**Cloud Publications**
International Journal of Advanced Cloud Computing and Applied Research
2012, Volume 1, Issue 1, pp. 5-10, Article ID Tech-05
ISSN 2320 - 0235

Case Study | Open Access

# Performance Analysis of Database on Different Cloud Computing Environments

**Gaurav Sharma**

Department of Computer, University College of Engineering, Rajasthan Technical University, Kota, India

Correspondence should be addressed to Gaurav Sharma, gaurav12mdr@gmail.com

Publication Date: 16 September 2012

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-05



**Abstract** Cloud computing provides a number of advantages to deliver services over the internet. The services are categorized into three distinct environments Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service. Now-a-days, a new emerging service called Database-as-a-Service which is a part of Software-as-a-Service. This service is prominent for database-driven applications. This paper lists important parameters of database. As a result, the performance analysis of database as MySQL varies significantly depending on the different cloud infrastructure such as Amazon EC2 and Joyent Cloud.
**Keywords** *Amazon EC2, Joyent, Xeround, MySQL, DBaaS*

## 1. Introduction

Cloud computing is technology that uses internet and control remote server to maintain data and application. Instead of installing set of software for each computer, you need to load your application and use it without installation every time and access personal files at any computer with the help of internet. Cloud computing is classified into three services: Infrastructure-as-a-Service, Platform-as-a Service and Software-as-a-Service even Database-as-a-Service (DBaaS) is included into Software-as-a-Service. This technology gives us efficient computing by centralized storage, memory, processing and bandwidth.

## 2. Amazon Elastic Cloud Compute EC2

Amazon Cloud EC2 provides cloud computing solution on the basis of as per usage. Amazon EC2 gives a web service API for manipulating, deprovisioning and provisioning virtual servers inside the Amazon Cloud. Amazon EC2 U.S. footprint has several data centres. Out of which, three data centres lie on the East Coast of the U.S. and two lie in Western Europe (1). We have to sign up separately for separate data centres account. In term of infrastructure, Amazon itself handles all the hardware and controls the network infrastructure. The servers are operated by Open Source Xen Hypervisor that provides facilities of dynamic provisioning, deprovisioning, and isolated computing environment for users (2). This paper is based on performance evaluation of database as a service on Amazon infrastructure.

### 3. Joyent Cloud

Joyent also provide cloud computing solution. Joyent provides public, private, or virtual private infrastructures across multiple data centres. Joyent infrastructure as a service incorporates load balancing and disk caching for improved input-output, enhanced security and reporting capabilities. Joyent Smart OS plays main role in an infrastructure service (3). It provides both KVM hardware virtualization and operating system level virtualization on single operating system. Moreover, Joyent Smart OS comprises DTree technology that gives visibility and insight. From security perspective, Joyent Smart OS delivers security and governmental standards including EAL 4+ compliance that isolate network processes storage and memory on virtual server (4).

### 4. Xeround

Xeround provides Database-as-a-Service (DBaaS) for MySQL database. Xeround delivers configuration and optimization to performance of database and availability on the cloud. Xeround works on tier-II architecture. This architecture is classified into two nodes: Access nodes and Data nodes. Access nodes are used for receiving application requests, communicate with data nodes, perform computations and deliver results while data nodes are used for storing data. The data storage is handled by virtual partitions. Each partition is available to the different data nodes located on separate servers and provide high availability. Xeround first keep our databases in two synchronous in-memory replicas, and then keeps our databases into persistent store such as Amazon EC2, Joyent and Rackspace asynchronously (5).

### 5. Methodology & Metrics

The goal of this performance evaluation is to study about throughput under different cloud infrastructures as Amazon EC2 and Joyent. To this end, we ran MySQL databases on different cloud infrastructures such as Amazon and Joyent cloud with the help of Xeround and measures throughputs and analysis which one infrastructure is best suitable for database-driven applications. We have used Webyog for the purpose of monitoring MySQL databases. Moreover, this paper reveals MySQL metrics on the basis of different cloud infrastructure such as Amazon EC2 and Joyent cloud.

We have taken following parameters:

#### a. Threads

Thread is created for each connection to the MySQL server and threads creation take time and resource. Threads cache holds threads that are not being used by any connection. Thread cache used threads that are available and not being used by any connection. We can find out number of threads in the cache by the thread_cache_size variable. Each thread normally uses 128KB of memory. The observing point is that always check Threads created and make sure that number of threads created per second should not be more than one. Last but not least, MySQL response should be much faster if it is using threads from cache and not creating them (7).

#### b. Table Cache

When MySQL access table, it stores table in the cache. It is called table cache. We should always check opened table status variable. If you observe that number is going to be large, you will have to increase the value of table cache by table cache variable. Hence, MySQL queries time will be faster with the help of table cache instead of opening the table file for each query (7).

**c. Query Cache**

The query cache stores the text of select statements together with the corresponding result that was sent to the client. It is very prominent for read-intensive applications. It enables very fast retrievals on cache query hit by storing query cache completely in memory. We can control the size of query cache by query_cache_size variables. The value should be in the range of 64MB to1024MB (7).

**d. Read Buffer Size**

Read buffer is generally used as storage. MySQL does not allocate memory until needed to query. In this way, the value of this variable should be smaller than 1MB.

**e. Table Locking**

Table locking enable many sessions to read from a table at the same time. If you want to write to a table, you will have to get exclusive access and wait for the other session to finish it. All other table have to wait until update is completed (7).

**f. MyISAM Key Cache**

MyISAM has capability of table locking and repair table functionality. It is usually used to minimize disk Input-Output and improve key cache performance. It uses index block where most used index block is stored and data block uses native operating system cache to store most used data block (7).

## 6. Results

We have observed following throughput regarding to the different cloud such as Amazon EC2 and Joyent cloud:

**a. General Parameters**

- *Connections*: The number of connection attempts whether it is successful or not to MySQL server.
- *Connection Used*: The number of connection is being used to MySQL server.
- *Bytes received from all clients:* The value indicates the amount of incoming network traffic to the MYSQL server.
- *Bytes sent to all clients:* The value indicates the amount of outgoing network traffic from the MySQL server.
- *Terminated abruptly*: The number of connections that were established successfully but got terminated abruptly. This might happen if the client does not the connection gracefully or the client had been sleeping more than wait timeout second (7).

**b. Data Manipulation language**

The total number of data manipulation statements that client have sent to the MySQL server. The data manipulation statements comprise SELECT, INSERT, UPDATE and DELETE commands.

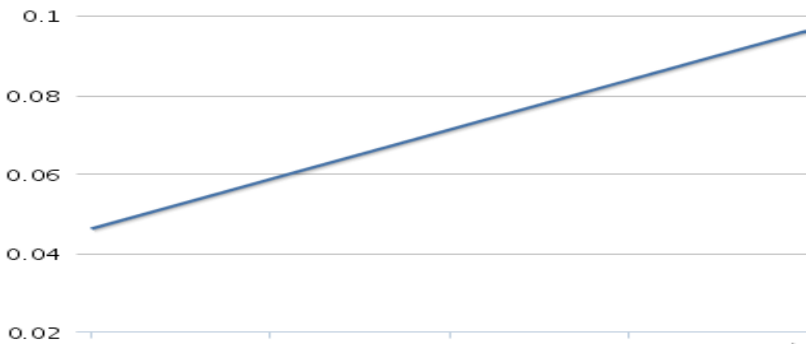



***Figure 1:*** *A Data Manipulation Language graph which demonstrates number of statements sent by client values/sec on Amazon EC2 cloud.*

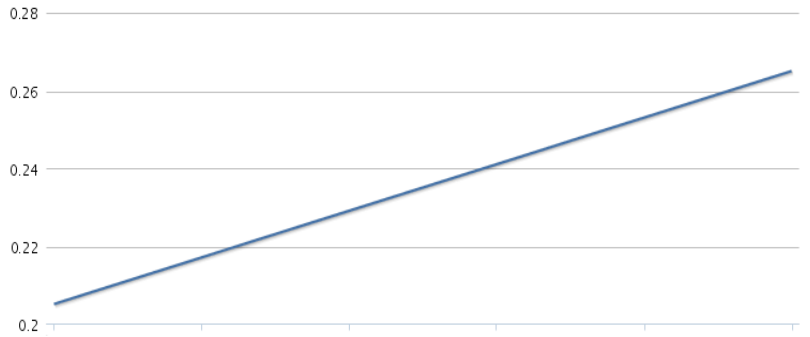



***Figure 2:*** *A Data Manipulation Language graph which demonstrates number of statements sent by client values/sec on Joyent Cloud*.

### c. MyISAM Key Cache

MyISAM key cache stores most frequently used index block and data block. It comprises

- *Allocated Memory*: This is common to both databases on different cloud such as Amazon EC2 and Joyent.
- *Block requested from cache*: The number of key requests from key cache.
- *Total block written:* The number of requests to write a key block into the MyISAM key.
- *Used block*: The number of blocks used from the key cache.

### d. Thread Cache

- *Thread cache size:* The thread creation is time consuming activity. It reveals size of threads cached.
- *Thread cache hit rate*: This variable shows hit rate of thread cache. The value is low indicates increasing thread cache.
- *Thread created*: It reveals number of threads created to handle connections. The increasing value of thread creation indicates insufficient size for thread cache.

### e. Query Cache

- *Query in cache:* The numbers of queries currently stored in the Query cache.
- *Query cache hit*: The number of queries that served successfully by query cache.
- *Query cache hit ratio:* Usually, query cache is used to improve speed of application. The cache hit rate should be high.

### f. Table Cache

- *Table open*: It shows the number of tables that are currently opened.
- *Number of table cache*: The number of table request that are not handled by table cache.

### g. Table Locking

- *Table locks*: The number of times table getting table lock.
- *Table lock waited:* It indicates the number of times wait was needed before getting table lock (7).

***Table 1**: MySQL Performance Table*

| MySQL Parameters | Amazon EC2 | Joyent Cloud |
|---|---|---|
| Number of open Connection | 4 | 3 |
| Connection used | 80.00% | 60.00% |
| Bytes Received | 11.22K (37.931/sec) | 7.96K (26.993/sec) |
| Bytes sent | 47.03K (158.931/sec) | 35.61K (120.742/sec) |
| Termination | 0.00 | 0.00 |
| Total number of Data Manipulation Language (DML) | 29.00 (0.096/sec) | 80.00 (0.265/sec) |
| Thread Cache Size | No thread in Cache | No thread in Cache |
| Thread cache hit rate | 0.00 | 0.00 |
| Number of Thread created | 29.00 (0.096/sec) | 21.00 (0.070/sec) |
| Table currently opened | 29 | 29 |
| Number of table cache | 1.76K | 1.76K |
| Number of times Table locked acquired | 22.00 (0.073/sec) | 79.00 (0.262/sec) |
| The number of times Table lock waited | 0.00 | 0.00 |

## 7. Conclusion

This paper represents performance analysis of database as MySQL on different cloud environments as Amazon EC2 and Joyent cloud. The main aim of this paper is to assess performance of MySQL database because most of the applications are database-driven. For this reason, database-driven

related applications are directly affected by performance of its databases in cloud computing. Thus, according to my experiment, we observed comparison between MySQL servers which are associated with different cloud environment as Amazon EC2 and Joyent Cloud. I would like to go on this way further to evaluate NoSQL databases as Cassandra and Hadoop on different cloud environment.

**References**


1. Ben-Yehuda et al., 2011: Deconstructing Amazon EC2 Spot Instance Pricing, CLOUDCOM '11 Proceedings of the 2011 IEEE Third International Conference on Cloud Computing Technology and Science, 304-311, IEEE Computer Society Washington, DC, USA.

2. Guohui Wang et al., 2010: The Impact of Virtualization on Network Performance of Amazon EC2 Data Center, INFOCOM'10 Proceedings of the 29th Conference on Information Communications, 1163-1171, IEEE Press Piscataway, NJ, USA.

3. Joyent Cloud. The Joyent Smart Technologies Architecture for Cloud Computing. [White Paper] Retrieved from http://www.joyent.com/documents/whitepapers/Joyent-Smart-Architecture-for-Cloud-Computing.pdf.

4. Joyent Cloud. The Joyent Smart Data Centers. [White Paper] Retrieved from http://www.joyent.com/documents/whitepapers/Joyent-Smart-Architecture-for-Cloud Computing.pdf.

5. Xeround. Cloud Database Whitepaper. (2012). [White Paper] Retrieved from http://xeround.com/main/wp-content/uploads/2012/03/Xeround-cloud-database-whitepaper.pdf

6. Donald Kossmann et al., 2010: An Evaluation of Alternative Architecture for Transaction Processing in the Cloud, SIGMOD '10 Proceedings of the 2010 ACM SIGMOD International Conference on Management of Data, 579-590, ACM New York, NY, USA.

7. MONyog. MONyog MySQL Parameters. [White Paper] Retrieved from http://www.webyog.com/en/whitepapers/MONyogWhitePaper.pdf.

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2012, Volume 1, Issue 1, pp. 1-4, Article ID Tech-06
ISSN 2320 - 0235

Research Article | Open Access

# Professional and Ethical Issues in Semantic Web

**Pankaj Kumar [1] and Dr. A. K. Singh [2]**

[1, 2] University Department of Mathematics, B. R. Ambedkar Bihar University, Muzaffarpur, Bihar, India

Correspondence should be addressed to Pankaj Kumar, pankaj@glug4muz.org and Dr. A. K. Singh, aksingh@brabu.net

Publication Date: 16 September 2012

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-06



**Abstract** This paper highlights professional and ethical issues in semantic web environment. As in case of semantic web environment information is more visible to search engines and other websites and so it raises significant privacy issues for users providing personal data on a semantic website. This paper also highlights the importance of informed consent in a semantic web environment. Finally it explores the challenge for developers and designers of semantic web environment and potential approach to meeting these issues in an efficient way.
**Keywords** *Semantic Web, RDF, OWL, Ethics, Privacy, Informed Consent*

## 1. Introduction

The main aim of semantic web (1) is to develop a website in which data available on it becomes as much visible to other websites as it is visible to its users. The information available on such websites becomes much more sharable as compared to information available on traditional websites. So the privacy issue for users signing up on these websites becomes more critical. The information provided by users become available in the source code of the web pages in very systematic way so that they can be easily scrapped by crawlers and other websites. The information provided by users may even become available in the URL of the web pages of that website. So such situation may become problematic for users. Some of the sensitive information given by the users can also become accessible on other websites. So it may violet the consent given by the user at the time of creating account on that website. Therefore the ethical responsibility of designer and developer of such website become much more than as compared to traditional websites.

## 2. Introduction to Semantic Web

Traditionally Internet was developed as collection of static web pages. It was simply collection of documents. But now the Internet has become collection of data. The documents available on Internet are collection of data provided by users. Traditionally it was one way communication between the website owner and visitor. But now days, the information available on web pages mostly consists of information provided by visitors itself. So one visitor is interested in searching for information provided by other visitor. The main aim of semantic web is to develop this searching process easy and accurate. For this purpose, the methods of displaying information on web pages are being redefined.

Therefore some advanced format of data representation has been defined such as RDF (2) (Resource Description Framework) and OWL (3) (Web Ontology Language). In addition to this, some frameworks have also been developed such as FOAF (4) (Friend of a Friend).

## 3. Privacy and Semantic Web

The method of integration of personal information in a semantic website is very critical. It should be done in such a way that the private information provided by the user should not be accessible by search engines or other websites. For this purpose the user should be provided with option to make his own information either private or public on such websites. Only information declared public by the user should be accessible by the search engines. The developers of such website must take care of the fact that any private data provided by the user should not become available in any data feed provided by such website. Similarly such information should also not be integrated in the URL of the web pages of that website. The main features of semantic web due to which the information on such website become more accessible are as follows:

### A. Universal Data Representation

As all data will be represented with the help of universal data representation format and so they can be easily queried by other websites.

### B. Ease of Integration

The integration of data in a semantic website is more easy and systematic. So the volume of data integrated into such website becomes much more as compared to traditional websites. So there will be more chance of sharing of private data from such website.

### C. Persistence of Data

Due to easy reusability of data available on semantic website, the data becomes more distributed as compared to traditional websites. So it also becomes more persistent. So it may happen that even if data has been removed from the original web page it may remain available on other web pages. So this also increases the chances of sharing of private data item in such cases.

## 4. Informed Consent and Semantic Web

Informed consent (5) implies the agreement accepted by the user while signing up on a website. This concept has been taken from the field of medical practice and research. It is associated with the fundamental right of a person. As the risk of linkage of data in semantic web environment is much higher and so the chances of break of informed consent become more vulnerable in such cases. The informed consent in a semantic web environment should have following features:

### A. Disclosure

It should disclose accurate information to the user. It should disclose both the benefit and harm which may occur to the user.

### B. Comprehensive

The matter written in the agreement must be easy to comprehend by the user. It should also be complete in nature.

### C. Agreement

The user must be provided clear opportunity to accept or deny the agreement. If possible then the user must be provided to cancel the agreement after some time. However this facility is not easy to be implemented in a semantic web environment as once agreement is made between the user and the website owner then the information given by the user is shared by so many websites and become out of control from the original website. The method of agreement should be implemented in such a way that the user should be forced to read whole agreement before clicking on the “I Agree” button.

## 5. Exploring Solution in Semantic Web

The privacy and ethical issues are arising with the evolution of the semantic web. These issues will co-evolve along with the semantic web. In order to tackle with these issues the following points should be considered in a semantic web environment:

### A. Education of Developers

The developers of semantic website should be educated from the point of the view that before making accessible any information given by the user, they should think twice about its nature. They must understand the situation and nature of information provided by the users. They must understand their responsibility before making public any data provided by the user on these websites.

### B. Education of Users

The users must be educated from the point of view of importance of informed consent. They should be educated to read carefully the text written in the agreement before clicking on the “I Agree” button. They should also be educated about declaring their information private or public on a website.

## 6. Conclusion

The concept of semantic web has significantly raised the issue of ethics in the world of Internet. In today’s world when everyone is busy in uploading personal information on web, the privacy of uploaded data has become a very sensitive issue due to easy sharing of information among websites. Now-a-days everyone is feeling secured after uploading scanned copy of his document on his account of a website. In addition to this everyone is also providing personal information such as Driving License Number, PAN Card Number, Educational Certificate Details etc. on website account. Uploading of such information are done from the point of view of backup of these information. But these information are also being shared to other websites in known or unknown way. And the implementation of semantic web technology has made this sharing more fast and accurate. So it has ultimately increased the responsibility of web developers to implement the concept of semantic web on websites in such a way that the personal information uploaded by users on a website must not be shared without their consent. The future of web from the point of view of implementation of semantic web technology is very exciting but professional and ethical issue about the user personal data must always be taken into consideration by web developers.

## References

1. W3C cited, 2012: Semantic Web. [http://www.w3.org/standards/semanticweb/]

2. W3C Semantic Web cited, 2004: RDF - Semantic Web Standards. [http://www.w3.org/RDF]

3. W3C cited, 2009: OWL 2 Web Ontology Language Document Overview. [http://www.w3.org/TR/owl2-overview/]

4. The Friend of a Friend cited, 2000: FOAF Project. [http://www.foaf-project.org/]

5. Paul Shabajee, 2006: Informed Consent on the Semantic Web - Issues for Interaction and Interface Designers, Proceedings of the Third International Semantic Web User Interaction Workshop (SWUI 2006), Fifth International Semantic Web Conference (ISWC 2006), Athens, GA.

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2012, Volume 1, Issue 1, pp. 11-19, Article ID Tech-21
ISSN 2320 - 0235

Research Article | Open Access

# Migrating Process and Virtual Machine in the Cloud: Load Balancing and Security Perspectives

**Varsha P. Patil[1] and G.A. Patil[2]**

[1, 2] D.Y. Patil College of Engineering & Technology, Kolhapur, Maharashtra, India

Correspondence should be addressed to Varsha P. Patil, varshappatil96@yahoo.co.in

Publication Date: 26 November 2012

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-21



**Abstract** For the purpose of load balancing, migration of VM instances or processes in cloud environment is quite useful. However, the live migration of VM is insecure. There is necessity of incorporating encryption and authentication mechanisms during migration process. An attempt is made to secure live migration of virtual machine and running processes from one machine to another. In this system, the virtual machine migration has been carried out by considering load balancing parameters like memory usage, disk usage, CPU usage, network bandwidth and total number of processes. CentOS with Xen virtualization package and python script is used for live migration of VM from one physical host to another. This paper highlights on secure live migration of VM using RSA with SSL protocol. Process migration has been handled with MOSIX software and tools.
**Keywords** *Live Migration, Process Migration, VM, Xen, Load Balancing, Encryption, SSL, MOSIX*

## 1. Introduction

Today, many organizations are still using the cloud computing technology offered for getting the services like hardware's and softwares. Virtualization technology is used to achieve the scalability property of cloud computing system. The use of virtualization has become increasingly popular in organizational network.

The operators and administrators are turning to live migration of VM (Virtual Machine). It allows separation between hardware and software. Also, it facilitates load balancing, fault tolerance & low level system maintenance. Live migration of VM is the process of moving a VM from one physical host to another with little or no downtime for services hosted by virtual machine. The live migration functionality is provided by vendors such as Xen, VMware, OpenVZ and VMotion. Due to increased demand in use of virtualization technology, it is essential to provide live migration of virtual machine in a more secured manner. Virtual machine is typically stored as regular file on the disk & this file is migrated from one host to another using network system. The network across which VM instance is migrated is not entirely secure. Secured live migration of VM is required because the attacker inside a

network employing live migration can facilitate untrusted access to migrating VM image. The attackers can view or modify the data associated with VM instance.

## 2. Literature Review

In the past, different systems have been designed for VM migration. A load balancing method has been designed and implemented for live migration of virtual machine [2]. The distributed algorithm COMPARE_AND_BALANCE assured the migration of virtual machine from physical host with higher cost to physical host having lower cost [3]. It also gives the logical steps for migrating VM between two physical hosts. Three classes of threats to VM migration are control plane, data plane & migration module [4].

In previous systems, software and hardware dependencies problems were occurred in process migration between machines [8]. In software dependencies, suppose a dynamic library is loaded at 0x007c0000 in virtual space of process. Since the process is already loaded the 0x007c0000 address is hard coded by the operating system loader. The process need to be reloaded on the host machine with correct address to avoid address conflicts. In hardware dependencies, if one machine has ARM Processor and another has Intel Processor then OPCODEs of machines are different. When the process is migrated from one to another then there is a need to change the opcodes, but some opcodes for specific function is not available like graphics processor.

Many systems are developed for live migration of virtual machine for load balancing using Xen, OpenVZ, VMware and VMotion. The limitations of existing systems used for live migration of VM are as under:

a. The migration for OpenVZ virtual machine is still slow.
b. The VMM component implementing the live migration functionality is vulnerable to attacks.
c. During live migration, sensitive information of Guest OS may be leaked or compromised.

