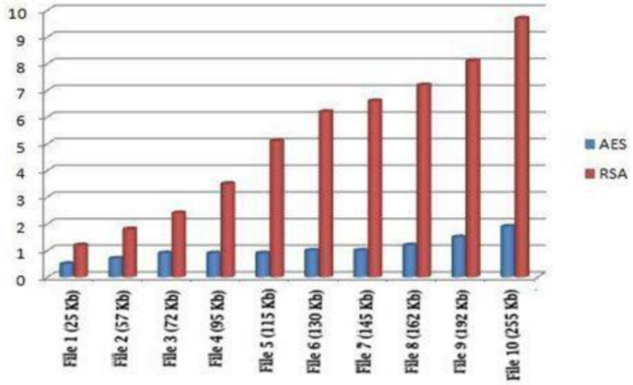


Fig6:Comparison of Computation Time among AES and RSA.

In Figure 7 which show memory usages by AES and RSA algorithm. It is notice that RSA algorithm memory usages are higher for all sizes of text file while memory usage should be least.

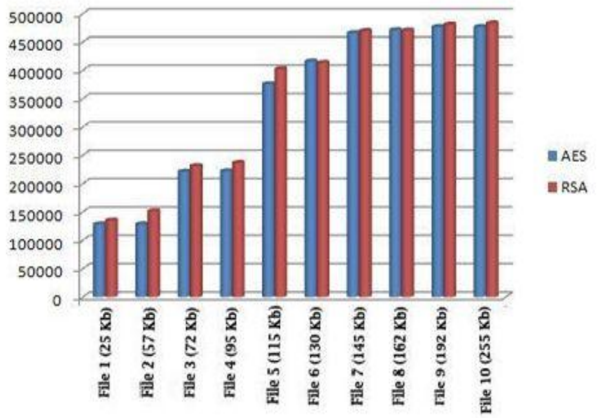


Figure 7: Comparison of Memory usage by AES and RSA

## 5. CONCLUSION

Cloud providers have to justify security issue and satisfy customer to purchase cloud resources in relatively lower cost and faster deployment of applications. Each of the Cloud providers has their own set of rules, pricing, flexibility, support and other important parameters. The key consideration dealt in this proposed scheme is how to secure data from the unauthorized person. In this proposal, we provide secure storage architecture and the process of communication with Broker Storage Cloud Communication Paradigm for data security. Also provide few guidelines that can be adopted by data owner in order to store and process the data securely. Implement AES for security over data provide benefits like it take less memory and computation time as compared to RSA, which has been displayed in tabular as well as graphical representations. This proposal provides wholesome security solutions. From this analysis, the data owner and user both can use storage cloud with AES security. It provide better solution to the data security for various cloud computing services It improves compatibility, implementation, deployment requirement, and development support and so on. Though each cloud infrastructure has its own security strength; the user can choose infrastructure according to his security requirements. According to us AES is better security for cloud in compare to RSA. We are also going to implement it over computing cloud to test whether it will work better in that scenario or not as our future work.

## REFERENCES

[1] Sameer Rajan and Apurva Jairath: “Cloud Computing: The Fifth generation of Computing”, 2011 IEEE.

[2] Keith Jeffery and Burkhard Neidecker-Lutz-“The future of cloud computing”, Opportunities for European Cloud computing beyond, 2010.

[3] William Voorsluys, James Broberg and RajKumar Buyya: “INTRODUCTION TO CLOUD COMPUTING”.

[4] Praveen Ram and Sreenivaasan, Department of Computer Science Engineering Rajalakshmi Engineering College, Anna University Chennai, India, “Security as a Service (SasS)” 2011 IEEE.

[5] Xiao Zhang, Hong-tao Du, Jian-quan Chen Yi Lin and Lei-jie Zeng, “Ensure Data Security in Cloud Storage” 2011 IEEE.

[6] Ramgovind S, Eloff MM, Smith E School of Computing, University of South Africa, Pretoria, South Africa,"The Management of Security in Cloud Computing" 2010 IEEE.

[7] G. Jai Arul Jose1, C. Sajeev, Research Scholar, Sathyabama University, Chennai, INDIA- “Implementation of Data Security in Cloud Computing” Aug Issue 2011.

[8] Minqi Zhou and Rong Zhang, “Security and Privacy in Cloud Computing: A Survey “2010 IEEE.

[9] Jianfeng Yang and Zhibin Chen “Cloud Computing Research and Security Issues” 2010 IEEE.

[10] Maheshwaran.M- Computer Science & Engineering School of Engineering Cochin University of Science and Technology-"Cloud Computing”, NOV 2008.

[11] Raj Gaurav, Lovely Professional University, Phagwara, Punjab, India *“An Efficient Broker Cloud Management*

*System"* in ACM proceeding through ACAI 2011 , July 21–22, 2011, Rajpura, Punjab, India.

[12] Farzad Sabahi Faculty of Computer Engineering Azad University Iran Cloud Computing *Security Threats and Responses*

Narjeet Singh was born in Khanna on 1th July. He received his MCA (CS) Degree from Punjabi University, Patiala and M.TECH Degree from Lovely Professional University in 2010 and 2012 respectively. His Research Interests include Cloud Computing, Grid Computing and Software Engineering etc.

Mr. Gaurav Raj received his M.Tech from Motilal Nehru National Institute of Technology, Allahabad. Presently he is working as Assistant Professor at Lovely Professional University Jalandhar, Punjab. His Research Interests include Cloud Computing, Grid Computing and wireless network etc.