The necessity was felt to overcome these above challenges by using various virtualization techniques and securely migrating live VM, processes and applications.

## 3. Secure Migration Process

The work presented in this paper focuses on secured live migration of virtual machine from source host to destination.

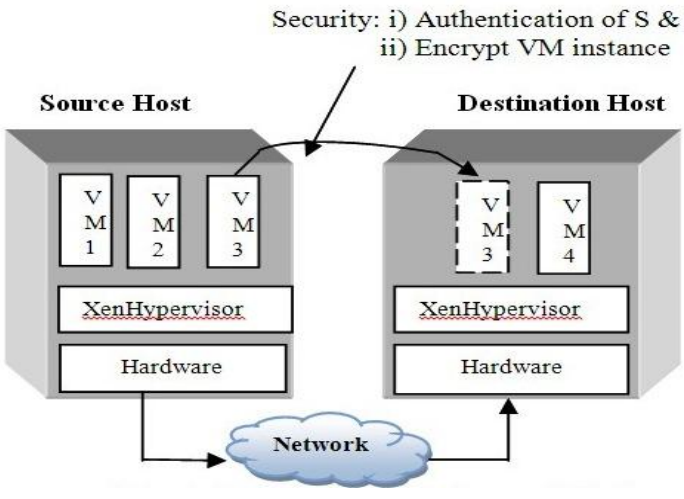



***Figure 1:*** *Secure Migration of VM's*

The entire process of migration includes following stages:

**Stage 1.** Check the load on physical hosts by considering the following parameters:

a. Memory usage
b. Disk usage
c. CPU usage
d. Network bandwidth
e. Total number of processes

The monitoring node will calculate load by considering above parameters and classifying the physical host into lightly loaded and heavily loaded. Whenever any node becomes overloaded due to any reason then load balancing algorithm starts and performs the VM migration. Migration of VM is one of the best ways to balance the load.

**Stage 2.** Live migration of VM from one physical host to another is done using pre-copy or post-copy method by considering following steps:

a. Reservation of resources on destination host.
b. Transferring the memory pages of virtual machine from source to destination.
c. Stopping the execution of the virtual machine running on source host and transferring modified memory pages from source to destination host.
d. Activating the execution of virtual machine on destination host.

**Stage 3.** The suitable encryption cryptography mechanism needs to be used for encryption and authentication. The suitability can be decided on the following factors:

a. Time required for encryption.
b. Strength of encryption algorithm.
c. Authentication support.
d. RSA has been used to provide authentication and confidentiality.

**Stage 4.** Process Migration from one physical host to another is carried out by using MOSIX software and Tools. In this system, process migration has been carried out by considering CPU usage load Balancing parameter. CentOS with Mosix software package is used for migration of process or application from one physical host to another.

## 4. Experimental Setup

The experimental setup is done by configuring the network in the intra-network of 25 systems which contains four node servers for load balancing, connected by cat6 cable through Ethernet switch (100 Mb/s). CENTOS with XEN virtualization package is installed on these machines. Each machine executes Domain0 as a default VM and node server collects the load information like CPU, memory, network and disk usage from each node. One of the four nodes is configured as collector and another as a node server.

The information collected from all nodes is used to find the load. The threshold for overloading on a node is considered as 75% of total workloads. The scripts are written for migrating VM from heavily loaded node to lightly loaded node based on the threshold value. The live migration of virtual machine has been done from node 2 to node 1 as shown in figure 2.

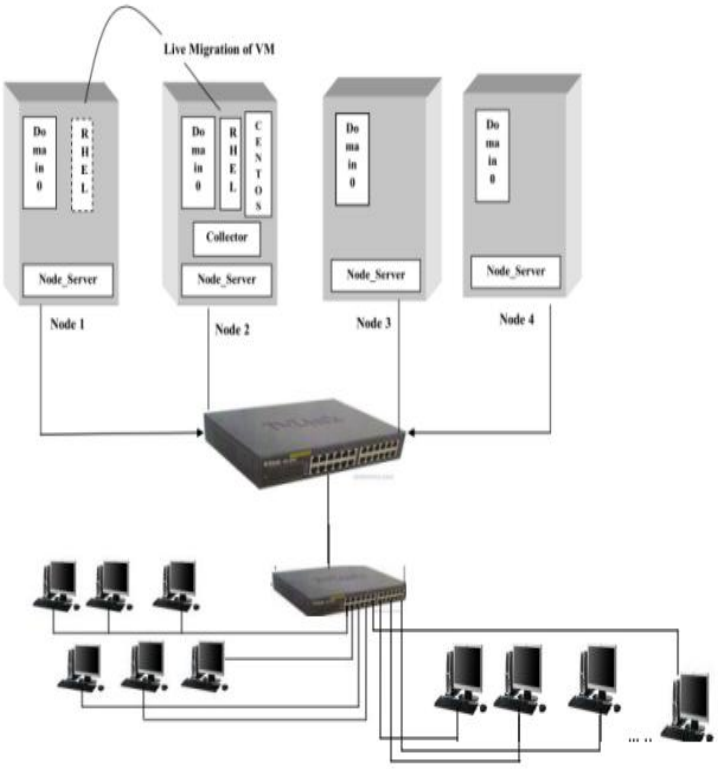



***Figure 2:*** *Experimental Setup*

## 5. Implementation

The implementation has been carried out by using CentOS which is Community ENTerprise Operating System based on Red Hat Enterprise Linux [7]. CentOS provides Xen virtualization package to perform the live migration of VM and CentOS with MOSIX software has been installed for performing process migration.

### 5.1 Live Migration of VM

Different scripts are written for load calculation and VM migration using python scripting language. Figure 3 depicts the mechanism for calculating the load by collecting the information from other nodes.

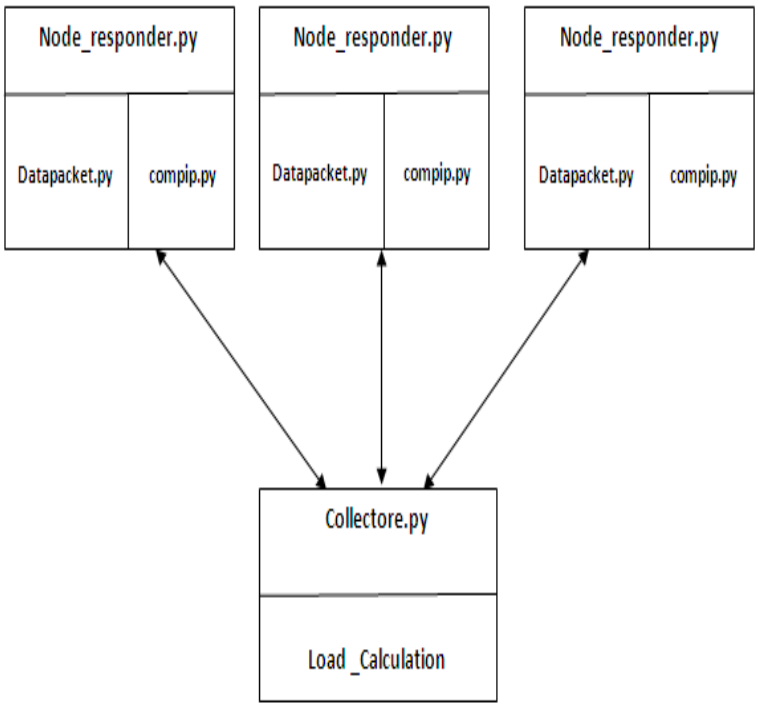



***Figure 3:*** *Load Calculation*

Few of them are mentioned below:

i) Collector.py: This graphically displays CPU usage, memory usage, disk usage, and network usage and load factor of each node.

ii) Node_responder.py: Usage data is collected from each node and sent the collector node.

iii).Avg_algorithm.py: The System Average Imbalance algorithm has been implemented to calculate load factor by considering parameters like CPU usage, memory usage, disk usage and network usage.

iv) Executer.py: If load value is greater than threshold value then VM will be migrated to lightly-loaded node.

**5.2 Dynamic Load Balancing**

The System Average algorithm calculates the load factor from load usage. The load factor can be calculated using following formula:

$$\text{Load factor} = (cu + du + mu + nb)/4$$

Where, cu -CPU usage, du-disk usage, mu-memory usage, nb-network bandwidth.

**5.3 Secure Live Migration of VM**

Secured live migration of VM has been performed by using RSA with SSL protocol:

i) The Xend server first saves the states of machine then transfers the states to other host. Other machine restores the states of virtual machine and then starts the guest machine executions.

ii) To save the state of the machine XendChepoint.save function is used. To restore the machine XendCheckpoint.restore function is used.

iii) Relocation protocol is waiting for a command. Whenever it receives 'receive' command then relocation protocol transfers the virtual machine and the virtual machine resumes at the other end.

### 5.4 Process Migration

Process migration is done by using MOSIX software and tools:

i) Start the Mosix daemon using mosd tool.
ii) Get the load information displayed in the form of graph using mon command.
iii) Run the process using the command,
# mosrun. /server
iv) Process information is displayed using MOSIX tool,
# mosps -AMn
v) Migrate the process using migrate command,
# migrate 4115 192.168.100.2

## 6. Result Analysis

The live migration of virtual machine was done by using Xen virtualization package and python programming language. RHEL and CENTOS Virtual Machines are migrated between two laptops and 4 machines within LAN. The migration time is based on virtual machine size and network traffic. RHEL and CENTOS Virtual Machines are migrated within different network traffics. The Migration Time and Virtual Machine size is shown in table 6.1, table 6.2 and table 6.3 in low, average and heavy traffic environments respectively.

***Table 6.1:*** *Migration time in low network traffic environment*

| Test No. | Virtual Machine | VM Size | Migration Time | Descriptions |
|---|---|---|---|---|
| **1.** | RHEL | 2.99GB | 12 sec & 782 ms | Tested on 2 laptop using cross cable |
| | CENTOS | 3.99GB | 46 sec & 880 ms | |
| **2.** | RHEL | 2.99GB | 12 sec & 743 ms | Tested on 4 machines within LAN |

***Table 6.2:*** *Migration time in average network traffic environment*

| Test No. | Virtual Machine | VM Size | Migration Time | Descriptions |
|---|---|---|---|---|
| **1.** | RHEL | 2.99GB | 34 sec & 217 ms | Between 15 machines within 4 labs and 2 switches |
| | CENTOS | 3.99GB | 125 sec & 127 ms | |

***Table 6.3:*** *Migration time in heavy network traffic environment*

| Test No. | Virtual Machine | VM Size | Migration Time | Descriptions |
|---|---|---|---|---|
| **1.** | RHEL | 2.99GB | 50 sec & 418 ms | Between 24 machines within 4 labs and 2 switches (heavy traffic generated) |
| | CENTOS | 3.99GB | 169 sec & 549 ms | |

The VM migration time in low, average and heavy traffic environments is shown in figure 6.1.

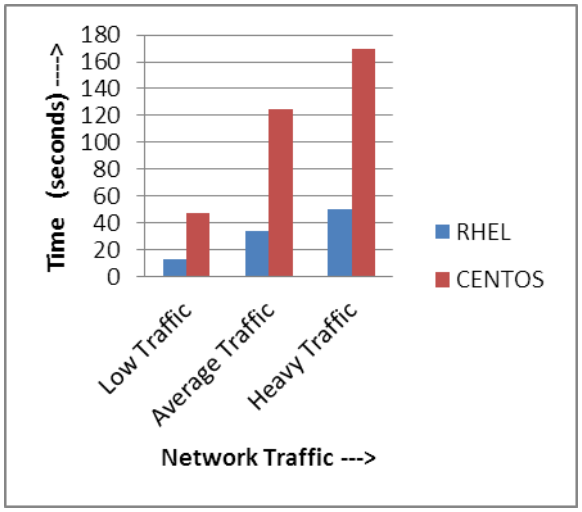



***Figure 6.1:*** *VM migration Time*

The migration time and encryption time for securing VM using RSA with SSL protocol is shown figure 6.2.

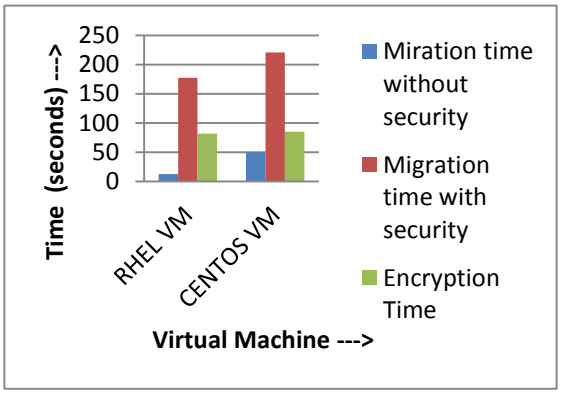



***Figure 6.2:*** *VM Migration and Encryption time*

The results obtained can be summarized as under:

i) The live migration was done satisfactorily by using Xen virtualization package and python script.
ii) Categorization of heavily loaded host was done based on load balancing parameters like memory usage, disk usage, CPU usage, network bandwidth and total number of processes.
iii) Migration was performed with a reasonable downtime based on time and network bandwidth.
iv) Secure live migration of VM required more migration time by using RSA with SSL.
v) Active data (512 MB) of VM was considered for secured live migration.

## 7. Conclusion

We presented methodology of secure live migration of VM in cloud environments by incorporating encryption and authentication mechanisms. This methodology achieves live migration of VM by considering load balancing parameters and using CENTOS with Xen virtualization software. The experiment was carried on the intra network of 25 systems which contained four node servers connected through Ethernet switch (100 Mb/s). Our results indicate that the migration time is based on size of VM and network bandwidth. Secured live migration of VM can be achieved by

compensating on the additional migration time of VM. The process migration was done by using MOSIX package with homogeneous environments.

## Further Work

A heterogeneous live migration of VM framework can be implemented in different hypervisors that enables the live VM migrations among different kinds of VMMs. We plan to extend it to support live migration in wide-area network. Similarly, heterogeneous process migration framework can be considered for process migration. These processes can be business application, web application, software processes etc. The public key cryptography mechanism can be used for implementation of secure process migration in heterogeneous system.

## References

[1] Greg Boss et al., *Cloud Computing*. Cloud Computing High Performance on Demand Solutions Workshop, IBM Corporation. 2007. Version 1.0; 1-17.

[2] Yi Zhao et al., 2009: Adaptive Distributed Load Balancing Algorithm Based On Live Migration Of Virtual Machines in Cloud. Fifth International Joint Conference on INC, IMS and IDC, 170-175.

[3] C. Clark et al., 2005: Live Migration of Virtual Machines. Proceeding of the Second Conference on Symposium on Network System Design and Implementation, Vol. 2.

[4] Jon Oberheide et al., 2008: Empirical Exploitation of Live Virtual Machine Migration. Proceeding of Blackhat DC Convention.

[5] Wei Wang et al., 2010: Secured and Reliable VM Migration of Personal Cloud. Computer Engineering and Technology (ICCET), 2nd International Conference, Vol.7. V1-705.

[6] M. Cermele et al., 1997: Dynamic Load Balancing of Distributed SPMD Computations with Explicit Message Passing. Proceedings Sixth Heterogeneous Computing Workshop, 2.

[7] Centos - The Community ENTerprise Operating System, CentOS-5.5-i386-LiveCD-Release2.iso [http://ftp.iitm.ac.in/centos/5.5/isos/i386/]

[8] Roberto Innocente, 2000: Automatic Load Balancing and Transparent Process Migration. [http://people.sissa.it/~inno/pubs/mosix.pdf]

[9] Anthony T. Velte et al., 2009: Cloud Computing a Practical Approach. 1st Ed. McGraw-Hill Osborne Media, 352.

[10] George Reese, 2009: Cloud Application Architectures, O'Reilly Media, 208.

[11] Najib Kofahi et al. *MOSIX Evolution on A Cluster Linux*. The International Arab Journal of Information Technology. 2006. 3 (1) 62- 68.

[12] L. Amar et al., 2010: *MOSIX Tutorial*. Department of Computer Science, the Hebrew University. [http://www.MOSIX.org]

[13] E. Rescorla, 2000: *SSL and TLS: Designing and Building Secure Systems*. 1st Ed. Addison-Wesley Professional, 528.

[14] Cisco System. Introduction to Secure Sockets Layer. [White Paper] Retrieved from [http://jmiller.uaa.alaska.edu/cse465-fall2012/papers/cisco2002.pdf]

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2012, Volume 1, Issue 1, pp. 20-28, Article ID Tech-37
ISSN 2320 - 0235

Case Study | Open Access

# Use of Internet Resources in University BDT College of Engineering Davanagere: A Study

**M.S. Lohar[1], Nasreen Banu[2]**

[1] Post Graduate Center, Kuvempu University, Kadur, Karnataka, India
[2] Research Scholar, JJT University Rajasthan, India

Correspondence should be addressed to Dr. M.S. Lohar, manjunathlohar@yahoo.com

Publication Date: 24 December 2012

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-37



## Abstract

The use of digital information resources on internet has revolutionized the academic community and it is a giving way for higher education. The investigator has made an attempt to know the use of internet resources by post graduate students of University B D T College of Engineering Davanagere University, Karnataka. Hence, the purpose of the study was done by using a set of questionnaires. The paper highlights various problems and issues involved in using internet resources and also giving suitable suggestions to improve the library services of the present day library facilities across India and also to meet the demands of the users.
**Keywords** *Digital resources, Internet resources, e-resources*

## 1. Introduction

Libraries are playing an important role in the propagation of information for learning activities where the users can discover/utilize the vast amount of information resources. In this context, the learning population requires information for day to day activities. The library and information centers (LICs) are playing an important role in extending the required latest/necessary information services quickly and efficiently to their users. Presently many libraries in India have access to the electronic information resources in multiple ways. Hence, the growth of electronic information resources increased and selection of information sources has become complex. Internet has made tremendous impact on the academic activities of the faculty members, researchers, and the students. After the advent of Internet, a significant transition is seen in users' approach and the way they seek information and the methods they use in research and learning activities. So, the internet provides a wealth of new study materials and acts as a powerful supplement to the traditional teaching and learning activities and also facilitating an excellent academic environment where the academic community can perform their activities in a rejuvenated manner.

## 2. Literature Review

Literature review reveals that studies on use of e-resources have been carried out by students, research scholars, and faculties of various institutions all over the world. Swain and Panda in their study, 'Use of e-services by faculty members of business schools in a state of India: A study', have discussed on quantitative and qualitative use of e-resources (1). Maunissamy and Swaroop Rani in their study, 'Evaluation of usage and usability of electronic journals', have identified the usage and usability of e-journals by the users of the NIT, Tiruchirapalli (2). According to Internet Governance Forum, India had 81 million internet users in the year 2008 and ranks fourth in the world in terms of internet users. The US with 220 million internet users, tops the world; China, with 210 million users, comes in a close second followed by Japan with 94 million users (3). The time spent on the Internet by the school children has increased as they spend average of 322 min, college students spend an average of 433 min, older men spend an average of 580 min, and working-women spend an average of 535 min, respectively. However, non-working women spend only 334 min per week (4).

## 3. Brief Introduction of University B D T College of Engineering (UBDT) Davanagere

University B D T College of Engineering (UBDT), Davangere, Karnataka, was established in the year 1951. In 1st June 1992, the college was transferred to Kuvempu University, B R Project (Shivvamogga). Hence, it became a constituent engineering College of Kuvempu University on 18-08-2009. Recently with an intention of overall development of the college, Government of Karnataka transferred the college to the Visvesvaraya Technological University (VTU), Belgaum on 24-02-2011 as a constituent engineering college. The institution has highly qualified and dedicated faculty members to impart advanced knowledge in Engineering and Technology to students and at present 380 PG students are studying in various disciplines.

***Table 1:*** *Programmes Offered by the College*

| Graduate Courses in Engineering | Post Graduate Courses in Engineering |
|---|---|
| **1**. Computer Science and Engineering | **1**. Computer Aided Design of Structures and Sub Structures |
| **2**. Electronics and Communications Engineering | **2**. Computer Science and Engineering |
| **3**. Electrical and Electronics Engineering | **3**. Digital Communication and Networking |
| **4**. Electronics and Instrumentation Engineering | **4**. Environmental Engineering |
| **5**. Mechanical Engineering | **5**. Machine Design |
| **6**. Industrial Production Engineering | **6**. Power System and Power Electronics |
| **7**. Civil Engineering | **7**. Production Engineering Systems and Technology |
| **Post Graduate Courses** | **8**. Thermal Engineering Systems |
| **1). M C A 2). M B A** | |

### 3.1. Digital Library

The library acts as a nerve centre, catering to the needs of the students, researchers and the faculty members of all under graduate departments and post graduate department, covering science, engineering & technology, computer science, engaged in higher pursuit of knowledge. The library has been turned as centre of excellence, for academic and research pursuits, by keeping it open to the changes brought in by Information Technology. In the year 2011 the college was availing digital library internet connectivity under the project of TEQIP. The MHRD, India provides online video lectures of national programme on technology enhanced learning and center for distance engineering education programme (NPTEL/CDEEP) to digital library for the benefit of the students, research scholars and teaching faculty. At present around 20 computers are connected to access the internet service to all the users of the digital library to search only specific websites with the help of library staff.

***Table 2:*** *Library Details*

| | |
|---|---|
| **Working Hours on Week Days** | Main Library: 10.00 AM to 5.30 PM. Reference : 08.00 AM to 8.00 PM |
| **Area of the Library** | Carpet area of Stack section – 6578 Sq. Reference section– 6578 Sq ft |
| **Total No of Books (Volumes)** | **Facilities Available in the Library** |
| Text book 60629 | Borrowing books & other reading materials |
| Reference **7500** | Book bank facility for SC&ST |
| Book bank **(SC&ST) 8422** | Educational multimedia packages 300+ CD's online lecturers videos of **NPTEL/CDEEP** |
| Total titles **28005** | Reprographic Services |
| Type Access: **Open access** | LAN |
| Seating Capacity in library **: 100** | Internet connectivity - **20 systems** 256 kpbs |
| Classification / Scheme adopted: **DDC 22nd edition** | |
| Software used : **SOUL** | |

## 4. Objectives of the Study

The objectives of the present survey are to study the use of Internet resources by the post graduate students who are studying in UBDT Engineering College Davangere. The specific objectives of the study are:

1. To study the purpose for which Internet is being used by the students
2. To identify the commonly used search engines by the students
3. To identify the extent of awareness of the important sites in their subject fields
4. To understand the difficulties faced while using the Internet
5. To know the users opinion to words making /developing model digital library in future
6. To make suggestions for improving the services in the study area/l library.

## 5. Methodology

Questionnaire method was used for the evaluation study to cover the maximum respondents to collect the information and to determine their responses towards internet. Keeping in view the objectives of the study, a structured questionnaire was designed and distributed to 100 PG students. Off the total, (out of 100) 75 questionnaires were received. The collected data was further supplemented through informal discussions with the respondents. The analysis and interpretation of the data is presented in the following tables.

## 6. Data Analysis

### 6.1. Frequency of Visits to the Library

The frequency of visit to library depends upon the nature of library collection organization information resources etc. The responses received in the quarry are analyzed in the following table 3 and figure 1. Majority (41.44%) respondents visit "daily" followed by 33.35% of users are visit "once in week" to their library. 39.03% of both users visited daily followed by 32.35% of users visit "once in a week. Significant numbers of (6.57) users are visited "once in a month".

***Table 3:*** *Frequency of Visit*

| S. No. | Frequency | No. of Responses | Percentage |
|---|---|---|---|
| 1 | Daily | 63 | 41.44% |
| 2 | Once in a week | 51 | 33.55% |
| 3 | Twice a week | 28 | 18.42% |
| 4 | One in a month | 10 | 6.57% |
| 5 | Rarely | 00 | 00.00% |
| | Total | 152 | 100.00% |

Multiple-choice question

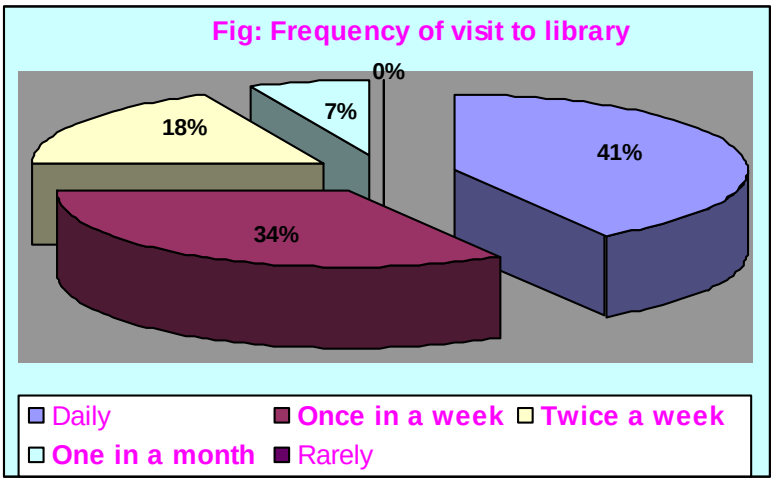



***Figure 1:*** *Frequency of Visit to Library*

### 6.2. Purpose of Visit to the Library

Table 4 shows the purpose of visit to library by the users. Of the total 22.17% of users are visit to "to collect relevant literature on their subject" and 20.16% of user visit "to prepare project proposals, and good number of students {37} visit to see technical sights for their study/learning purpose it represents 16.95% of the total responses.

***Table 4****: Purpose of Visit to Library*

| S. No. | Purpose | No. of Responses | Percentage |
|---|---|---|---|
| 1 | To collect relevant literature in my subject | 55 | 22.17% |
| 2 | For communication | 33 | 13.30% |
| 3 | To prepare project proposals | 50 | 20.16% |
| 4 | To see technical sights | 42 | 16.95% |
| 5 | Update the subject/general knowledge | 37 | 14.93% |
| 6 | For carrier development | 31 | 12.05% |
| | Total | 248 | 100.00% |

. Multiple-choice question

### 6.3. Method of Learning to Use Internet

Of the total 27.91% of users indicate to learn "self instruction through trial and error". This shows majority of post graduate students are capable of learning on their own. But the trend is not being very encouraging as it may leads to lots of their time wastage and without any in-depth knowledge of

searching skills. 19.79% of users learned through “Internet orientation programmes conducted at the beginning of academic year by the library staff”. The good numbers of users {32} are taking help from “their friends” in using internet for their study/academic work it represents 16.24% of the total responses.

***Table 5:*** *Method of Learning to Use Internet*

| S. No. | Purpose | No. of Responses | No. of Responses |
|---|---|---|---|
| 1 | Self instruction through trial and error | 55 | **(27.91%)** |
| 2 | Internet orientation programmes by the library staff | 39 | **(19.79%)** |
| 3 | Guidance from departmental staff of computer science | 27 | **(13.70%)** |
| 4 | Guidance from friends | 32 | **(16.24%)** |
| | | | |
| 5 | External courses | 21 | **(10.65%)** |
| | Courses offered by the Institutions | 23 | **(11.67%)** |
| | Total | 197 | **(100.00%)** |

Multiple-choice question

### 6.4. Type of Internet Resources Used

Majority of respondents using (39; 21.66%) internet for “the purpose of project reports” which is helpful to prepare their project reports in future and 20.55% of students who use “Technical reports” “e-books” are using 16.11% and each 13.33% of users are used e-books and Internet based databases for their study. Significant number of users is use “full text of articles”.

***Table 6:*** *Type of Internet Resources Used*

| S. No. | Internet Resources | No. of Responses | Percentage |
|---|---|---|---|
| 1 | e-books | 29 | 16.11% |
| 2 | e-journals | 24 | 13.33% |
| 3 | Technical reports | 37 | 20.55% |
| 4 | Internet-based databases | 24 | 13.33% |
| 5 | Theses and dissertations | 19 | 10.55% |
| 6 | Project reports | 39 | 21.66% |
| 7 | Full text of articles | 8 | 4.44% |
| | Total | 180 | 100.00% |

Multiple-choice question

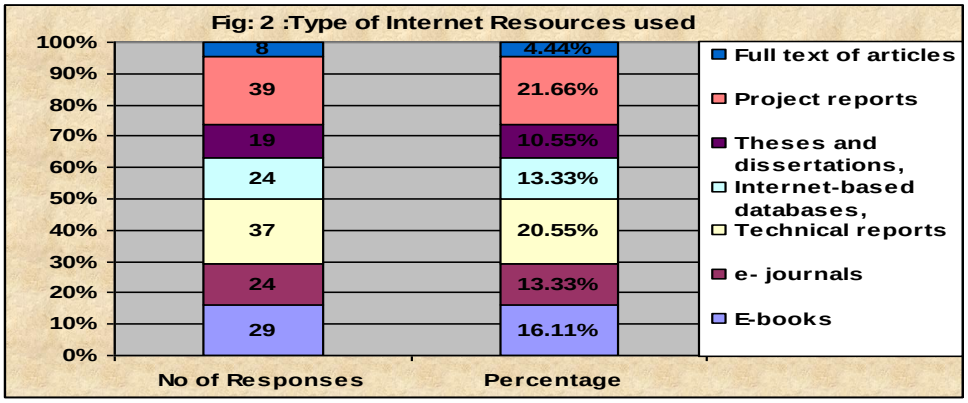



***Figure 2:*** *Type of Internet Resources Used*

### 6.5. Problems in Using Internet Services

The users were asked to indicate the specific problems faced by them while using Internet. Majority (25.00%) of users' opined "overload of information on the internet" is main problem while using internet followed by 24.58% opined "slow access" may be the telephone lines were busy. For enhance the speed of the Internet the authority should go for broadband whose speed is much faster or alternatively for dedicated lines. Most of these problems were due to lack of knowledge and experience in conducting the information searches. Once, the concerned authority should appoints a trained and experienced system administrator, all these problems will be minimized and users could be satisfied.

***Table 7:*** *Problems in Using Internet Services*

| S. No. | Reasons | No. of Responses | Percentage |
|---|---|---|---|
| 1 | Slow access | 59 | 24.58% |
| 2 | Slow download | 47 | 19.58% |
| 3 | Overload of information on the Internet | 60 | 25.00% |
| 4 | Privacy & difficulty in finding relevant information | 41 | 17.08% |
| 5 | lack of knowledge and experience in using Internet | 10 | 4.16% |
| 6 | Lack of time | 14 | 5.83% |
| 7 | Lack of operating systems | 09 | 2.75% |
| | Total | 240 | 100.00% |

Multiple-choice question

### 6.6. Preference of Using Search Engines

Access and finding of relevant Information or required e-books, e-journals from databases is a difficult task. It requires skill and experience on the part of users. Hence the study tried to collect data on the search strategy of the users. The following table 8 shows the users preference of using search engines. 28.13% preferred "Google" followed by 22.07% preferred to use "Yahoo" and 18.61% students preferred to use Mozilla Firefox search engines.

***Table 8:*** *Preference of Using Search Engines*

| S. No. | Search Engines Preferred | No. of Responses | Percentage |
|---|---|---|---|
| 1 | Google | 65 | 28.13% |
| 2 | Yahoo | 51 | 22.07% |
| 3 | Mozilla Firefox | 43 | 18.61% |
| 4 | M S N | 31 | 13.41% |
| 5 | Excite | 19 | 8.22% |
| 6 | Ask Jeeves | 10 | 4.32% |
| 7 | Alta Vista | 12 | 5.19% |
| | Total | 231 | 100.00% |

Multiple-choice question

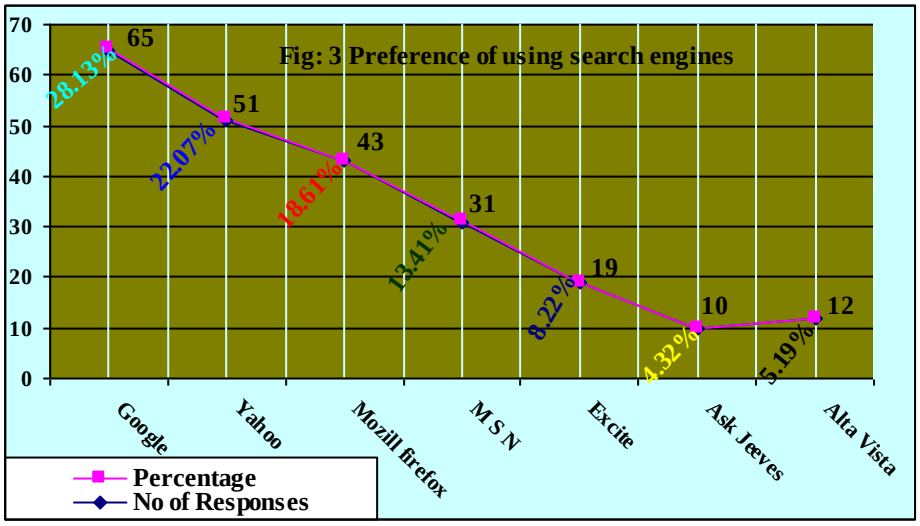



***Figure 3:*** *Preferences of Using Search Engines*

### 6.7. Usefulness of Internet Resources on Print Resources

Table 9 shows the users opinion on the usefulness of internet resources. Majority (71.33%) of respondents were of the opinion that internet resources are more useful than print resources to a "Great extent" followed by 28.66% to a "Small extent" and surprisingly none on "not at all".

***Table 9:*** *Usefulness of Internet Resources on Print Resources*

| S. No. | Extent of Usefulness | No. of Responses | Percentage |
|---|---|---|---|
| 1 | Great extent | 49 | 65.33% |
| 2 | Small extent | 26 | 34.66% |
| 3 | Not at all | 00 | 00.00% |
| | Total | 75 | 100.00% |

### 6.8. Users Opinion towards Making a Model Digital Library in Future

The users were requested to indicate their opinion towards making of model digital library in future. The responses received regarding this analyzed in the following table 10. Average 20.00% of each respondent opined "20.34% create machine readable details of their Library records" and "20.67% library should automate its entire housekeeping services" then only it is possible to develop a model

digital library in future. Majority {55} of students indicates "library should develop/create required infrastructure for networking", it represents 18.97% of the total responses.

***Table 10:*** *Model Digital Library in Future: Users Opinion*

| S. No. | Reasons | No. of Responses | Percentage |
|---|---|---|---|
| 1 | Create machine readable details of their Library records | 59 | 20.34% |
| 2 | Library should develop/create required infrastructure for networking | 55 | 18.97% |
| 3 | To provide training for the users in the use of network based services | 41 | 14.13% |
| 4 | Library should automate all its housekeeping services | 60 | 20.67% |
| 5 | Provide to access scholarly journals in digital form | 32 | 11.03% |
| 6 | Sharing the information resources in regional and national cooperative efforts | 15 | 5.17% |
| 7 | Visvesvaraya Technological University (VTU) net-work or consortium of technical libraries if established in our college campus will be useful | 28 | 9.65% |
| | Total | 290 | 100.00% |

Multiple-choice question

## 7. Findings of the Study

1. Majority (41.44%) of post graduate students visit "daily" followed by 32.35% of users visit "once in a week".
2. Of the total 22.17% of users are visit to "collect relevant literature in their subject" and 20.16% visit to "prepare project proposals".
3. Majority (27.91%) of users indicate to learn "self instruction through trial and error" method.
4. 19.79% of users learned through "Internet orientation programmes conducted at the beginning of academic year by the library staff". But it may lead to lots of their time wastage and without any in-depth knowledge of searching skills.
5. Majority (39; 21.66%) of respondents use internet for "preparing their project reports" which is submitted at the end of their academic year and 20.55% of students who use "technical reports".
6. 25.00% of users opined "overload of information on the Internet" and 24.58% opined "slow access" is the main problem while using internet.
7. Access of relevant information or required e-books, e-journals from databases is a difficult task. It requires skill and experience on the part of users. Off the total users 28.13% preferred "Google" and 22.07% preferred to use "Yahoo" as search engines.
8. Majority (71.33%) of respondents were of the opinion that Internet resources are more useful than print resources to a "Great extent" and 28.66% to a "Small extent".
9. Average 20.00% of each respondent opined "(20.34%) create machine readable details of their Library records" and "(20.67%) library should automate its entire housekeeping services".

## 8. Suggestions

Based on the findings of the study, the following suggestions are made to improve the Internet resources and services:

2. More number of computer terminals should be provided in the digital library and speed of Internet needs to be increased for quick access to the available e-resources.
3. More computers with latest specifications and multimedia kit should be installed so that users can use Internet telephony, video-conferencing, chatting and other useful services of the Internet.
4. Some computers with floppy disk/CD-ROM drives/ USB ports may be provided in the library so that the users can download relevant information from the Internet and take to their home/hostels etc. to read it leisurely. That helps not only to them but also to others in getting more time in searching information on the Internet.
5. A networked printer may be provided in the centre so that the users can take print-outs. This facility may be provided for all the users on payment basis.
6. Digital library should keep open 8 am - 8 pm on all working days so that the systems can be optimally used by the users.
7. There is a need for extensive training programme on regular basis at the beginning of each semester. This is required for all the categories of library users so that they can use Internet-based resources optimally for their studies and research.
8. A system administrator may be appointed for providing right kind of help during their day-to-day Internet use and also useful for conducting regular training programmes.

## 9. Conclusion

It is evident from the results that Internet has a great impact on the academic community. The users are making maximum use of Internet facility provided by the college. However, library should provide short term training programmes to users so that they can take advantage of freely available subject gateways on the Internet. For this purpose, the academic staff should be encouraged to use electronic information sources for their study purposes. The library environment has currently undergone drastic change in terms of collections and services. The proliferation of e-resources especially internet has had a significant impact on the way the academic community uses, stores, and preserve the information. The advantages of internet have drawn attention of the library users to a great extent. Accordingly, these resources have occupied a significant place in the digital library.

## Reference

[1] D.K. Swain, et al. *Use of e-Services by Faculty Members of Business Schools in a State of India: A Study.* 2009. Collection Building. 28 (3) 108-116.

[2] P. Mounissamy et al., *Evalution of Usage and Usability of Electronic Journals*. SRELS Journal of Information Management. 2005. 42 (2) 189-205.

[3] JuxtConsult, 2008. [http://www.getcounted.net]

[4] Leo Appleton. *Perceptions of Electronic Library Resources in Further Education*. 2006. Electronic Library, The. 24 (5) 619 – 634.

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2013, Volume 2, Issue 1, pp. 29-33, Article ID Tech-68
ISSN 2320 – 0235

Review Article | Open Access

# Password Authentication System (PAS) for Cloud Environment

**Bhavana A., Alekhya V., Deepak K., and Sreenivas V.**

Department of C.S.E., K L University, Vaddeswaram, Guntur, Andhra Pradesh, India

Correspondence should be addressed to Bhavana A., bhavana@kluniversity.in

Publication Date: 5 April 2013

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-68



**Abstract** Verification is the major part of protection against compromising secrecy and authenticity. Though long-established login/password based schemes are easy to implement in the cloud environment, they have been subjected to numerous attacks. As a substitute, token and biometric based verification systems were introduced for security. However, they have not enhanced significantly to justify the expenditure. For providing more security-in this paper, we introduce a new framework i.e., Password Authentication System for Cloud Environment (PASCE), which is immune to the common attacks suffered by other verification schemes.
**Keywords** *Password Authentication System, Cloud Computing, Smartcards*

## 1. Introduction

Because of emergent threats to networked computer systems, there is great need for security innovations. Security practitioners and researchers have made strides in defending systems and, correspondingly, individual users' digital possessions. However, the difficulty arises that, until recently, security was treated completely as a technical problem- the system user was not factored into the equation. Users interact with protection technologies either passively or actively. For passive use understandability may be enough for users. For active use people need much more from their security solutions: ease of use, exorability, competence and satisfaction [5]. Today there is an increasing detection that security issues are also basically human computer interaction issues. Validation is the process of determining whether a user should be allowed access to a particular system or resource. It is a critical area of security research and practice. Alphanumeric passwords [4] are used widely for verification, but other methods are also available today, as well as biometrics and smart cards. However, there are problems of these substitute technologies. Biometrics raise confidentiality concerns and smart cards usually need a PIN because cards can be lost [6]. As a result, passwords are still leading and are expected to continue to remain so for some time. Yet conventional alphanumeric passwords have drawbacks from a usability standpoint, and these usability problems tend to transform directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can utilize.

## 2. Cloud Computing

Cloud computing gets its name as a symbol for the Internet. Typically, the Internet is represented in network diagrams as a cloud. Cloud computing promises to cut operational and capital costs and, more importantly, Cloud technology provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services [11]. Cloud computing [11] is distributed processing, parallel processing and the development of grid computing, or commercial implementations of these concepts of computer science. In the cloud computing model is the essential structure of which, the foundation part is collected of more than one computer server "cloud." It gathers all the resources together to form large data storage and processing center. Let IT departments focus on intentional projects instead of keeping the datacenter running. Cloud computing provides the most consistent and secure data storage center. Users do not have to worry about data loss, virus attack and other problems. The "cloud" manages information by a professional team. Besides, strict rights management strategy can help to share data.

## 3. Introduction for Authentication

There are numerous validation schemes existing in the literature. They can be broadly classified as follows:

- What you know
- What you have and
- What you are

The conventional username/password or PIN based certification scheme is an example of the "what you know type". Smartcards or electronic tokens are examples of "what you have type of authentication" and finally biometric based certification schemes are examples of the "what you are" type of validation. Some validation systems may use an arrangement of the above schemes. In This paper, we focus only on "what you know" types of validation. Although traditional alphanumeric passwords are used widely, they have problems such as being hard to memorize, vulnerable to guessing, dictionary attack, key-logger, Shoulder-surfing and social engineering. In addition to these types of attacks, a user may tend to choose a weak password or record his password. This may further decline the validation schemes. As an alternative to the conventional password based scheme, the biometric system was introduced. This relies upon exclusive features unchanged during the life time of a human, such as finger prints, iris etc. The major problem of biometric as a validation scheme is the high cost of additional devices needed for recognition process. The false-positive and false negative rate may also be high if the devices are not robust. Biometric systems are bare to replay attack (by the use of close excess left by finger on the devices) [3], which decrease the security and usability levels. Thus, modern developments have attempted to defeat biometric shortcomings by introducing token-based authentication schemes. Token based systems rely on the use of a physical device such as smartcards or electronic-key for validation purpose. This may also be used in conjunction with the conventional password based system. Token based systems are vulnerable to man-in-the middle attacks where an intruder intercepts the user's session and records the credentials by acting as a proxy between the user and the authentication device without the knowledge of the user. Thus as an unusual, graphical based passwords are introduced to resolve security and usability restrictions mentioned in the above schemes. Graphical-based password techniques have been proposed as a potential alternative to text-based techniques, supported partially by the fact that humans can remember images better than text. Psychologists have confirmed that in both detection and recall scenarios, images are more memorable than text. Therefore, graphical-based proof schemes have higher usability than other validation techniques. On the other hand, it is also complex to break graphical passwords using normal attacks such as dictionary attack, brute force and spyware

which have been affecting text-based and token-based authentication. Thus, the security level of graphical based validation schemes is higher than other authentication techniques.

In broad-spectrum, the graphical password techniques can be classified into two categories:

1. Recognition-based graphical technique.
2. Recall based graphical technique.

### A. Recognition-Based Systems

In recognition-based systems, a cluster of images are display to the user and a usual validation requires a correct image being touched in an exacting order. Some examples of recognition-based system are IAS system [2], reliable Graph, and Pass faces system [4]. An image password called IAS [2] is a new system which enables users to use their preferred image instead of a text password for validation purpose. Even though PAS system has a superior usability, it is difficult to execute due to the storage space needed for images and also the system cannot stand replay attack.

***Image Authentication System (IAS): Image-based Authentication with Image Registration and Notification Interfaces***

IAS is a validation system using photographs as a substitute of passwords. It, Moreover, integrates image check and notification interfaces into current validation frameworks (Figure 1). The image muster line enables users to add their preferred images to the validation system. As a result, this makes it possible for users to use their preferred image as a “pass-image”. Almost 20 million users currently have mobile phones with digital cameras in Japan. Most of them send photos by E-mail with a few key clicks on the spot. The image muster interface is implemented using this function. It is implemented independently from a pass-image [2] setting in order to ensure the privacy against copying attempts. This task simply enables users to add a photo to the system and a registered photo does not automatically become a pass-image. In other words, not all registered images become a passim age. A user must set at least one pass-image before authenticating oneself using IAS.

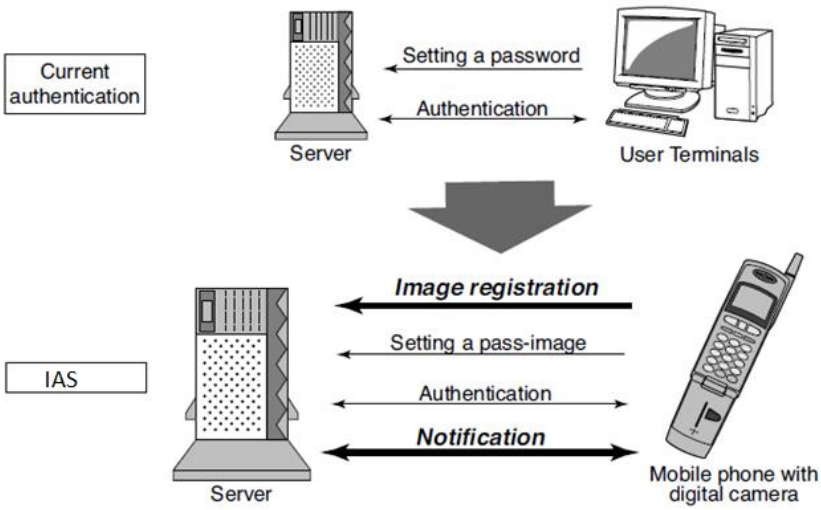



***Figure 1:*** *Transition between Current and Proposed Authentication Framework [2] Takada.T and H. Koike*
*Source: This image has taken from the paper entitled Awase-E: Image-based authentication for mobile phones using user's favorite images authored by Takada.T and H. Koike*

The warning interface gives users activate to handle a risk sensibly. It notifies users of the incidence of all kinds of events related to the validation process. For example, IAS sends an E-mail to the user who has registered a photo. The E-mail has a URL. The web page that is linked by that URL contains the photo that a user has just registered. A user can thus confirm the registered photo immediately through a web page. If a user receives such an E-mail even though the user had not registered the photo, it means that someone has registered it unknown as a legitimate user. A reasonable user, therefore, quickly knows when an invasive attempt has been made. From these scenarios, we would stoutly recommend using IAS with mobile phones to ensure a user's rapid awareness of a security breach. IAS keeps an event history of past usage for certain periods for the purpose of auditing the user's validation usage. A user can investigate the history through a web page. It enables users to check the authentication usage even if a user has lost their mobile phone.

IAS is implemented through both E-mail and Web. Prerequisite supplies for a user terminal are that it has access to the above two network service types. This means that it is also possible to use IAS from computers. The detail of the validation process is shown in Figure 2.

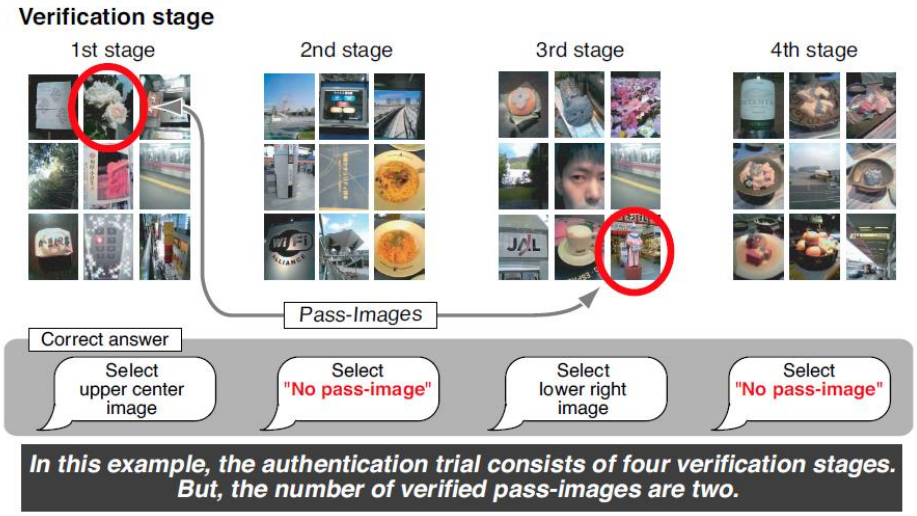



***Figure 2:*** *A Detailed Authentication Process in PAS (N=4, P=9) [2] Takada.Tand H. Koike*
*Source: This image has taken from the paper entitled Awase-E: Image-based authentication for mobile phones using user's favorite images authored by Takada.T and H. Koike*

One verification test consists of R times of qualifications stages. IAS, of course, authorizes a user as genuine user only if all verifications are successful. In each verification stage, IAS shows X pieces of images on the screen, a user must select a pass-image correctly from them. Only one pass image is built-in in each verification image set. The motive for this is to decrease the possibility that an accidentally selected attacker's answer would be a correct answer. We call an image that is not a pass-image as a "decoy image". The position of each image in the image set is randomly determined. This means that the location of both pass-image and decoy images can change each time. It is also possible that there is no pass image in an image set. In this case, the user must answer "no pass-image". IAS is an easier method for users to complete the validation process than before, even when using a mobile phone. The arithmetical keys on a mobile phone are uniquely corresponding to each of the images on the screen at any given stage. This enables users to decide any image in the screen with one click. In using IAS, it is possible to substantiate oneself by just N + 2 times of key types.

Additionally, IAS does not need to input any text in validate oneself because it uses an E-mail address as a user ID.

### B. Recall-Based Systems

In recall-based systems, the user is asked to replicate something that he/she created or selected former during the registration phase.

***Password Authentication System for Cloud Environment (PASCE)***

Graphical authentication system with image reshuffle format is given for the cloud environment when the data upload/download into the cloud account.

## 4. Conclusion

In this paper, we have proposed a new Password Authentication System for Cloud Environment where the verification information is absolutely accessible to the user. If the user "clicks" the image for verification and it compared with the server, the user is implicitly genuine. No password information is exchanged between the client and the server by using PAS authentication system. Since the authentication information is conveyed absolutely. Strength of PASCE lies in creating a good verification space with adequately huge set of images to shun short repeating cycles.

## References

[1] Susan Wiedenbeck et al., 2005: *Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice*. Symposium on Usable Privacy and Security (SOUPS) Pittsburgh, PA, USA.

[2] Takada T., et al. *Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images*. Human-Computer Interaction with Mobile Devices and Services, Springer Berlin/ Heidelberg. 2003. 2795; 347-351.

[3] Dhamija R., et al., 2000: *A User Study Using Images for Authentication*. 9th Usenix Security Symposium, Denver, Colorado, 45-58.

[4] Suo X., et al., 2005: *Graphical Passwords: A Survey*. Computer Security Applications Conference, 21st Annual, Tucson, AZ, 472.

[5] Wu C.W. *On the Design of Content-Based Multimedia Authentication Systems*. IEEE Trans. Multimedia.2002. 4 (3) 385-393.

[6] R. Morris et al. *Password Security: A Case History*. Commun. ACM. 1979. 22; 594-597.

[7] Birget J.C., 2003: *Robust Discretization: With an Application to Graphical Passwords*. Cryptology ePrint Archive, Report 2003/168.

[8] Renaud K. *On User Involvement In Production of Images Used in Visual Authentication*. J. Vis. Lang. Comput. 2009. 20 (1) 1-15.

[9] Wiedenbeck S., et al., 2005: *Authentication Using Graphical Passwords: Effects of Tolerance And Image Choice.* Symposioum. Usable Privacy and Security, Carnegie-Mellon Univ., Pittsburgh, PA.

[10] Blonder G., 1996: *Graphical Password*. U.S. Patent 5 559 961.

[11] Sreenivas V., et al. *Efficient Use of Cloud Computing in Medical Science*. American Journal of Computational Mathematics. 2012. 2; 240-243.

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2013, Volume 2, Issue 1, pp. 34-41, Article ID Tech-69
ISSN 2320 – 0235

Cloud Publications

Review Article | Open Access

# New Generation Networks Architecture between H.323 and SIP Protocol

**Anshuman Srivastava[1] and Kumud Sharma[2]**

[1]Department of Computer Science and Engineering, SRM University (NCR Campus) Chennai, Tamil Nadu, India
[2]Department of Information Technology, Banasthali University, Jaipur, Rajasthan, India

Correspondence should be addressed to Anshuman Srivastava, anshuman.mtech@ymail.com, kumudsharmakec@gmail.com

Publication Date: 30 April 2013

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-69




**Abstract** Today in this new era everyone wants to achieve the goal or target in minimum time as per his schedule, for business purpose, corporate sector, or make a better relationship via meetings either in his personal life. It's a major challenge for new generation is to provide multimedia teleconferencing services. For this challenge there are special standards have recently populated for signaling and control for Internet teleconferencing. Here discussed on two standards: One is ITU Recommendation H.323, and the other is the IETF Session Initiation Protocol (SIP). Both signaling protocols are responsible for call setup and call tear down. Several comparisons of these two protocols have been published already, but their service architectures have been rarely addressed. This paper provides a unique architecture based on mechanism, with comparison of H.323 and SIP both protocol, and focusing on their service architectures. While architecture of both standards are quite similar. Here in this paper focused on considerable differences regarding their transferable and supplementary service. H.323 is still the more standard, smooth interworking with the PSTN and interoperability between different implementations. It has specific advantages for IP telephony applications. SIP has been designed with a broad scope, providing more generic syntax and semantics regarding feature definition and session description. A coexistence of both protocols can be foreseen, stressing the importance of interworking between them. This paper describes to all differences, properties and provides a unique architecture.

**Keywords** *SIP, H.323, Multipoint Control Unit, CMA Gatekeeper, and Testing of Services*

## 1. Introduction

H.323 and SIP standard provides a foundation for audio, video, and data communications across IP-based networks, including the Internet. Both are apply specially for video conferencing services at broad level in today network. Since for provide useful services in Internet telephony, requires a set of control protocols for connection establishment, capabilities exchange, and conference control for voice and video. Currently, these two protocols exist to meet this need. One is ITU-T H.323, and the

other is the IETF Session Initiation Protocol (SIP). The H.323. By abidance to H.323, multimedia products and applications from multiple sources can interoperate, allowing users to communicate without concern for compatibility. H.323 will be the keystone for LAN-based products for consumer, business, entertainment, and professional applications. In this paper, H.323 and SIP are compared according to the following criteria: standardization status, supported services, supplementary service architecture, and mechanisms, interoperability of services and features, and service creation issues. Basic call features like call setup and session modification are distinguished from supplementary services. First we discuss about both protocols briefly then compared on all activities.

### 1.1. H.323 Standard

The ITU-T H.323 standard fulfill to all the communicational needs for multimedia system by using packet based network [11]. The network can may be included any types like as Local Area Networks, Enterprise Area Networks, Metropolitan Area Networks, Intra-Networks, and Inter-Networks (including the Internet). There are some related coefficient of H.323 discussed here those mainly associated points. H.323 Terminals: multi endpoint connection those able for real time voice or video communications with other H.323 terminals, gateways or MCUs on the network.

MCU/MC/MPs: for this standard need a central hob which able for manage multi connection, i.e. called Multipoint Controller Units (MCU), which include a Multipoint Controller (MC) and one or several Multipoint Processors (MPs), these all devices worked centrally and control to multi connection and process.

Gateways: Gateway use for provide interconnection between IP networks and Switched Circuit Networks (SCNs), such as ISDN and PSTN. It's used when the two endpoints not connected with same MCU.

Gatekeepers: Gatekeepers play very important role for VoIP services to the endpoints. Mandatory functionality includes address resolution (aliases to IP address mapping), authentication and service authorization. In addition, gatekeepers may offer an array of services such as CDR generation (service accounting for billing), supplementary services (such as call forward, diversion and park and pick-up) and dialing plans.

### 1.2. SIP Standard

The IETF Session Initiation Protocol (SIP) standard maintain the complete session of video and voice. This is a signaling protocol which initiates, manage and terminate the session across packet networks. The main benefits of use the SIP standard is able to one or more participants at same session or different session. Its SIP supports unicast and multicast communication, borrowing from Internet protocols, such as HTTP, SIP is text-encoded and highly extensible. SIP may be extended to accommodate features and services such as call control services, presence, instant messages, mobility and interoperability with existing telephony systems. Following are the four types of logical SIP entities:

User Agent: User Agent (UA) is the endpoint entity. User Agents initiate and terminate sessions by exchanging requests and responses. The User Agent as an application, which contains both a User Agent client and User Agent server. Devices that could have a UA function in a SIP network are workstations, IP-phones, telephony gateways, call agents, automated answering services and many more.

Proxy Server: It's an interrelationship entity which acts as a server and also as a client for the purpose of making requests on behalf of other clients. Proxy server also works for hold to end points till the response will not be available from other side.

Redirect Server: Its accept SIP request, maps the SIP address of the called or more new addresses and return them to the client after mapped. Unlike Proxy servers, Redirect Servers do not pass the request on to other servers.

Registrar: Its mainly use for register and record to all the operation. SIP has one protocol format for all actions, such as Registration, Call Control, and Presence.

### 1.3. Basic H.323 - SIP Call Scenario

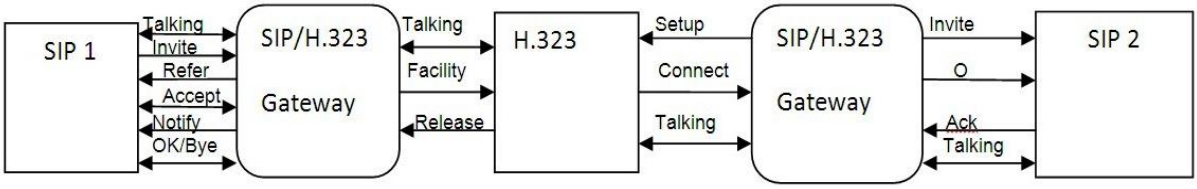



***Figure 1:*** *Schematic Scenario for Call Transfer by using H.323 and SIP*

## 2. Methodology

### 2.1. The Basic Protocol Architectures

**2.1.1.** ***H.323 Protocol Architecture*** H.323 protocol architecture first time passed by Study Group 16 in December as a first version of this standard H.323 v.1. Those completely capable for established a videoconferencing call on a LAN network [1, 2]. In which used to all the recommended connection and entities like as Gatekeepers, Gateway, and MCU, which provide multimedia communication over packet based networks. This standard is able for both audio and video. After then passed a new version the ITU-T H.320 protocol suite (H.245, H.225.0-CC), which able for used the existing protocol directly RTP and RTCP, This standard was designed a new concept for established the connection RAS (Registration, Admission and Status). RAS signaling functions are required for endpoint registration, admission control and address resolution. Call signaling function includes connection setup, capability exchange and open logical channel procedures, which also useful for maintain the records. H.323 established the end to end point connection by connected with MCU which perform the conference. Here following we define the protocol suit based basic architecture diagram of H.323 protocol, in which all the steps and mechanism will very clear. Diagram related to reference no. [8].

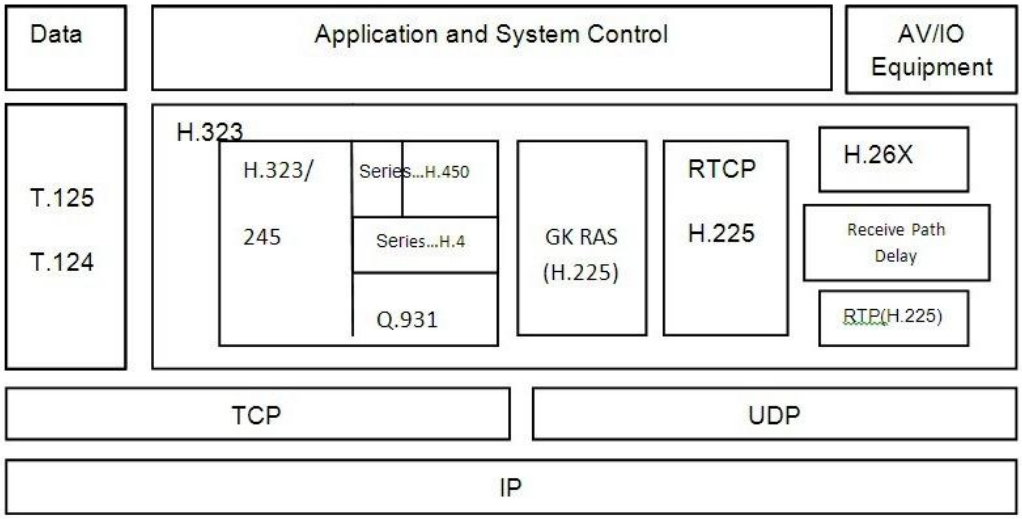



***Figure 2:*** *H.323 Protocol Suit*

**2.1.2.** ***SIP Basic Protocol*** SIP Protocol first time proposed by IETF (Multiparty Multimedia Session Control Working Group), which is capable for control telephony features over wide area network. In this standard, the main benefits are applicable for any type of network and able to integrate stores with conference multimedia. SIP capable for providing advanced signaling and control functionality for a large range of communication. The function of this standard is to locate the parties or resources, finds the actual address and network then sends invitation for service session and negotiation of session parameter. SIP provides a small number of text based messages to be exchanged between the SIP peer entities. By sending the message, servers will able for traverse by network. In this way, baseline SIP according to RFC 2543 includes all basic call control functionality in one signaling transaction using the INVITE request message. Conferences in SIP are normally lightweight multicast conferences, to which a user can be invited. Some Extensions for the management of distributed multipoint conferences have been drafted; in addition to the session processing using SIP, the IETF IPTEL WG proposes several possibilities for the programming of services either for administrators or for the users. SIP session signaling from audio/video media processing is shown in protocol suit. This SIP Protocol suit taken from reference no. [9].

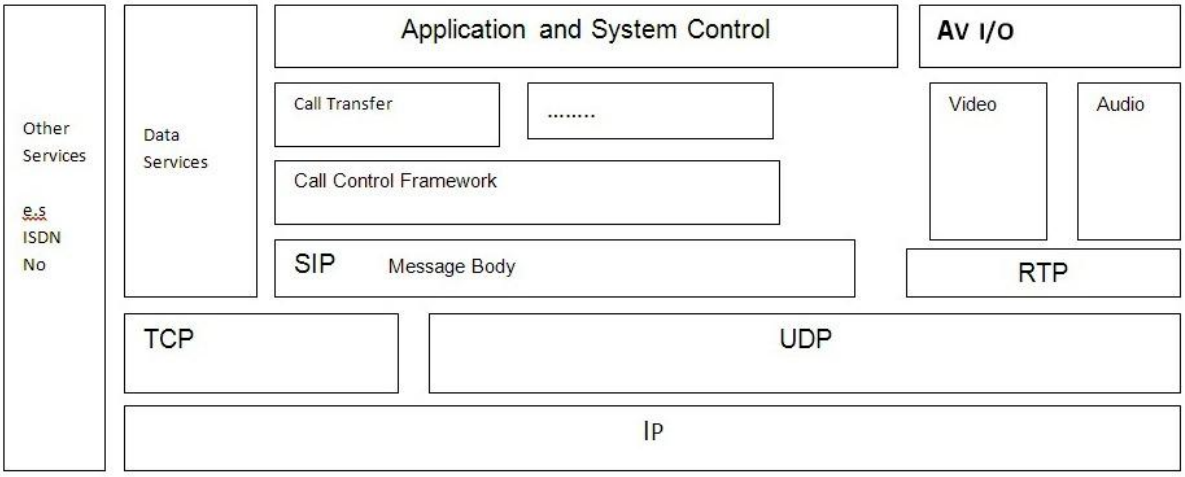



***Figure 3:*** *SIP Protocol Suit*

## 2.2. The Service Architectures

**2.2.1. H.323 *Service Architecture*** In this section, discussed service control of H.323, which is monitored by different models. In this, mainly described Distributed feature control (H.450), Stimulus feature control (H.323 Annex L) and Application layer feature control (H.323 Annex K).

**A) Distributed Feature Control Using H.450**

This features categorized into three different classes, in which first is local features. Local features can be implemented in the endpoints without requiring specific signaling to other network entities. Examples for local features are: repeat a call, call history and call lists, local address book, and speed dialing, privacy functions like do not disturb and mute, etc. [3]. Next features network-based features are implemented in a centralized fashion in the gatekeeper or as a backend service behind the gatekeeper. Examples are authorization, address resolution, call admission, call detail recording, name/number suppression, etc. The third category of features is the set of supplementary services (H.450). These features are important for special signaling between the corresponding entities. Examples are: call forwarding, call transfer, call completion, call hold, etc.

***I. Extension of H.450*** H.450 provides different types of process those allow easy extension of feature with define the set. H.450 supplementary service information sent on H.450 APDUs (application protocol data units) that may be contained in any H.225.0-CC message. H.450 APDUs are exchanged between supplementary service entities and does not influence the underlying H.225.0 call state. H.450 APDUs can be extended by manufacturer specific information. H.450.1 provides call-related and calling dependent transport of H.450 APDUs. Further, H.450 defines in a generic way how to proceed with H.450 APDUs that are not supported. This enables interoperability between endpoints with differing feature sets and a stepwise deployment of new supplementary services without having to support them in all endpoints at the same time.

***II. H.323/H.450 Architecture Endpoints*** The concept of H.450 features can be defined; they can be used together with the basic call as building blocks, which allow conceptual formats as a feature by combination of all small set with carefully designed building blocks. While application and further features are built by using local machine.

***III. Building Feature Combinations for 3rd Party Applications*** The building features of this architecture creating 3rd party call control applications. The functionality provided via the interface may also include functions like monitoring. The H.323/H.450 building blocks may as a remote controlled. The interface is accessible via a common protocol that may be used CSTA (Computer Supported Telephony Applications). An example for a 3rd party application is ACD (Automatic Call Distribution). It can be built up by combining basic call, call transfer to a music/video server, monitoring an ACD agent.

**B) Stimulus Feature Control Using H.323**

It is used to control the end point features into the network, defined in H.323 Annex L. Endpoints conforming to H.323 still use functional signaling (H.225.0) for controlling the basic call. This yields basic call interoperability with fully functional H.323/H.450 endpoints. There is little intelligence in the endpoints, the feature logic and the semantic procedures are defined in the centralized feature server. This allows an easier deployment of features only the feature server has to be updated, the endpoints do not have to be changed. On the other hand, there are no standardized semantics for the features. The semantics are implementation dependent. Applications that want to use the feature functionality for 1st party call control need a functional interface (API), which cannot easily be provided using the stimulus approach. A further downside of stimulus feature control is the scalability problem due to

feature processing in centralized network components.

**C) Application Layer Feature Control Using H.323**

H.323 capable for developing to the new services without any interchange or updating the protocol or end points. This mechanism allows for call-related and call-independent service control. Service control sessions can be maintained between endpoints or between endpoints and the network. In this feature the service control session will be connected after exchange the relevant information such as session ID, URL etc. [6]. The HTTP protocol is used in this service control channel to actually offer, select and activate the services. The service logic is described in HTML pages, scripts, etc. All of these can transfer by HTTP protocol. Thus, features can be controlled from any device running a conventional Web browser.

**2.2.2. *SIP Service Architecture*** SIP session based protocol, its control based on a distributed control model. SIP establishing VoIP connections. It is an application layer protocol for creating modifying and terminating the session with one or more end points. The SIP architecture so similar to HTTP, request is generate by client and forward to the server. For SIP the same feature categories can be applied as in H.323. Local features, network based features like authorization and address resolution in an outbound SIP proxy, and supplementary services. But, in defining supplementary services, SIP started with a different approach as compared to H.323 and standard telephony. Whereas traditional supplementary service implementation is standardized, SIP provides several elements to allow the construction of services. SIP defines the mechanism create the message like Invite, which identify by the headers like a receiver either it will transfer to his destination for proper route discriminators. SIP offers several different possibilities for programming of services with dedicated languages. SIP support session description that allow participants to agree on a set of compatible media type. It's also support user mobility by proxying and redirecting request to the user current activities. The SIP architecture provides services include- User location, Call Setup, User availability, User Capabilities, call handling. SIP provides a well-defined specification for feature negotiation. When a header is not known by a SIP entity it is ignored without affecting the rest of the request. SIP provides the require header that could be used by a SIP client to make sure in advance that a desired behaviour.

**2.2.3. *H.323 and SIP Service Architectures*** The implementation methods between the SIP and the H.323 service architecture in this survey is based on the following criteria: architecture, protocol extensions, message coding, service programming. The key characteristic of the H.323 service architecture is its explicit definition of separate state machines for each feature independent from the basic call state machine. From the signaling point of view the function split of feature control into framework and extensions is a consequence of this separation. In this SIP architecture, we assume two configurations are used for the call scenarios. One is basic configuration, which includes an H.323 and a SIP block. The other configuration contains an H.323 block and a SIP server block, which reside respectively in an H.323 zone for address resolution and admission control, and in a SIP administrative domain for pre-call registration service and address resolution.

As a consequence, important challenges like the subsequent integration of new features into a running system, the interoperability with heterogeneous endpoints. While according to the SIP baseline SIP features are not explicitly signaled and may even be hidden in the carried session description. Several programming languages are defined in the context of SIP for the programming of SIP servers. Although missing in H.323, they could also be applied for it. Since these programming languages are derived from the HTTP context they are more easily applicable for SIP as SIP is based on HTTP. To activate the appropriate service in the route IP network, SIP can specify the proxy servers that must be traversed by a SIP message; in H.323 this is not possible.

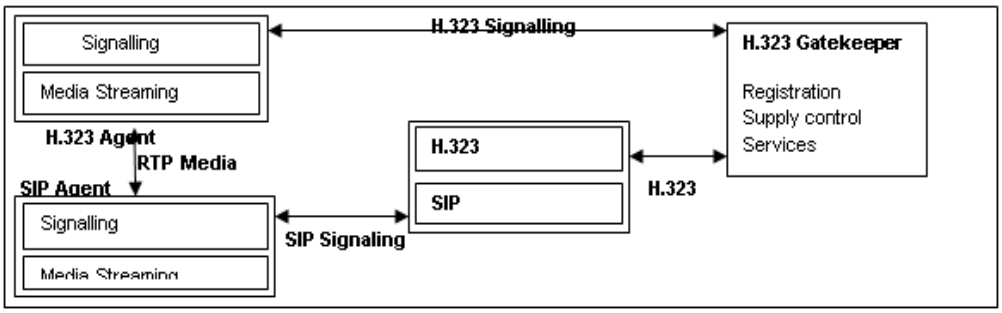



***Figure 4:*** *Interworking between H.323 and SIP*

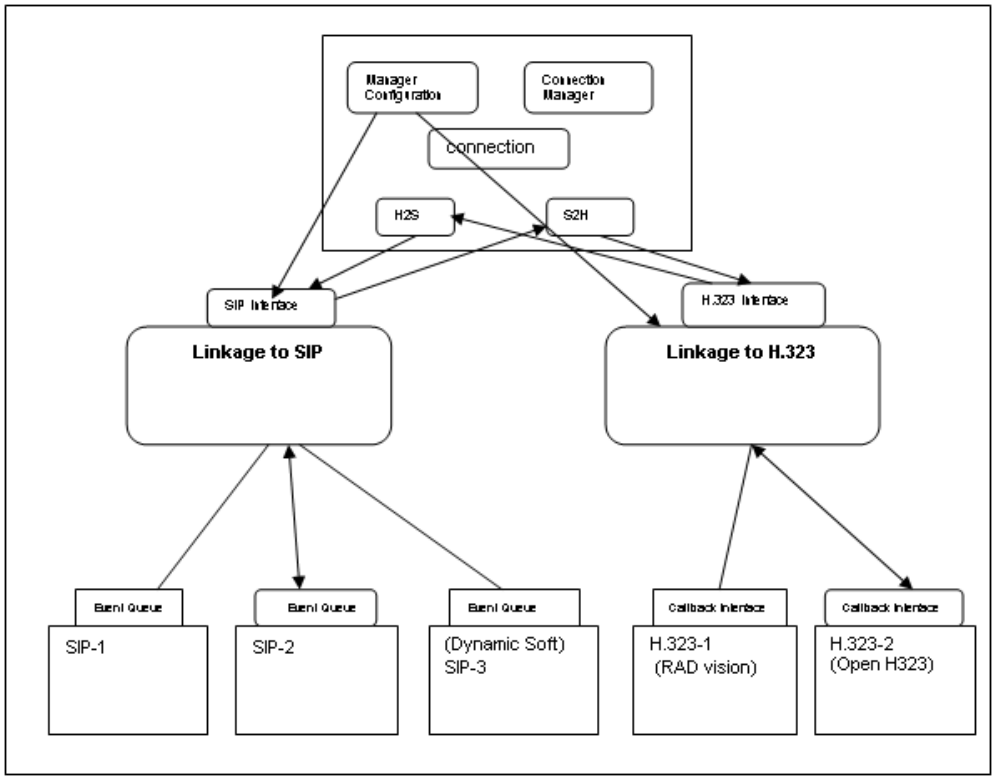



***Figure 5:*** *SIP/H.323 Architecture with Gateway*

## 3. Conclusion and Future Work

This survey has given overview architecture and the mechanisms to develop services using the two standards. Although both protocols may be used for video and voice applications. Both standards are design with a different specific features and assets. SIP implements for control the session for end points and also for create the session. H.323 has been set to handle voice and multimedia calls including supplementary services. In this paper, we have modelled and verified the system of interworking between H.323 and SIP with different configurations. H.323 describes and enables an object-oriented approach based on separating supplementary services from basic call control.

As per supporting on voice and multimedia over IP including supplementary services, H.323 is the good choice for IP telephony applications. This includes replacement scenarios for legacy, but is especially true when IP telephony supplements and coexists with legacy telephone systems. H.323 becomes more important for carrier implementations. Although the two standards are approaching each other, their focus and applicability is still different. It can be expected that neither of the two

protocols will succeed over the other. They will probably coexist in different environments and implementations over a longer time, putting also a strong requirement on interworking between them. Here in this we analyses and discuses too completely onto the two standards protocol H.323/SIP, which completely beneficial for the today era in voice and video calling. We consider the use of scripting within the gateway logic as promising approach that should be discussed as work in progress.

## References

[1] Henning Schulzrinne et al., 1998: *A Comparison of SIP and H.323 for Internet Telephony*. In Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV), Cambridge, UK.

[2] M. Handley. *SIP: Session Initiation Protocol*. Internet Draft Internet Engineering Task Force. http://tools.ietf.org/html/draft-ietf-mmusic-sip-12.

[3] R. Ackermann et al. *An Open Source H.323-SIP Gateway as Basis for Supplementary Service Interworking*. Darmstadt University of Technology, Industrial Process and System Communications (KOM), German National Research Center for Information Technology (GMD IPSI).

[4] International Telecommunication Union, 1996: *Visual Telephone Systems and Equipment for Local Area Networks Which Provide a Non-Guaranteed Quality of Service.* Series H: Audiovisual And Multimedia Sytems. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[5] Ajay P. Deo et al., 2000: *The SIP Servlet API*. Java SIP Servlet API Specification.

[6] Ralf Ackermann et al., 2000: *Implementation of a H.323/SIP Gateway*. Technical Report TR-2000-02, Darmstadt University of Technology, Industrial Process and System communications (KOM).

[7] Anshuman Srivastava et al. Detection of Tamporing in Fragile Watermark for Images by Using Back Propagation Method in ANN. International Journal of Research and Practices in Engineering Sciences. 2012. 1 (1) 82-86.

[8] Ashim Karim. H.323 and Associated Protocol. Technical Report in CSE WUSTL on h.323 protocol. 788-99. http://www1.cse.wustl.edu/~jain/cis788-99/ftp/h323.pdf.

[9] M. Jeffries, 2000: *An Interoperable Signaling Solution for IP-based Next Generation Networks*. Broadband Application and Networks Group, Department of Computer Science, University of the Western Cape, Cape Town, South Africa.

[10] ITU, 1998: T Recommendation H.323. *Packet-Based Multimedia Communications Systems*.

[11] RADVISION, 2001: An Overview of H.323 - SIP Interworking. [White Paper] Retrieved from http://www.radvision.com/NR/rdonlyres/1B7C291A-148C-4506-8312 D6DA2C58C7B7/0/OverviewofH323SIPInterworking.pdf

[12] DataBeam Corporation, 2002: *A Primer on the H.323 Series Standard. [White Paper] Retrieved* From http://www.packetizer.com/ipmc/h323/papers/primer.

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2014, Volume 3, Issue 1, pp. 51-67, Article ID Tech-136
ISSN 2320 – 0235

Review Article | Open Access

# Computer Crimes: Factors of Cybercriminal Activities

**Okechukwu Wori**

Department of Business Administration, Wayne State University, Detroit, USA, Department of Computer Information Systems, Detroit, USA

Correspondence should be addressed to Okechukwu Wori, ow.java@gmail.com

Publication Date: 23 January 2014

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-136



**Abstract** Cybercrime has increased exponentially in conjunction with the introduction and widespread use of electronic medium. This is not just confined to one area, but rather is occurring worldwide. Some progress has been made to counter this type of crime, but criminal legislation which crosses international borders is severely lagging behind. Some sort of public policy must be adopted, according to individuals, educational institutions, organizations and corporations who are interested in combating this wave of crime.
**Keywords** *Cybercrime; Profiling; Cyberthieves; Malicious Code; Attacks*

## 1. Introduction

Viewing cybercrime on a global level, there is an understanding that it has gone beyond rooftop of electronic medium. There is an ongoing effort to combat cybercrime, nevertheless, it continues unabated even across international borders. This vicious crime has continued to be a growing concern for individuals, organizations, corporations, and institution of higher learning hence has asked for legislation or public policy. The definition of cybercrimes is “Offenses that are committed against individuals or groups of individuals using modern telecommunication networks such as Internet and mobile phones” (Britz, 2008). Some amount of research has investigated the extent and types of cybercrime and the process of the prosecution of those crimes (Roberson, 2009; Hinduja, 2009; Shoemaker & Kennedy, 2009).

Cohen and Felson, in 1979, along with Hindelang, Gottfredson & Garafalo in 1978 published studies which looked at the lifestyles and routine activities perspective as well as the theories of crime (Gottfredson & Hirschi, 1990). There were also studies done by Ashalan, 2006; Bossler & Holt, 2010; Choi, 2008; Holt & Bossler, 2009 and Marcum, 2008. These were done to determine the reason for cybercrime. In general, they confirmed that not only situational but individual factors were important to analyze the criminal cybercrimes. However, determining how to pinpoint the characteristics of the victims of these crimes has not been determined (Bossler & Holt, 2010). Some studies have noted that a lack of self-control is one of the factors of victimization when an individual was the actual target

of the crime. But when computers were the targets of the crime, which would not, of course, be the case (Bossler & Holt, 2010). Therefore, the roles individuals and situational factors play must be assessed. According to Shoemaker, 2009, this will be vital in the development of a theory to explain cybercrime victimology and to come up with information to establish public policies.

Initially, cybercriminals were inclined to be counterculture types who worked alone and on the fringes of society. That situation has changed as the Internet has become an increasingly pervasive social medium. Now, instead of being inspired by a need to prove their art, cybercriminals are often motivated by financial gain. As a consequence, the old stereotypical image of the kid living on Skittles, while doing seventy-two hour hacks, has been replaced by a much darker and more complex approach, which is well organized and much more focused on making trouble (Bednarz, 2004). Today, cybercrime is about making money (Hochmuch, 2004). Just like the bank robbers of old, organized groups of cybercriminals perpetrate large scale raids on financial institutions. Much of that activity originates in places like China, India, Russia, Romania and Latin America, which puts those perpetrators out of reach of U.S. law enforcement agencies (Gudaitis, 2005).

With financial institutions, the repertoire for cybercriminal activity ranges from extortion and fraud to outright electronic theft (Gudaitis, 2005). In fact, the opportunities for financial gain from cybercrime are so great that established criminal syndicates have gotten into the business of electronic crime (Garretson & Duffy, 2004). As a result, security experts generally agree that law enforcement has to learn a lot more about the skill level, personality traits, and various methods of operation of computer criminals (Rogers, 2003). Cybercriminals count on the remoteness and anonymity that the Internet provides. Therefore, it is essential to be able to understand what cybercriminals actually know and, more importantly, what motivates them (Bednarz, 2004).

## 2. Progressive Effort

It should not be assumed that all cybercrimes are alike. In fact, cybercrimes and cybercriminals differ as much in motive, intent, and outcome as any type of physical criminal. Moreover, the general set of assumptions that underlie the investigation of cybercrime are the same as they would be for crimes in physical space. What is different is the form of the evidence. Evidence arising out of the electronic discovery process is not part of the physical world, so cyber-evidence is not the same as the evidence that investigators typically work with (Heiser & Kruse, 2002). Consequently, criminal investigators who, in the past, have relied on such concepts as physical artifacts, eyewitnesses, and confessions to solve crimes will now have to accommodate the fact that in most cybercrimes the bulk of the actual evidence will be in electronic or digital format (Rogers, 2003). Cybercrimes, just like physical crimes, still adhere to “Exchange Principle”, in that the perpetrator leaves some form of evidence at the scene and takes away some form of evidence which links them to the crime (Saferstein, 2001). In its raw, electronic form none of that evidence is easy to read or understand, so the task of evidence gathering and analysis in cyberspace is not an easy one. As a discipline, digital forensics makes that elusive virtual or electronic evidence meaningful to the conventional investigator. Digital evidence typically consists of binary data inscribed on a mass storage device, like a hard drive or a flash memory stick. The evidence itself can comprise everything from executable code artifacts, to the contents of a system table, all the way up to plaintext, or encrypted electronic content, or pictures. Sometimes for example, there are even very tiny pictures placed within pictures, which is known to cyber-forensic investigators as steganography.

While forensics is a useful tool in the evidence discovery process, there are a variety of other investigative techniques that are also important to the solution of any type of crime. Any or all of those approaches might be relevant to some aspect of the investigative process (Rogers, 2003). The problem is that cyberspace creates unique situations that no conventional investigative practice can accommodate. For instance, the actual perpetrators might be on the other side of the planet when

they commit the crime. Because of conditions such as this, new investigative approaches have to be employed. For example IP tracing techniques are common tools. These allow authorities to determine the origin of an Internet action even if it is located in a far-away place. The disconnectedness that the Internet provides raises another important issue, which is the location of the actual crime-scene. The investigator has to answer the practical question: is the real crime scene located where the perpetrator performed the act, or is it the victim's location?

One of the wonders of electronic criminality is it is possible to commit a criminal act that could best be described by a layman as a "bank robbery" from the safety of a location 6,000 miles away from the actual scene of the crime. The virtual nature of cyberspace allows that kind of unanimous crimes. (Cohen & Felson, 1979) have stated that "This has created a physical separation between the actual crime scene and the perpetrator, which then imposes unique complications of access and timing on the investigation of the crimes".

It is almost impossible to be able to use physical evidence to identify criminals who are operating under cyberspace's anonymous conditions. This can only be done by utilizing the single piece of evidence that will be available to investigators: the behavioral signatures of the individual perpetrator. In order to obtain that, highly technical information - evidence from unfamiliar sources like system logs and system level reconstructions of attack behavior have to be factored into the investigative process (Gudaitis, 2005).

## 3. Investigating Cybercrimes

In the investigation of traditional crimes, it is essential to understand three fundamental things: what motivated the offenders; how did they choose their particular victim; and what are the details of the crime? In the case of cybercrimes, common investigative techniques are modified to allow the investigator to approach the computer and its network as if it were a physical crime scene where those three factors can be studied. The investigator then gathers electronic evidence present at the scene in order to paint a meaningful picture of the specific motive and methods of a given offender (Bednarz, 2004).

Behavioral analysis is a key factor in this effort because, according to (Steven Branigan, 2004), companies are not going to solve computer security issues just by throwing technology at the problem. "It is about understanding how people behave," (Bednarz, 2004, p.1). In the case of a cybercrime, which is typically anonymous and can originate from an almost infinite number of places on the Internet, the ability to differentiate the unique behavioral characteristics of the perpetrator is an invaluable aid to the investigation.

As is the case with conventional investigations, profiling does not solve the crime itself. Instead, it focuses the investigator upon a workable set of suspects. Investigators analyze the unique set of behaviors exhibited by the offender in order to reconstruct a profile of the criminal's distinguishing characteristics. The investigator can use those distinctive behaviors to differentiate a particular offender from a group of potential suspects with similar Modus Operandi (MO). Because profiling is based on evidence gathered at the crime scene, the description of the perpetrator does not depend on the presence of witnesses. Thus, the ability to characterize a person who is otherwise not known, based strictly on signature behaviors, is one of the reasons why criminal profiling is such a productive contributor to the investigation of such offenses as serial crimes, where there are no witnesses to describe the suspect.

Profiling assumes that the psychological landscape of every individual criminal is different and so each perpetrator will behave slightly differently. As a consequence, profiling helps the investigator "see" the person behind the crime. This more intimate understanding is independent of other factors,

such as the criminal's method of operation (MO), which can typically be inferred from the physical evidence. Because it is important to understand the difference between the MO and the offender's personal behavioral "signature," we are going to elaborate on this idea a little further.

Most classes of crime, even cybercrimes, have a common method of operation (MO). For example, many hacking exploits rely on "canned" scripts that people pull down off the Internet. Knowing that a website was violated by a "script kiddy," as this type of offender is called, will not narrow the field of potential suspects down to a workable set. However, even script kiddies exhibit distinctive individual behaviors that are a result of their unique psychological composition. Some of the more immature types like to leave unique markings on a violated site to tell the world that (in effect) "Kilroy was here." Other more politically motivated offenders like to leave manifestos while others like to make intricate changes or additions to the website that they can subsequently display to their friends as a personal 'trophy" of their great intellectual prowess. Some will make surreptitious alterations, such as installing "back doors", that essentially allow the hacker to control the website.

All of these actions are distinctive behaviors that can potentially be used as identifiers to eliminate other individuals or classes of suspects. For instance, a script kiddy who leaves simple markings is usually just a novice hacker. On the other hand, a script kiddy leaving political messages can be inferred to be motivated by activist ideologies and thus more mature. Script kiddies who need to collect trophies are typically more broadly disturbed and, therefore, exhibit deviant behavior in other aspects of their life. Some, for example, have become involved in Internet stalking and sexual predation in the past (McGrath & Casey, 2002). Other hackers may display characteristics likened to Asperger's Syndrome an autism spectrum disorder which has surfaced in the background of a variety of other types of serial offenders (Murrie, Warren, Kristiansson, & Dietz, 2002; Silva, Leong, & Ferrari, 2004).

The one advantage that cyberspace provides to criminal investigators is the ability to look at an infinite number of individual actions in an infinite number of places, all at computer speed. Since the gathering and analysis of behavioral evidence can be automated, differentiating anonymous individuals based on their psychological characteristics is a particularly important aid to the investigation of cybercrime. That degree of data gathering and analysis would be impossible in physical space. However, because of the processing and retention capabilities of modern computer technology, it is not only possible, but relatively easy to monitor and analyze the actions of each individual user on any network in great detail. Therefore, whether anonymous or not, it is conceivably possible to differentiate every person from another in cyberspace if a detailed enough profile of the unique individual behaviors could be constructed. The assumption behind this is straightforward. Since computers are operated by people, and every person has a different set of personal capabilities and psychological terrain, it can theoretically be assumed that, if sufficient computing power was available, it would be possible to differentiate between every user based on unique capabilities and behaviors.

The psychological characterization of unknown subjects forms the basis of criminal profiling. The ability to use unique individual behavioral factors as a means of sorting out and identifying a specific criminal is not new. As a formal practice, some form of behavioral analysis has been a part of criminal investigations for well over a century. The earliest example of a behavioral profile was done by Dr. Thomas Bond in the "Jack the Ripper," case in the late 1880s (Hicks & Sales, 2006). It would seem logical then, to consider the usefulness of profiling when it comes to the investigation of cybercrimes as well. The only constraint is that those conventional profiling methods and techniques have to be modified to meet the unique conditions and requirements of virtual space.

## 4. Essence of Profiling Notion

Since cybercriminals rely on the anonymity that the Internet provides, it is essential to understand what they know and, more importantly what motivates them (Bednarx, 2004). Accordingly, additional actions which are irrelevant to the purpose of the crime but which are consistently carried out by the person can sometimes be used to build a particularized description of that individual (Rogers, 2003; Turvey, 2002). Moreover, since these actions are all part of the fundamental psychological make-up of the individual and are, therefore, unlikely to change, those behaviors can serve as a uniquely identifying fingerprint, or signature in the investigative process.

In terms of the practical investigation, however, it has to be remembered that building a profile based on signature behaviors is separate from the common aspects of a criminal investigation, such as determination of primary motive, method of operation and post-offense behavior (Rogers, 2003). In actual application, signature behaviors are unique to each perpetrator. Therefore, the gathering of that type of evidence should be carried out irrespective of considerations of the general motive and MO.

Because investigators must rely on virtual rather than physical evidence, a different set of evidence-gathering techniques has to be used. As we said earlier, because evidence is processed and stored by some form of computing device, the investigator has to employ evidence and analysis techniques that are primarily technological. Therefore the investigation must pay scrupulous attention to the details of system processing. This includes such meticulous exercises as time-stamp/time-pattern analysis, which uses data in the system logs, or analysis of programming behavior, which involves differentiating the stylistic and linguistic characteristics of the offender's coding technique (Gudaitis, 2005). In fact, if the right data-gathering utilities are in place, there might even be the capability to obtain a range of physiological observations, such as keystroke timing and even keyboarding technique (Rogers, 2003).

Finally, these micro-focused and somewhat esoteric technical practices are all very useful in building an individual profile of a particular cyber offender. However, it should also be noted that it is equally important to view the actions of each individual from the standpoint of the big picture, including factors like changes in the internal and external corporate environment (Gudaitis, 2005). There is nothing like a lay-off, mass firing, or plant closure to motivate individuals to mischief. Thus, knowledge of broader political, economic, and social conditions is also useful to the professional cyber profiler (Gudaitis, 2005).

The remainder of this article will review the history and possible applications of criminal profiling to future cybercrime investigations. This discussion will be built around an examination of the various current methodologies and how each of these methods adds to the investigation of common types of cybercrime. In addition, we will present and discuss some basic generic profiles the authors have developed using these technique.

## 5. Criminal Profiling

According to Canter, D., et al., "criminal profiling is a method for identifying the personal and behavioral characteristics of an unknown perpetrator of a crime. Profiling is based on an analysis of the nature of the offence and the manner in which it was committed". Profiling can either be reactive or proactive. With reactive or retrospective profiling, the investigator builds a profile in order to solve a crime that has already been committed. In the case of proactive or prospective profiling, the investigator is specifically attempting to prevent a crime from occurring (Reddy, Borum, Berglund, Vossekuil, Fein & Modzeleski, 2001).

One ordinary example of a proactive offender profile is the current Transportation Safety Administration (TSA) profiling of potential airplane hijackers. Proactive profiles such as these are not developed from the evidence of a specific crime scene, rather they are meant to inform TSA workers about behaviors that might be indicative of a potential hijacker, such as buying a one-way ticket with cash. Other examples of proactive offender profiling include drug dealer and pedophile profiles (Homant & Kennedy, 1998). It should be noted, however, that, in the past when proactive profiles have been used they have tended to be controversial because they are liable to generate false positives which can be used to support a claim of bias or prejudice. As a result, the more common use of profiling by police agencies is to support investigators after the occurrence of the crime.

The general aim of all profilers is to isolate identifiable behaviors or actions that describe how the offender is fulfilling a basic psychological or physical need above and beyond the commission of the crime itself (Petherick, 2005). Profilers do this by comparing the behavior at a specific crime scene with the behavior of criminals who were “profiled” in the past (Turvey, 1998). That comparison then allows profilers to make specific inferences about the lifestyle and offending history of an unknown person (Canter, 2000).

It is a common myth that the FBI’s Behavioral Sciences Unit developed the techniques of profiling during the 1970s (Petherick, 2005). In fact, however, the earliest handbook for profilers might be the Malleus Maleficarum, which was published circa 1486. That little manual provided helpful practitioner advice to professional witch hunters about ways that people of interest could be identified for the Inquisition (Turvey, 2002). There have been many examples of the use of profiles in the history of criminology starting as early as the 19th Century with the work of Jacob Fries and Cesare Lombroso. It should be kept in mind however, that no approach to profiling has been conclusively determined by rigorous scientific research to be theoretically and empirically correct (Palmero, 2005).

## 6. Methods of Profiling

Profiling can be approached from either retrospective or proactive perspectives. Additionally, profiling methods fall into two basic categories: inductive and deductive profiling (Petherick, 2005).

### 6.1. Inductive Profiles

With the inductive approach, the profiler assumes that people who have committed similar crimes in the past share characteristics with people who commit the same type of crime now. Thus, the characteristics of an unknown offender can be inferred from the characteristics and behavior of known similar offenders with the same general method of operation or even similar signature. Criminal investigators and profilers have found it useful to construct typologies of rapists (Hazelwood & Burgess, 2001), sexual murderers (Keppel & Walter, 1999), arsonists (Canter & Fritzon, 1998; Kocsis, Irwin & Hayes, 1998) and child molesters (Lanning, 1992) based on their experiences with prior crimes and criminals who have manifested similar crime scene behaviors.

Detailed explanations of the deductive approach to profiling, which characterizes much of the FBI method, can be found in treatises by (Douglas, Ressler, Burgess, and Hartman, 1986; Ressler, Burgess, Douglas, Hartman, and D’Agostino, 1986). Finally it should be noted that the organized-disorganized dichotomy that is the centerpiece of the FBI model also has its critics (Canter, Alison, Alison & Wentink, 2004; Hicks & Sales, 2006; Turvey, 2002), as has the entire discipline of profiling (Allison, Bennell, Mokros & Ormerod, 2002).

### 6.2. Applying Profiling to Cybercriminals

While there are no practical examples of the application of profiling to victimless crimes, it should be understood that when I use the term cybercrime I am talking about intentional crimes that harm a specific victim, or victims. In that respect, cybercrimes follow the same common set of rules as crimes in the physical universe. They can be targeted (organized), or untargeted (disorganized), they involve an MO, and they will leave behind specific behavioral signatures depending on the individual attacker. There is also a victimology associated with cybercrimes that can accurately suggest the type of criminal involved. Moreover, there is always some form of geographic component. For instance, it is almost impossible to pass a logic bomb through a firewall. Therefore, proximity is required that fits within the parameters of geographical profiling. My point is that the classic methods of profiling can all contribute to the prevention and solution of cybercrime.

In application, the organized-disorganized dichotomy is useful when it comes to understanding perpetrators of cybercrimes. For instance, untargeted worm based denial of service (DOS) exploits, which are the most common source of harm on the Internet, rarely fit the organized typology. Although the code exploit itself is planned, its impacts are unknown. Thus, the motive and intent are more typically characteristic of unfocused social patterns and psyche.

Just as physical crimes are often characterized by mixed motives, so too are cybercrimes. As cyber profiling efforts become more sophisticated, the organized-disorganized dichotomy may be replaced by a more appropriate heuristic model. Until such time, however, the beginning profiler may wish to consider the methodology evolved by Shoemaker and Kennedy. This approach is based both on the FBI's method of profiling, known as Criminal Investigative Analysis, and a second approach known as Turvey's Behavioral Evidence Analysis. Using these two models we believe that there are five sequential stages to the cybercriminal profiling process. These stages are sequential and they all apply directly to the investigation of cybercrime:

- Evidence gathering: Whether it is called an assimilation phase, or equivocal forensic analysis, the first step in any investigation is the collection of forensic evidence. This is no different for cybercrimes; the entire discipline of cyber forensics, has been created to address it.

- Behavior analysis focuses on the observable relationship of behavior to determine pattern in an attempt to obtain some set of characteristics facts of the crime. This process requires a follow up in evidence gathering and is a critical part of criminal investigation on cybercrime. Behavior analysis uncovers the unknown perpetrators based on the behaviors they display.

- Victimology: The victim profile can tell the investigator a lot about the type of perpetrator since there are well- known signatures associated with different types of crimes in cyberspace. This is as true for cybercrime investigation as it is for the investigation of crimes in physical space. For instance, an attack on a Microsoft product without an obvious motive beyond the actual attack is usually a statement, and statements are associated with counterculture behavior. That narrows the list of suspects down to cyberpunks who are frequently well known to authorities.

- Crime pattern analysis: This determines the 'what and how' of a cybercrime. Crime pattern analysis combines already known factors with any other considerations, such as geography and timing, into a logical theory of the actors and events of the crime. This is obviously a critical element of a typical physical investigation. Notwithstanding that fact, however, it would be impossible to approach a cybercrime intelligently without a fact-based, working hypothesis about the execution of the crime.

- Profile development: Once the crime itself is reconstructed, it is possible to formulate a profile of the offender. While these methods support deductive reasoning about the nature of the offender, it may be helpful to have generalized inductive typologies on hand to aid in the interpretation of fact patterns.

### 6.3. Twelve Cybercriminal Profiles

After a basic profile is constructed, investigators can compare the profile against different “types” of cybercriminal in order to further narrow their pool of suspects. The twelve profiles of cybercriminals were developed by Shoemaker and Kennedy which might be routinely encountered by law enforcement and information assurance professionals. They differentiated each of these types based on the motive, intent, and post-offense behavior of cybercriminals to build inductive profiles, which are derived from cybercriminal acts, which have been well documented in the literature as well as the media.

It should be noted however that although most of these profiles are unique, several of them, specifically the “Kiddie” (cf. Fitzgerald, 2005), the “Cyberpunk” (cf. Hafner, 1991) the “Cyberthief” (cf. Goodell, 1996) and the “Cyberstalker” (cf. Bocij, 2004) have had varying degrees of coverage in both academic publications and the popular literature.

Kiddies are technologically inept. Motivated by ego, they use preprogrammed scripts, and their intent is almost always to trespass. More advanced kiddies will engage in privacy exploits. Kiddies can be any age, but they are always outsiders and not technologically hip. They are usually new to crime and can be tracked by matching a crime to the individual who has downloaded a suitable tool-set from hacker websites.

Cyberpunk Hackers are members of the counterculture. Because they are also ego-driven, their intent is almost always trespass or invasion. Invasion based hacks are usually motivated by pure exposure. Cyberpunks will engage in theft and sabotage, but only against what they perceive as legitimate targets. Cyberpunks are responsible for many viruses, application layers, and DOS attacks targeted on “establishment” organizations, companies, and products. A cyberpunk is invariably young, technologically proficient, and a social outsider.

Old-Timer Hackers are perhaps the most technologically proficient members of the hacker community. They are ego driven and the last of the Old Guard whose only intent was to prove their art by trespassing. They are relatively harmless because they know what they are doing and their motives are relatively benign. Where their actions cause harm, they generally specialize in website defacement. An old-timer is middle aged or older with a long personal and/or professional history in technology and possibly hacking.

Code Warriors are the first of the more destructive profiles. In the past they were driven by ego or revenge. Now, they are almost motivated by monetary gain. As such, they usually engage in either theft or sabotage. Their crimes are built around code exploits - specifically application layer attacks and Trojan horses. Like old timers, they are technologically proficient with long and visible histories in technology, and are likely to have been identified as having committed hacking exploits in the past. They can be any age but, because their art is a profession in and of itself, most of these individuals fall into the 30 to 50 age range. They are likely to have a degree in technology but are not employed in that sector or may even be unemployed. Code warriors are almost always socially inept and show signs of social deviance.

Cyberthieves are motivated by monetary gain, either through the illicit sale of valuable information or by outright theft. Their crimes are built around any means to that end. They are specifically adept at

surreptitious network attacks such as sniffing or spoofing. As such, the individuals in this profile use network tools and simple programming exploits such as Trojans and malware rather than targeted code. They are also very adept at social engineering, which amounts to running a classic con game. They can be any age, but this profile does not require a long history in technology. Therefore, these perpetrators can be younger than the code warrior. Most are organizational insiders, but some are found outside the organization.

The unhappy insider is perhaps the most dangerous profile in the entire set. These people commit crimes from inside most organization's defenses. They are motivated by revenge or monetary gain and uses extortion or exposure of company secrets for the purpose of theft, or sabotage. The unhappy insider's intent is to steal, or harm items of value to the company. He can steal information, set destructive logic bombs, or perform other malicious acts on the system. A distinctive characteristic of this perpetrator is his unhappiness with the organization. These individuals are insiders who can be of any age and employed at any level. The only protection against this type of perpetrator is to identify signs of unhappiness and closely monitor further actions.

An Ex-insider is the terminated former employee motivated by extortion, revenge, sabotage, or disinformation. These individuals are focused on harming the organization that dismissed them. If they can see the dismissal coming, they might set logic bombs or perform other destructive acts. Otherwise, they will make use of insider information to harm or discredit the company from the outside. They can be any age and work at any level. The only protection from this type of malcontent is to plan a dismissal to ensure a clean break. A sure sign of the work of an ex-insider are attacks on company vulnerabilities that were not public knowledge.

The Cyberstalker is an individual motivated by ego and deviance. The primary intent of this perpetrator is an invasion of privacy for the purpose of learning something to satisfy some specific personal need (like jealousy). The chief tool of the perpetrators in this category is the key-logger; however, more sophisticated cyberstalkers will use targeted Trojan horses or sniffers. This profile is differentiated from the other ego-driven profiles by the fact that these invasions of privacy are driven by an actual psychological need. Identification of that need, which is their fingerprint, will often point to the cyberstalker.

A Conman is an individual motivated by simple monetary gain, and his intent is primarily theft, or some form of illicit commercialization. This type is adept at social engineering and spoofing. Members of this group run traditional con games like the Nigerian scam, as well as newer exploits like phishing. These attacks are typically untargeted and anonymous. Because of that anonymity, con men are very difficult to catch once they have hit. Since the con man depends on the ignorance of his victim, the best defense is awareness.

The Mafia Soldier is organized crime's entry into the field of cybercrime and is differentiated from all other categories by its purposefulness and high level of organization, which is second only to that of the war fighter. Mafia soldiers are motivated by the same goals of their non-technical brethren in crime monetary gain. This end is achieved by the same means: theft, extortion and, occasionally, invasion of privacy for the purposes of blackmail. Mafia soldiers have the distinguishing characteristics of the code warrior or con man. However, they always work in highly organized groups; often with the best technology money can buy. The most common incarnation of this type currently works out of the Far East and Eastern Europe. However, given the ease and profitability of Internet crime, it is expected that every organized crime group in the world will eventually be into this business.

## 7. Types of Cybercriminal Exploits

As we said earlier, all forms of cybercrime are constrained by the technology. Therefore, there are a limited number of ways that the perpetrator can go about committing a cybercrime, no matter the typology. Fundamentally, all computer based crimes are limited to two general categories: the injection of some form of malicious code, or a technological exploit aimed at a selected target. The latter type of attack can be either electronic, or physical. Any of the profiles we have just discussed could execute either of these exploits. Since the approach is usually shaped by the intent, one can assume that certain types of criminal exploits can be more closely associated with particular criminal types and they include:

### 7.1. Malicious Code

Much of the malicious code currently encountered by cyber investigators is a hangover from the earlier days of cybercrime when the motivation was ego, instead of profit or revenge (Honeynet, 2001). When ego is the motivator, most of this code is a product of two of the profile types we discussed earlier: cyberpunks and code-warriors. Script kiddies have also been involved in spreading some viruses, but since they depend on the other two categories for the tools, they will be discussed separately. There are four accepted categories of malicious code: viruses, logic bombs, Trojan horses and malware. Each of these has a slightly different criminal application; therefore, each involves a different typology.

Most malicious code exploits may be defined as “disorganized” in that there is no particular target involved, ego is a primary motivator, and there is no financial profit motive that would accrue directly to the perpetrator. Where profit from a malicious code exploit is involved, the typology is clearly organized. That is because the crime is conceived, targeted, and executed with a plan for criminal gain or revenge, and utilizes a certain degree of care. Targeted malicious code is being written to put in bot-nets, key loggers, to steal databases, or to harvest computers and then sell the bandwidth off to spammers (Hochmuth, 2004). Based on some degree of past study, most of the people who carry out the organized type of malicious code exploits fit the characteristics of the “organized” typology (Saita, 2001; Honeynet, 2001; Casey, 2000).

Viruses are generally created as a demonstration of programming technique rather than as any focused attempt to take over the world. On the other hand, worms, which are a specialized type of virus, might have features that would be associated with an organized type of perpetrator since they are responsible for denials of service (DOS). When activated, they carry out preprogrammed attacks on a network or networks. Because they cause denials of service, worms are increasingly being used for extortion and sabotage. The motivation behind a worm is almost always aggressive and destructive. Therefore, people who construct worms are more likely to have specific criminal motives. Criminals who have carried out acts in this category, and who have been apprehended and studied, tend to fit very solidly into the organized typology. The first example of a worm based exploit is the Great Worm of 1988, which specifically targeted the UNIX operating system. The perpetrator was almost immediately tracked down and arrested, because the authorities were able to associate the intent of that worm with critical comments made about that specific vulnerability. Thus, in effect, this case also becomes the first instance of the use of a profile to solve an Internet cybercrime. Logic bombs, on the other hand are examples of planned exploits. They are programs activated in a host machine based on specific parameters and are almost impossible to detect once they are set. These exploits are invariably used for destructive purposes. As such, they are a key tool for crimes like extortion, sabotage, and even infowar. Their weakness is that close or hands-on access is usually required to set a logic bomb, unless it is delivered by a Trojan horse. As such, they are also almost perfect examples of an organized type of crime. They can be extremely dangerous because, if set by hand, it is possible to build a great deal of malicious functionality into a logic bomb’s programming.

Profiles are extremely useful investigating logic bomb cases because they invariably require physical access to set them. Therefore, the perpetrator can be profiled just as he or she would for a physical crime. Crime scene evidence can be gathered and analyzed, and geographic profiling can even be used. The only problem with profiling in this respect is that it is mostly after the fact, since logic bombs are usually discovered after the harm is already done.

Finally, if commercialization and cyberstalking are issues, there is the special case of malware. Malware is code that is transferred to a visitor's computer when his browser visits a site preselected by the cybercriminal. Malware can include such innocuous things as data miners and ad-ware. But malware can also deliver things like home page hijackers and key-loggers. Ad-ware is an example of Internet commercialization.

The more malicious forms of malware are always set for specific criminal purposes such as theft. The problem with profiling this category is that malware offenders exhibit both organized and disorganized characteristics. Although the primary purpose of their endeavor is known and planned in advance with a certain degree of remorselessness, the actual victim can be any person who visits the site. The dispersal of the adware exhibits some of the characteristics of "sin" type victimologies in the sense that the websites associated with "mainstream" activity do not set malicious objects. Consequently, the most likely place to pick up a botnet hijacker is from a site associated with "fringe" type commerce, such as a pornography site. In that respect, some of the attitudes and criminal motivations for people who set highly malicious objects match those of their sin-trade counterparts.

The problem with investigating malware is that those malicious agents are usually unfocused in their intent. Since the victim usually randomly self-selecting, the perpetrators of those crimes are hard to profile deductively. Plus, because the malware itself is usually picked up from a fringe site, the crime is not as likely to be reported. The only way to profile the writer of malware is through inductive profiling techniques, which are usually less accurate. Because of the constraints of geographic space, this almost never produces a workable list of suspects.

### 7.2. Targeted Attacks

Profiling is particularly useful in the case of targeted attacks. A good profiler can differentiate the general characteristics of the attacker based on attack type (Petherick, 2005). This makes it possible to prepare a defense in advance where the attack can be anticipated from an inductive typology, or it can facilitate the tracking and prosecution of otherwise anonymous attackers by analyzing their signature or MO.

Targeted attacks are just like any other kind of organized criminal activity. They are motivated, methodological, and usually have a specific victimology associated with them. Targeted attacks fall into eight generic types: Insider, Password, Sniffing, Spoofing, Man-in-the-Middle, Application Layer, Denial of Service, and Social Engineering.

#### 7.2.1. Insider Attacks

The insider attack has always been the most prominent threat, and probably always will be. No one knows the security system better than an insider. If that person becomes disgruntled, they can easily steal privileged information by loading it on a memory stick, for example, and walking out the door with it. They can also send that information to any external place since the firewall is outward facing. That is, most firewalls are designed to detect potential inbound violations instead of outbound ones. Finally, besides violations of confidentiality, insider attacks can also be extremely destructive since, "until just a few years ago, most security appliances didn't even look internal within the network" (Hochmuth, 2004, p.2). As a result, insider attacks account for up to three-quarters of the reported

annual loss to cybercrime in the U.S. (Garretson & Duffy, 2004; CSI, 2004). Since these crimes center on human behavior, insider attacks can be profiled, and the ability to predict who might execute them can help get monitoring in place to prevent the acts before they occur.

Although some insider attacks might be directed towards targets of opportunity and thus fit the disorganized typology, most are planned; as such, the characteristics of the perpetrator almost always fit the organized type. The victim is overwhelmingly the insider's place of work. However, there are a significant number of instances where an insider uses his or her status with a business partner to carry out a crime. No matter the victimology, insider attacks fit the general motivation and method of an organized type of crime aimed at criminal profit.

### 7.2.2. Password Attacks

Password attacks are simple exploits. The aim of a password attack is to either guess a password or obtain it through confidence scams, which are otherwise known as social engineering. In the past, the aim of most password attacks was to trespass merely for the sake of ego. However, access can also lead to theft and sabotage. In both cases, the attack has to be carefully planned and executed. Therefore, it is invariably classifiable as an organized type of exploit, and the general characteristics associated with that typology apply.

Nevertheless, given the reliance on social engineering, which is the manipulation of people in order to trick them out of sensitive information such as passwords, the most likely method of attack is through personal contact. Social engineering type password attacks constitute up to 90 percent of the total attacks of that type (Garretson & Duffy, 2004; CSI, 2004). As such, the likeliest person to perpetrate a password attack is an individual who is in close physical proximity to where the attack originated, such as an insider or client.

### 7.2.3. Sniffer Based Attacks

Finally, in addition to the types of criminal behavior that we have discussed so far, deviants also use sniffing exploits for the purpose of invasion of privacy. These are almost always motivated in the same way as other types of personal crimes, such as sex crimes. The aim of this behavior is to gain some form of advantage or control over the victim by securing knowledge that is either private or personal. In cases such as this, the perpetrator almost always has some form of direct relationship to the victim, or the victim fulfills some type of common fantasy. In both cases, this type of offender closely fits the typical methods and doctrines of physical profiling.

### 7.2.4. Spoofing Based Attacks

Spoofing is another example of an organized type of crime because it requires careful planning and execution to convince others that the sender of an Internet packet or message is legitimate. As such, the attributes of the organized typology are just as accurate for spoofers as they are for other criminals of this type.

There is one difference, however; because spoofing has become something of a business enterprise in various third-world countries (Bednarz, 2004; Garretson & Duffy, 2004; Gudaitis, 2005); the spoofer is almost never a classic loner. Instead, he is part of a large and well- organized group of criminal participants. Just like sniffing, spoofing is done in order to perpetrate more destructive crimes like theft or sabotage. At the technological level, this exploit typically involves spoofing an IP address by changing the packet-header information. At the behavioral or social engineering level, this can entail simple or elaborate phishing scams or spamming using recognizable addresses.

Spoofing is almost always done for the purpose of gaining access for profit. It is a common technique used by every category of criminal; however, it is the chief technique of the electronic con man. In order for the spoof to work properly, the victim has to be tricked into believing something that is not true. One of the interesting asides of this method is that, because of IP spoofing, the computer itself is as likely to be the target victim as any human dupe.

The likeliest type of individual to employ IP spoofing is the cyber thief or code warrior. The more powerfully malicious categories, such as the mafia soldier and the war fighter, also employ this technique but, compared to the other categories, there are relatively few of those latter types in the game. The common thread for all of these types is their technical proficiency. As such, the list of suspects in an IP spoofing incident is fairly easy to compile compared to the practitioners of the behavioral spoof.

The individuals who engage in behavioral spoofing are exactly like the old-fashioned con men of literary fame. In fact, many of these spoofing exploits bear the same time-worn names, like the Nigerian Scam, the Lottery Scam, and the ever popular Pigeon Drop. In a behavioral exploit of this type, the victim is unknown to the criminal until they respond to the spoof. The spoof itself is usually a “mass-mailing” exploit involving a very large number of unknown but potential victims. Because the behavioral spoof does not involve specifically targeting a victim, the victimology can also fit into the disorganized typology (e.g., the specific behavior of the victim creates the target).

### 7.2.5. Application Layer Attacks

Application layer attacks are explicit code exploits which involve inserting a malicious code entity into a two-party conversation as a third party. This usually takes place on a network, using a Trojan horse as a delivery mechanism. However, it can also be a direct physical attack if the agent is a key logger placed on the victim’s system by the criminal party.

On the other hand, application layer attacks arrive at a specific application through a defect or vulnerability in the code (buffer overflow, for example). Application layer attacks are the most common direct exploits in the cyber universe. These attacks require careful planning and execution. They also invariably require a reasonable level of technical know-how and skill. As such, the perpetrators in this case have attributes that are very close to the typology associated with the organized criminal.

Most frequently, these exploits occur for the purposes of theft, extortion, sabotage and infowar (CSI, 2004; Garretson & Duffy, 2004; Bednarz, 2004). As such, where profit is involved, they tend to best describe the exploits of the mafia soldier, cyber thief the code warrior, or even the cyberpunk profile if the target is an institution like Microsoft. The more sinister types like the war fighter could also use these exploits to commit the sort of mayhem that is typically international in significance.

The majority of the crimes that are rated as significantly destructive by agencies such as the FBI’s Computer Security Institute (CSI, 2004) and the U.S.-CERT are application-layer attacks. The problem for law enforcement is that the perpetrator is almost always unknown and to some extent unknowable. Because of the level of technical proficiency required to carry out such an attack, the attacker is ensured in advance there will be no evidence. As such, the only effective option available is solid cyber profiling.

### 7.2.6. Denial-of-Service

Finally, denial of service (DOS) is an explicit attack aimed at preventing a host from gaining access to the Internet. Targeted attacks can be technological, or they can be simple physical assaults, such as vandalizing the server. There can also be untargeted, broad-spectrum attacks, such as worm-based

DOS attacks. Monetarily, this category of exploit is the most harmful type in the entire group of potential attacks. It is estimated that one DOS exploit alone, MyDoom, cost companies up to $250 million dollars in lost productivity and prompted Microsoft to offer a $250,000 reward for the capture of the criminals involved (Stein, 2004).

Since targeted DOS attacks are done for profit or revenge, these perpetrators fit squarely into the organized typology. If the purpose of the attack is profit, the perpetrator is likely to be a code warrior or a mafia soldier. Conversely, if the attack is strategic, then one can assume that the perpetrator is a war fighter. All of these individuals display skill, careful planning, and precise execution. They can also be counted on to leave no useful evidence. However, because of the nature of the exploit, which typically involves overwhelming the transmission medium with a large number of messages or requests, it is almost impossible to target a DOS attack to a single victim. Therefore, a targeted DOS attack is nowhere near as common or harmful as a broad spectrum or untargeted DOS.

Broad-spectrum or untargeted DOS attacks are typically motivated by personality issues or even occur by accident. Therefore, they fit into the disorganized typology. In fact, if the assumption is made that the perpetrator did not have mass-destruction in mind, it can be said that every worm-based crime, from Code Red to Santy, displays the same lack of organization.

Accidental DOS, which is an attribute of the disorganized type, is a particularly common occurrence and is a consequence of a lack of knowledge. For instance, the person who perpetrated the first DOS attack, the Great Worm, claimed that he was only trying to discover the limits of the Internet. Untargeted attacks are characteristic of the cyberpunk who typically has an axe to grind, such as the SQL Slammer (aka the Sapphire Worm) or MyDoom. A cyberpunk motivated DOS could be considered to be targeted in the sense that companies such as Microsoft are frequently the intended victim. However, since the actual victims are the millions of users of their products, it is hard to classify that type of attack as specifically targeted.

Every cybercriminal could conceivably engage in DOS attacks; however, recently kiddies have been among the most notorious. The attributes of a script kiddy are also a perfect example of the attributes of a disorganized cybercriminal: technologically inept, a younger or immature personality and a fringe worker in a non-technical field.

### 7.2.7. Social Engineering

Social engineering is a strictly behavioral exploit. It is also a very common form of attack. Social engineering scams can vary in sophistication from dumpster diving to actually running short and long-term con games and stings. These are always organized type crimes, and they almost perfectly fit the attributes of that category of cybercriminal.

If they are not ego driven, social engineering attacks are typically done to steal something like a password or account information. However, they are also used for everything up to Infowar and strategic, political, or disinformation purposes. Since social engineering gambits are behavioral, they can generally be classified based on what the attacker seeks to gain (Hochmuth, 2004). The only true practitioner of a strictly social engineering exploit is the con man type. However, social engineering is still a part of the art of the cyberpunk, the cyber-thief and the cyberstalker.

Table 1 used dichotomous dependent variables, and logistic regression from lifestyles/routine activities theory (LRAT)**)** to assess the effects of individual and situational factors on the prevalence of nine forms of cybercrime. They include: malicious code, targeted attacks, insider attacks, password attacks, and sniffer based attacks, spoofing based attacks, application layer attacks, denial-of-service, and social engineering.

***Table 1:*** *Logistic Regression of Nine Forms of Cybercrime on LRAT Measures and Control Variables*

| | 1 Malicious Code (n=231) | 2 Targeted Attacks (n=230) | 3 Insider Attacks (n=231) | 4 Password Attacks (n=229) | 5 Sniffer Based Attacks (n=231) | 6 Spoofing Based Attacks (n=230) | 7 Application Layer Attacks (n=230) | 8 Denial of-Service (n=231) | 9 Social Engineering (n=229) |
|---|---|---|---|---|---|---|---|---|---|
| **Exposure to Motivated Offender** | | | | | | | | | |
| Internet Hours | -.01(.99) | .00(1.00) | .01(.99) | .02(1.02) | .03(1.03) | .00(1.00) | .00(1.00) | .00(1.00) | .03(1.00) |
| Email Hours | .01(1.01) | .00(1.00) | .00(1.00) | .00(1.00) | .04(1.04) | -.01(.99) | -07(.93) | .05(1.00) | .00(1.00) |
| IM Hours | .03(1.03) | -.02(.98) | .06(1.06) | .02(1.02) | -.01(.99) | .01(1.01 | .00(1.00) | .02(1.01) | .00(1.04) |
| Chart Room Hours | -.01(.99) | .05(1.05) | -.03(.97) | .02(1.02) | -.04(.96) | -.(.98) | .00(1.00) | .01(1.00) | .00(1.00) |
| **Target Suitability** | | | | | | | | | |
| Communication with Strangers | .49(1.63) | .0(1.01) | .85(2.33) | .33(1.39) | -.01(.99) | .32(1.38) | .88(2.41) | .03(2.51) | .07(3.08) |
| Provide Personal Information | -.02(.98) | .89(2.43) | -.13(.88) | -.(.41) | .51(1.66) | -.55(.57) | .77(2.16) | .02(1.56) | .04(3.00) |
| Click Open Link | -.43(.65) | -.11(.99) | -.20(.82) | .10(1.10) | .03(1.03) | .00(1.00) | -.18(.83) | .03(1.76) | .03(1.00) |
| **Capable Guardianship** | | | | | | | | | |
| Computer Skills | .00(1.00) | -.43(.65) | -.38(.69) | .16(1.18) | -.53(.59) | .05(1.05) | .43(1.16) | .08(1.09) | .01(2.00) |
| Security Software | .74(2.10) | .53(1.70) | .05(1.05) | .49(1.62) | -.53(.59) | .05(1.41) | -.06(.95) | .04(1.06) | ..01(1.07) |
| Computer Crime Information | .47(1.59) | .61(1.84) | -.41(.66) | .80(2.22) | .05(1.05) | -.01(.99) | -.24(.78) | .06(.49) | .02(1.09) |
| **Control Variables** | | | | | | | | | |
| Male | -.30(.74) | -.05(.96) | .59(1.80) | .44(1.55) | -.89(.41) | .13(1.14) | .30(1.35) | .56(.35) | .37(1.07) |
| Age | -.02(.98) | -.03(.97) | -.03(.97) | .02(1.02) | .00(1.00) | .47(1.61) | -.38(.69) | .03(1.24) | .76(1.78) |
| Employment | -.49(.61) | -.48(.62) | 1.29(3.62) | -.58(.56) | .16(.31) | .47(1.61) | -.38(.69) | .16(1.20) | .54(1.34) |
| Married | .30(1.35) | .00(1.00) | .06(1.06) | -.43(.65) | -.29(.75) | -.16(.85) | .63(1.88) | .14(1.30) | .26.(1.09) |
| Computer Deviance | -.11(.89) | .01(1.01) | .67(1.95) | .50(1.64) | .23(1.26) | .37(1.44) | .01(1.01 | .12(1.45) | .19(1.65) |
| Constant | -.20(.63) | .27(1.29) | .15(1.16) | .39(1.48) | .48(.08) | -.49(.04) | .87(2.39) | -.84(.43) | .-.44(.64) |

Data analysis (from Cybercrime Victimization reference to, lifestyles/routine activities theory (LRAT))

## 8. Conclusion

In conclusion, we have introduced and discussed herein the practice of cyber profiling. As physical crimes are sometimes quite amenable to criminal profiling, so too are cybercrimes. Many physical crimes leave behind insufficient evidence to support criminal profiling, and this may be true of certain cybercrimes as well. Because the art of cyber profiling is evolving so rapidly, we fully expect portions of our discussions on this chapter to be somewhat outdated in the near future. (Kilger, et el., 2004) in their writing identified that motivations such as money, entertainment, ego, and entrance to social groups and status have been with us for a long time and are unlikely to disappear soon. Perhaps a better model for understanding and identifying cybercriminals may evolve through the creation of a typology which more intricately blends the concept of organized and disorganized cyber-attacks with the motives mentioned above. We hopefully await this development.

## References

Alison, L., Bennell, C., Mokros, A., and Ormerod, D. *The Personality Paradox in Offender Profiling: A Theoretical Review of the Processes Involved in Deriving Background Characteristics from Crime Scene Actions.* Psychology, Public Policy and the Law. 2002. 8; 115-135.

Bednarz, A., 2004. Profiling Cybercriminals. Network World. www.networkworld.com, November 29, 1–2.

Bocij Paul. *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. Praeger Publishers, 2004.

Branigan, S., 2004: *High-Tech Crimes Revealed: Cyber War Stories from the Digital Front*. Addison-Wesley, Boston.

Canter, D.V. *Offender Profiling and Criminal Differentiation.* Legal and Criminological Psychology. 2000. 5; 23-46

Canter, D., Alison, L., Alison, E., and Wentink, N. *The Organized/Disorganized Typology of Serial Murder: Myth or Model?* Psychology, Public Policy, and Law. 2004. 10*;* 293-320.

Canter, D., and Fritzon, K. *Differentiating Arsonists: A Model of Firesetting Actions and Characteristics*. Legal and Criminal Psychology*.* 1998. 3; 73-96.

Casey, E. *Criminal Profiling, Computers and the Internet*. Journal of Behavioural Profiling*.* 2000.

Computer Security Institute. 2004: *Annual Survey of Computer Crime in America*. Federal Bureau of Investigation, Washington, D.C.

Douglas, J., and Olshaker, M., 1995: *Mindhunter: Inside the FBI Elite Serial Crime Unit*. Mandarin Paperbacks, London.

Douglas, J.E., Ressler, R.K., Burgess, A.W., and Hartman, C.R. *Criminal Profiling from Crime Scene Analysis*. Behavioural Science and the Law. 1986. 4; 401-421.

Fitzgerald Michael, "Hackers, Crackers and Script Kiddies, Oh My!" Yahoo! Tech Tuesday, January 13, 2004, accessed January 2007.

Garretson, C., and Duffy, J., 2004: *Cybercrime: The Story behind the Stats. Network World.*, *www.networkworld.com*, November 29, 2004, 1–2, accessed 12/2006.

Goodell Jeff, 1996: *The Cyberthief and the Samurai: The True Story of Kevin Mitnick-And the Man Who Hunted Him down*. Dell, New York, USA.

Gudaitis, T., 2005, April 6: Profiling Cybercrime. *ITBusinessedge*. Retrieved September 2006, from www.ITBusinessedge.com.

Hafner Katie, 1991: *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Simon & Schuster, Inc., New York, USA.

Hazelwood, R., and Burgess, A. (Eds.). 2001: *Practical Aspects of Rape Investigation: A Multidisciplinary Approach.* 3rd Ed. CRC Press, Boca Raton, FL.

Heiser, J.G., and Kruse, W.G., 2002: *Computer Forensics: Incident Response Essentials*. Addison Wesley Professional Series, Boston.

Hicks, S., and Sales, B., 2006: *Criminal Profiling: Developing an Effective Science and Practice*. American Psychological Association, Washington, D.C.

Hochmuth, P., 2004: *Profiling Cybercrime–"Network Threats and Defence Strategies",* Network World, *www.networkworld.com*, November 29, 2004, 1–2, accessed 12/2006.

Homant, R., and Kennedy, D. *Psychological Aspects of Crime Scene Profiling: Validity Research.* Criminal Justice and Behaviour. 1998. 25; 319-343.

The Honeynet Project (ED.), 2001: *Know Your Enemy: Revealing the Security Tools, Tactics and Motives of the Blackhat Community.* Addison-Wesley, Boston.

Keppel, R., and Walter, R. *Profiling Killers: A Revised Classification Model for Understanding Sexual Murder.* International Journal of Offender Therapy and Comparative Criminology 1999. 43; 417-434.

Kilger, M., Arkin, O., and Stutzman, J., 2004: Profiling. In: The Honeynut Project (Ed.), *Know Your Enemy: Learning about Security Threats.* 2nd Ed. 505-556. Addison Wesley, Boston.

Kocsis, R., 2006: *Criminal Profiling.* Totowa, Humana Press, NJ.

Kocsis, R., Irwin, H., and Hayes, A. *Organized and Disorganized Criminal Behaviour Syndromes in Arsonists: A Validation Study of a Psychological Profiling Concept*. Psychiatry, Psychology and Law. 1998. 5; 117-131.

Lanning, K., 1992: *Child Molesters: A Behavioural Analysis*. National Center for Missing and Exploited Children, Alexandria, VA.

McGrath, M., and Casey, E. *Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace*. Journal of the American Academy of Psychiatry and Law. 2002. 30; 81-94.

Murrie, D., Warren, J., Kristiansson, M., and Dietz, P. *Aspergers Syndrome in Forensic Settings.* International Journal of Forensic Mental Health. 2002. 1; 59-70.

Palermo, G.B., and Kocsis, R.N., 2005: *Offender Profiling: An Introduction to the Socio-Psychological Analysis of Violent Crime.* Charles C Thomas Publisher, Springfield, IL.

Petherick, W., 2005: *The Science of Criminal Profiling*. Barnes and Noble, New York.

Petherick, W., (Ed.), 2006: *Serial Crime: Theoretical and Practical Issues in Behavioural Profiling.* Academic Press, New York.

Radcliff, D., 2003: *Profiling Defined*. Network World Fusion. Retrieved January 2005 from www.nwfusion.com.

Reddy, M., Borum, R., Berglund, J., Vossekuil, B., Fein, R., and Modzeleski, W. *Evaluating Risk for Targeted Violence in Schools: Comparing Risk Assessment, Threat Assessment and Other Approaches*. Psychology in the Schools. 2001. 38; 157-172.

Ressler, R.K., Burgess, A.W., Douglas, J.E., Hartman, C., and D., Agostino, R. *Sexual Killers and Their Victims: Identifying Patterns Through Crime Scene Analysis.* Journal of Interpersonal Violence. 1986. 1; 288-308.

Rogers, M. *The Role of Criminal Profiling in the Computer Forensics Process*. Computers and Security. 2003. 22; 292-298.

Saferstein, R., 2001: *Criminalistics: An introduction to Forensic Science*. 7th Ed. Prentice Hall, Upper Saddle River, NJ.

Saita, A., 2001: Hacker Psychology, Understanding Peopleware. *Information Security Magazine*. http://infosecuritymag.techtarget.com/articles/june01/featureshacker_psychology.shtml.

Silva, J., Leong, G., and Ferrari, M. *A Neuropsychiatric Developmental Model of Serial Homicidal Behaviour*. Behavioural Sciences and the Law. 2004. *22;* 787-799.

Stein, A., 2004, January 30: Microsoft offers MyDoom reward, CNN/Money. Retrieved December 2006 from http://money.com.

Turvey, B., 1998: Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques. Knowledge Solutions Library. http://www.corpus-delicti.com/Profiling_law.html.

Turvey, B., 2002: *Criminal Profiling: An Introduction to Behavioural Evidence Analysis.* 2nd Ed. Academic Press, New York.

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2013, Volume 2, Issue 1, pp. 42-50, Article ID Tech-160
ISSN 2320 – 0235

Research Article | Open Access

# Comparative Analysis of Trends of Cyber Crime Laws in USA and India

**Rajlakshmi Wagh**

IMED, Department of Management, Bharati Vidyapeeth IMED, Pune, Maharashtra, India

Correspondence should be addressed to Rajlakshmi Wagh, rajlakshmi@wagh.org

Publication Date: 9 December 2013

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-160



**Abstract** Today's Global era needs laws governing fast paced cyber crime. The popularity of on-line transaction is on the rise thereby having attempts made by unscrupulous entities to defraud internet users. The modus operandi may be in the form of Hacking, Spoofing, Pornography, Scanners, Device, Fake card and the like. The Educational sectors, Defense sector, Law Enforcement Bodies, Bank sectors are exposed to risk as the information sought usually includes data such as username, passwords, bank account and credit card number, revelation of which is huge loss for not only every individual but also the state at large. The paper is an analysis of the USA Laws for Cyber Crime with a comparative analysis with the Indian Laws. The aim is to analyze the conviction rate in cyber crime with comparison to both the countries and suggest various remedies.
**Keywords** *Statutes; Offences; Sections; Conviction*

## 1. Introduction

The challenges faced by cyber laws are vast due to geographical hurdles, cultural patterns and land laws governing one's particular land. Easy access to cyberspace is one of the main reasons for the growth of cyber crime thereby threat to the National security of the country. There exists a dearth of adequate laws. According to NASSCOM, there is extremely low rate of conviction of cyber crime in India. It saddens to say that India as a country in its 10 years old history of cyber crime investigation has so far witnessed only four convictions.

The statistics show that 1600 have been arrested against 3682, where the conviction is shocking 7 of which 3 are significant. To look into more detail the number of crime has gone up by 10 fold. I would like to bring to the notice that such a rise in the crime is due to low rate of conviction rate [1]. In the year 2007, the arrests made were 154 while in the following year there was 178. In the years 2009 and 2010, the numbers of persons arrested were 288 and 799 and in 2011, it was 1,184. This shows clearly a huge rise in the number of arrests but yet a single digit conviction rate [2]. A further record

also show that 217,288, 420,966 and 1,791 cyber crime cases were registered under IT Act, 2000 during the years 2007, 2008, 2009, 2010 and 2011.

## 2. Overlook of Some of the Cyber Crime Affected States in India

In Karnataka 307 cases of cyber crime were booked in the last 9 years and only 60 of them have been charge sheeted and not seen a single case of conviction in cyber crime [3]. According to State Criminal Investigation Department (CID) statistics, the conviction rate is 8.2 per cent, which means it has achieved in only nine out of 100 cases [4].

## 3. An Overview of Some of the Status of Convictions in India

The first conviction came in through the Sony India Private limited case. The complaint was filed by Sony India Private Limited which used to run a website sony-sambandh.com which enabled NRIs to send Sony products to India. On this site a colour television was ordered and the payment was made through a credit card. The product was to be delivered to Noida and all procedures had been followed. However two months later the credit card said that this was an unauthorized transaction following which a case of cheating was filed with the CBI. On investigation it was that the person who received the television set had gained access. Before court the crime was admitted and the accused was convicted. However the court released the accused on probation for a year since he was only 24 years old [5].

## 4. An on Look of Conviction Rate in the USA

A total of 145 cases against 243 defendants were also terminated during the year, representing an eight percent decrease in cases terminated and 19 percent increase in defendants terminated when compared to the prior year. Eighty-six percent of all terminated defendants were convicted, with 61 percent of the convicted defendants sentenced to prison. This data represents only those cases and defendants charged directly under the federal computer intrusion statute, 18 U.S.C. § 1030, and the provisions regarding stored electronic communications, 18 U.S.C. §§ 2701-2711 computer intrusion cases involving financial loss are often charged under the federal fraud statutes, and other intrusion cases may be brought under the federal identity theft statute, 18 U.S.C. § 1028.

The number of complaints registered with Internet Crime Control Centre (IC3) of the USA from 2006, 2007, 2008, 2009, 2010, 2011 are 207,492; 206,884; 275,284; 336,655; 303,809; 314,246 [6]. This also shows the awareness of cyber laws among the Americans.

A detail study of the Cyber law legislation in America show a listing of various statutes from 1970 till date.

### 4.1. US Cyber Crime Laws: An Exordium

**The Wire Fraud Statute** being the first law used to prosecute computer criminals in the USA. It was seen that the communication wires were used in international commerce to commit fraud. To overcome such US passed the Law so as to prohibit the use of communication wires. This was an effective statute as it was to overcome defrauders trying to obtain money, property by false representation or promise; modus operandi being radio or television communication, signs or signals [7]. This statute was successfully used in 1970's and 1980's to convict government officials of defrauding the public of its intangible right [8]. In a paradigmatic case Governor Marvin Mandel of Maryland was convicted of mail fraud for promoting certain legislation beneficial to the owners of a race in violation of his obligation to render the citizen of the state fair and impartial service free from bribery [9].

The era witnessed technological progress so this Statute suffered certain limitations the wire fraud statute was written without computer crime in mind and as such it has serious limitations when dealing with it, not all computer related crimes can be prosecuted with it, not every crime committed using a computer is done with the intent to commit a fraud, and not all computer crimes use interstate or international wires [10]. A need for a more effective law namely **The Computer Fraud and Abuse Act CFAA** – 1984 and amended in 1986. This being one of the most important statute as it deals with computer crime. The main reason for it to be amended in 1994 was that it could deal with the problem of "Malicious Code" such as viruses, worms and other programs which are designed to destroy data on a computer. The Act suffered major lacunae as it could not prosecute those who transmitted programs with intent to cause damage to the computer [11].

The National Information Infrastructure Protection Act was created to further expand the protections granted by the Computer Fraud and Abuse Act of 1986. Under the new act, protective measures were extended to computer systems used in foreign and interstate commerce and communication. The bill consolidated several older laws, including standing espionage laws, and labeled new crimes for stealing classified information from government computers [12]. CFAA is also known as Title 18 U.S.C Section 1030. NIIA made it illegal to view information on computer without authorization [13].

In 1986 the Electronic Communication Privacy Act (ECPA) was amended making it illegal to intercept stored or transmitted electronic communication without authorization. It prohibited illegal access and certain disclosures of communication contents. Later on amended in 1994 [14]. The CSEA (Cyber Security Enhancement Act) was passed together with Homeland Security Act in 2002. This Act granted powers to the law Enforcement Organizations and increased penalties set out in the Computer Fraud and Abuse Act [15]. The Act authorizes harsher sentences for individuals who knowingly or recklessly committed a computer crime that resulted in death or serious bodily injury.

## 5. Other Laws for Computer Crime Prosecution

EEA Economic Espionage Act passed in 1996. To stop trade secret misappropriation. There being other Statute namely National Stolen Property Act and Virginia Internet Policy Act comprising of 7 bills. The proposed Computer Crime Legislation namely,

FOISA – Fraudulent Online Identity Sanction Act, registering online domain under false identification, increase jail time to provide false information.

CSPCA – Computer Software Privacy and Control Act, to deal with eighth problems of spyware. When passed it would prohibit transmission of software that collects and transmits personal information about the owner or operator of the computer.

The US legal system is and always more tech savvy and specialized to tackle various issues. In case of credit Card Fraud in USA there is a separate Federal Credit Card Law that stipulates the consumer. The Fair Credit Billing Act (FCBA) will apply to billing errors on credit card, unauthored charges, charges for goods and services. This Act is an attempt to minimize Credit Card Fraud in India.

## 6. Laws Governing Cyber Crime in India

The Information Technology (Amendment) Act 2008 is the only Legislation that governs cyber crime in India. Till date it has brought various sweeping changes. The various sections that have been amended are Section 66 A - An offence to send offensive messages, Section 66B – An offence to receive stolen computer resource. Section 66C, 66D, 66E & 67F are inserted to declare identity theft, cheating and percolation, violation of piracy, video voyeurism and cyber terrorism and such which are

punishable under the IT Act. The section 67A, 67B & 67C which provides punishment of imprisonment of three years and fine for acts such as, child pornography.

## 7. Civil Wrong

Section from 43 to 47 tackles the civil liability of individuals. The liability is to the extent of damages. The quantum of compensation is decided by the adjudicating officer as he has jurisdiction to adjudicate such claims which does not exceed Rupees five Crore. Section 64 provides for recovery of penalty as arrears of land revenue for the suspension of license or Digital Signature Certificate till penalty is paid.

## 8. Criminal Wrong [16]

| | |
|---|---|
| Section 65 –Tampering with computer Source Documents, imprisonment up to 3 years or fine which may extend to two lakh rupees or both. | Sec 66E – Punishment for violation of privacy, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees or both. |
| Sec 66 – Computer Related Offences with reference to section 43, punishable with imprisonment for a term which may extend to 3 years or with fine which may extend to five lakh rupees or both. This section has reference to IPC for some definitions. | Sec 66F – Punishment for cyber terrorism, shall be punishable with imprisonment which may extend to imprisonment for life. |
| Sec 66A – Punishment for sending offensive messages through communication service, punishable with imprisonment for a term which may extend to 3 years and with fine. | Sec 67 – Punishment for publishing or transmitting obscene material in electronic form. |
| Sec 66B – Punishment for dishonestly receiving stolen computer resource or communication device. | Sec 67A – Punishment for publishing or transmitting of material containing sexually explicit Act shall be punished on first conviction with imprisonment for a term which may extend to five years and with fine which may extend to ten lakh rupees and further punishment on subsequent conviction. |
| Sec 66C – Punishment for identity theft, punishment with imprisonment which may extend to 3 years and liable to fine which may extend to one lakh rupees. | Sec 67B – Punishment for publishing material depicting children in sexually explicit act in electronic form shall be punishable on first for a term to five years and with a fine which may extend to ten lakh rupees and for subsequent offence, punishment for term which may extend to seven years and also with fine which may extend to ten lakh rupees. |
| Sec 66D – Punishment for cheating by personating by using computer resource, punished with imprisonment which may extend to three years and shall be liable to fine which may extend to one lakh rupees. | |

## 9. There are Other Offenses Covered Under IPC and Special Laws

| | |
|---|---|
| Sec 503 – Sending threatening messages by email | Sec 464- False document |
| Sec 499 – Defamation | Sec 468 – Forgery for cheating |
| Sec 463- Forgery | Sec 469 – Forgery for purpose of harming reputation |

- **Bogus Website, Cyber Frauds**

Sec 420 – IPC Cheating and dishonestly inducing delivery of property.

- **Web – Jacking**

Sec 383 IPC Extortion

- **Email Abuse Online Defamation**

Sec 500 – Punishment for defamation
Sec 509 IPC Word gesture or act to insult modesty of women.

- **Criminal Intimidation by E-Mail or Chat**

Sec 506 – Punishment for criminal intimidation
Sec 507- Criminal Intimidation by an anonymous communication

- **Online Sale of Drugs, NDPS Act**
- **Online Sale of Arms Act**
- **Piracy – In Copyright Act**

Sec 51, Sec 63, Sec 63 B

- **Obscenity**

Sec 292 – Sale of obscene books
Sec 292- A printing of grossly indecent matter for blackmail
Sec 293- Sale of obscene objects to young persons.
Sec 294 – Obscene acts 7 songs.
Section 378. Theft
Section 379. Punishment for theft

**The Indian Evidence Act 1872** is another legislation amended by the ITA. Earlier to the passing of ITA, all evidences in a court were in the physical form only. By the passing of the ITA it gave recognition to all electronic records and documents as subsequent amendments were made to The Indian Evidence Act. Words like 'digital signature', 'electronic form', 'secure electronic record' information' as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations [17].

**The Bankers' Books Evidence (BBE) Act 1891 has been** amended. Prior to the passing of ITA, any evidence from a bank to be produced in a court, necessitated production of the original ledger or other register for verification at some stage with the copy retained in the court records as exhibits. With the passing of the ITA the definitions part of the BBE Act stood amended.

**The Anti Money Laundering Act 2002** having its main objective to for confiscation of property derived from, or involved in, money laundering.

**The Critical Information Infrastructure Protection (CIIP)** the Central Government being empowered to appoint a National Nodal Agency responsible for all measures including research and development [18].

## 10. Status of Persons Arrested as against Cases Registered in India

The table below shows a list of cyber crime for the past 5 years from 2009 to 2011. A Crime wise statistical report of increase in crime and also persons arrested. Source NCRB [19].

| Sr. No. | Crime Head under IT. Act | Cases Registered from 2009 Onwards | | | | Persons Arrested | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 08 | 09 | 10 | 11 | 08 | 09 | 10 | 11 |
| 1. | Tampering computer source documents | 26 | 21 | 64 | 94 | 26 | 06 | 79 | 66 |
| 2. | Hacking with Computer System i) Loss/damage to computer resource/utility 109.0. (ii)Hacking | 56 | 115 | 346 | 826 | 41 | 63 | 233 | 487 |
| | | 82 | 118 | 164 | 157 | 15 | 44 | 61 | 65 |
| 3. | Obscene publication/transmission in electronic form | 105 | 139 | 328 | 496 | 90 | 141 | 361 | 443 |
| 4. | Failure (i) Of compliance/orders of Certifying Authority ii) To assist in decrypting the information intercepted by Govt. Agency | 1 | 3 | 2 | 6 | 1 | 2 | 6 | 4 |
| | | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| 5. | Un-authorized access/attempt to access to protected computer system | 3 | 7 | 3 | 5 | 0 | 1 | 16 | 15 |
| 6. | Obtaining license or Digital Signature Certificate by misrepresentation/suppression of fact | 0 | 1 | 9 | 6 | 11 | 0 | 1 | 0 |
| | Publishing false Digital Signature Certificate | 0 | 1 | 2 | 3 | 0 | 0 | 0 | 1 |
| | Fraud Digital Signature Certificate | 3 | 4 | 3 | 12 | 3 | 0 | 6 | 8 |
| | Breach of confidentiality/privacy | 8 | 10 | 15 | 26 | 3 | 3 | 5 | 27 |
| | Other | 4 | 1 | 30 | 157 | 0 | 0 | 0 | 68 |
| | **Total** | 288 | 420 | 966 | 1791 | 154 | 178 | 288 | 1184 |

From the above table it is seen that the cyber crime criminals arrested is 50% less overall, showing that the law enforcement agency should mold themselves to the fast paced cyber crimes and the effective Legislations.

## 11. Conclusions

Legislations in other nations as against the lone legislation ITA and ITAA in India, in USA there are many legislations governing e-commerce and cyber crimes going into all the facets of cyber crimes. Data Communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in the particular area focused in the Act.

In the US, they have the Health Insurance Portability and Accountability Act popularly known as HIPAA which inter alia, regulates all health and insurance related records, their upkeep and maintenance and the issues of privacy and confidentiality involved in such records. Companies dealing with US firms ensure HIPAA compliance insofar as the data relating to such corporate are handled. The Sarbanes-Oxley Act (SOX) signed into law in 2002 and named after its authors Senator Paul Sarbanes and Representative Paul Oxley, mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud.

Besides, there are a number of laws in the US both at the federal level and at different states level like the Cable Communications Policy Act, Children's Internet Protection Act, Children's Online Privacy Protection Act etc. In the UK, the Data Protection Act and the Privacy and Electronic Communications Regulations etc are all regulatory legislations already existing in the area of information security and cyber crime prevention, besides cyber crime law passed recently in August 2011.

In India the government has taken steps in the framing of The National Cyber Security Policy. This policy proposes to

a) Facilitate collaboration between government agencies and private cyber security solutions developers in order to optimize and protect critical government initiatives

b) The policy is a road map for strengthening cyber security as it will secure a computing framework that will inspire consumer confidence for electronic transaction.

c) At the macro level the policy will facilitate cyber security intelligence that will form an integral component to anticipate attacks and quickly adopt counter measures.

The Central and the State Government have been authorized to issue directions for interception or monitoring or decryption of any information through any computer resource. Both the governments, in the interest of sovereignty or integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, may intercept, monitor or decrypt or cause to intercepted, monitored or decrypted any information generated, transmitted received or stored in any computer resource. They can block public access to any information through any computer resource.

Dream to keep the society crime-fee will remain a dream in India as there should be constant endeavor for the legislation to keep in pace with the fast pace in crimes. Especially in a society that is dependent more and more on technology, crime based and electronic offences are bound to increase and the law makers have to go the extra mile keeping in pace to the fraudsters as technology is always a double-edged sword and can be used for both the purposes – good or bad.

We can conclude that though the cyber police have become proactive but the rise in the number of instances may be due to weak law and to have appropriate legislations for the fast track crime. To suggest Fast Track courts to be set up to keep in pace with the giga second of commission of cyber crime.

The government has set up cyber crime cell in various states of India yet the need to have well trained Law Enforcement bodies so they do not find it difficult to defend their cases in the court of law. The need is felt to have expertise personnel police who could specialize to handle cyber crime. These cyber crime offences are bailable offences leading to the lack of confidence in the laws.

## References


[1] Rediff.com, Dec, 2012. http://www.rediff.com/business/report/tech-cyber-crime-1600-arrested-only-7-convicted/20121211.htm

[2] NCRB Report. http://www.rediff.com/money/report/tech-cyber-crime-1600-arrested-only-7-convicted/20121211.htm

[3] indlaw.com (The Definitive Guide to Indian Law), 1997-2013. www.indlaw.com/guest/Displaynews.aspx?indlaw.com

[4] PuneMirror.in, 24th Nov., 2012: Rate of Conviction Shows Decrease, Cyber Crime Up. Bennett Coleman & Co. Ltd. http://www.punemirror.in/article/2/20121124201211240823554 8196c927a5/Rate-of-conviction-shows-decrease-cyber-crime-up.html?pageno=9

[5] National Crime Records Bureau (Ministry of Home Affairs). http://ncrb.nic.in.

[6] Internet Crime Complaint Center. 2011 Internet Crime Report. http://www.ic3.gov/media/annualreport/2011_ic3report.pdf

[7] Legal Information Institute (LII). 18 USC 1343-Fraud by Wire, Radio, or Television. 1988. 113-36.

[8] Aaron. D. Hoag. *Defrauding the Wire Fraud Statute: United States v La Macchia*. Harvard Journal of Law and Technology. 1995. 8 (2) 511.

[9] Aaron. D. Hoag, Defrauding The Wire Fraud Statute: States v. Mandel, 591 F.2d 1347, 1360 n.7 (4th Cir. 1979), cert. denied, 445 U.S. 961 (1980). Harvard Journal of Law and Technology. 1995.

[10] Maxim May, Fedral Computer Crime laws, SANS Institute: Reading Room Site. June 1, 2004, 2.

[11] Maxim May, Fedral Computer Crime laws, SANS Institute: Reading Room Site. June 1, 2004, 2.

[12] National Information Infrastructure Protection Act, United States, Gale Encyclopedia of Espionage & Intelligence, 1. http://www.answers.com/topic/national-information-infrastructure-protection-act-united-states

[13] Maxim May, Fedral Computer Crime Laws, SANS Institute: Reading Room Site. June 1, 2004, 3.

[14] Maxim May, Fedral Computer Crime laws, SANS Institute: Reading Room Site. June 1, 2004, 5,

[15] 99th Congress. Electronic Communications Privacy Act (ECPA). Public Law 99-508. October 21, 1986. Retrieve on May 24, 2000. http://www.cpsr.org/cpsr/privacy/communications/wiretap/electronic_commun_privacy_act.txt.

[16] Maxim May, Fedral Computer Crime laws, SANS Institute: Reading Room Site. June 1, 2004, 6.

[17] Ministry of Law, Justice and Company Affairs (Legislative Department), 9th June 2000: The Information Technology ACT, 2008. New Delhi.

[18] NCRB, Chapter 18. Cyber Crimes. http://ncrb.nic.in/CD-CII2011/cii-2011/Chapter%2018.pdf.

[19] Ministry of Law, Justice and Company Affairs (Legislative Department) Section 69, Information Technology (Amendment) Act 2008. New Delhi.

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2015, Volume 4, Issue 1, pp. 68-77, Article ID Tech-367
ISSN 2320-0235

Cloud Publications

**Research Article** **Open Access**

# Analysis and Evaluation of NLP Training Effectiveness

**Abha Purohit and Chiranjiv Kumar Kantiya**

Department of Management, Jodhpur National University, Jodhpur, Rajasthan, India

Correspondence should be addressed to Chiranjiv Kumar Kantiya, chiranjivkantiya@gmail.com

Publication Date: 8 January 2015

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-367



**Abstract** The main objective of this paper is to analyze and evaluate NLP training effectiveness in terms of efficiency, behavior and perception of trainees who have undergone NLP training course of different levels at various places of India from different trainers and evaluate their response on the basis of questionnaire filled by them after the training. NLP Stands for Neuro Linguistic Programming and it consists of series of techniques and well tested methods to achieve success satisfaction and excellence in life in your core domain. The basic assumption of NLP is that if someone can do you can also and this technique is called modeling. NLP assumes that actual impact of an event in life is just 10% and 90% is the ways we respond, handle and use our resources on the happening of that event. So if you want to take control of your life take your reactions in control by changing mindset. Analyzing the feedback questionnaire of 530 participants who have undergone NLP training course it is clearly visible that more than 75% (Pie charts of individual question attached) of participants agree that NLP training can really act as a catalyst and as a tool for positive transformation and rapport building, increasing efficiency of an individual, managing thoughts, moods, and behavior and for overcoming depression. NLP can also be used for changing perception and broaden thinking horizon. NLP can also be used in goal setting and defining life purpose. The feedback also states that NLP may help in decision making, conflict management and the statement 'Words can change Minds' appears true. The analysis also gives a signal that NLP can increase efficiency of individual and organization moreover people agree that NLP education should be given at school level itself. Corporate employees, working professional and housewives should undergo NLP training to look at things with a different mindset to get different results. The evaluation also indicates that Lemay be used as a relationship building tool that can improve relationship like Husband/Wife, Employer/employee, Parent/child and Teacher/Student. The paper is a study of 530 participants who have undergone training from various parts of India. Further scientific evaluation is also proposed to test the validity of results and reach at a concrete decision.

**Keywords** *NLP Training Effectiveness; Communication; Perception; Behavior*

## 1. Introduction

### 1.1. History of NLP

NLP was invented by two academicians Richard Bandler and John Grinder in 1970 at University of Santa Cruz California. Bandler was a psychology student and he studied a range of subjects from Gestalt therapy to mathematics and computing at the University of California. Grinder was an assistant professor of linguistics at the university. The two men became friends and began working together, both influenced by the Family Therapy work of Virginia Satir, Fritz Perls' Gestalt Therapy, and Milton H. Erickson's.

Grinder and Bandler modeled these three successful therapists, seeking to discover the difference that made the difference-what it was that set these people apart from average.

### 1.2. Components of NLP

**Neuro**: Refers to the nervous system. Neuro is to do with the way we use our minds, our bodies, and our senses to think and make sense of our experience. Our experience of the world enters the brain via nervous system through 5 senses visual, auditory, kinesthetic, olfactory and gustatory. The more awareness we have of our thinking patterns, the more flexibility and therefore the more influence we have over our life. NLP is concerned with how we process this sensory experience and translate it into conscious and unconscious thought. By increasing our awareness of the patterns in our thinking, we can learn how these thought patterns influence the results we are getting in work and in life. The key to finding personal and business success comes primarily from within ourselves and learning about how we think enables us to tap into our inner resources [1].

**Linguistic**: Refers to language, specifically the way we use language to give meaning to experience. Our language is our life. What we can say is what we can think and what we can do. Learning to understand and master the structure of our language is essential in a world where we trade increasingly through our ability to communicate.

**Programming**: It refers to the way we consistently think or behave. Just like a computer, each of us run specific programs to produce our behavior. Programme consists of series of steps that automatically produce certain results in different circumstances. NLP can reveal the program you run and the result they produce. We run our lives by strategies, in a similar way that a computer uses a program to achieve a specific result. By understanding the strategies by which we run our lives we give ourselves choice: choice to do more of the same or choice to enhance our potential and our individual excellence. NLP does this not by prescribing fixed techniques that work for some, but by enabling you to explore what it is that you do when you "think positively," "stay calm," and "keep control." You have your own unique ways of accessing and using these kinds of resources, no matter how infrequently or how briefly you may have used them in the past. Once you understand the elements of your personal "program" you can run that program when you choose. So it is Important to know how you do what you do [1; 2; 3].

## 2. NLP Guiding Presupposition

Founded on the modern sciences of biology, linguistics, and information, NLP begins with new assumptions of how the mind/brain works. These assumptions are called the NLP Presuppositions. If we could summaries all the NLP Presuppositions in one phrase, it would-be: PEOPLE WORK PERFECTLY. Our specific thoughts, actions, and feelings consistently produce specific results. We may be happy or unhappy with these results, but if we repeat the same thoughts, actions, and

feelings, we'll get the same results. The process works perfectly. If we want to change our results, then we need to change the thoughts, actions, and feelings that go into producing them. Once we understand specifically how we create and maintain our inner thoughts and feelings; it is a simple matter for us to change them to more useful ones, or if we find better ones, to teach them to others.

## NLP Presuppositions

### i) The Map is not the Territory

What we see is not the whole picture or the complete truth. Our mental maps of the world are not the world. We respond to our maps, rather than directly to the world. It is important to distinguish between several semantic levels. First there is the world. Second comes the person's experience of the world. This experience is the person's 'map' or 'model' of the world and is different for each person. Every individual creates a unique model of the world and thus lives in a somewhat different reality from everyone else. You do not operate directly on the world but on your experience of it. This experience may or may not be correct [4].

### ii) Experience has a Structure

Our thoughts and memories have a pattern to them. When we change that pattern or structure, our experience will automatically change. We can neutralize unpleasant memories and enrich memories that will serve us. Language is at a third semantic level. First is the stimulus coming from the word, second is the person's representation of experience of that stimulus, third is the person's description of that experience by way of language. Language is not experience but a representation of it. Words are merely arbitrary tokens used to represent things the person sees, hears or feels. People who speak other languages use different words to represent the same things that English speakers see, hear or feel.

People are able to communicate effectively to the degree that these meanings are similar. When they are too dissimilar, problems in communication begin to arise.

### iii) If One Person can do Something, Anyone can Learn to do it

We can model a person whom you feel perfect in his domain by studying his mental map and make it our own. If any other human being is capable of performing some behavior, then it is possible for you to perform it, too. The process of determining 'how' you do it is called 'Modeling' [1; 5].

### iv) The Mind and Body are Parts of the Same System

Our thoughts instantly affect our muscle tension, breathing, feelings, and more, and these in turn affect our thoughts. When we learn to change either one, we have learned to change the other. Mind and body are parts of the same cybernetic system and affect each other. There is no separate 'mind' and no separate 'body'. Both words refer to aspects of the same 'whole' or 'gestalt', they act as one and they influence each other in such a way that there is no separation. This means that the way a person thinks affects how they feel and that the condition of their physical body affects how they think.

### v) People already have All the Resources they need

Mental images, inner voices, sensations, and feelings are the basic building blocks of all our mental and physical resources. We can use them to build up any thought, feeling, or skill we want, and then place them in our lives where we want or need them most. People have all they need to make

changes they want to make. The task is to locate or access those resources and to make them available in the appropriate context. NLP provides techniques to accomplish this task. What this means in practice is that people need not to spend time trying to gain insight into their problems or in developing resources to deal with their problems. They already have all the resources to deal with their problems they simply need to access these resources and transfer them to the current time frame [1; 2; 10].

**vi) You cannot NOT Communicate**

We are always communicating, at least non-verbally, and words are often the least important part. A sigh, a smile, and a look are all communications. Even our thoughts are in communication with ourselves and they talk to others through our eyes, voice tones, postures and body movements.

**vii) The Meaning of Communication is the Response You Get**

When someone hears something different from what we meant, it's a chance for us to notice that communication means what is received. Noticing how our communication is received allows us to adjust it, so that next time it can be clearer. In communication it is usually assumed that you are transferring information to another person. You have information that 'means' something to the other person and you intend for the other person to understand what it is you intend to communicate. Frequently a person assumes that if they 'say what they mean to say'; their responsibility for the communication is over. Effective communicators realize that their responsibility doesn't end when they finish talking. They realize that, for practical purposes, what they communicate is what the other person thinks they say and not what they intend to say. Often the two are quite different.

In communication it is important what the other person thinks you say and how they respond. This requires that the person pays attention to the response they are getting. It is said**' Actions speak louder than words,'** and in NLP people are trained that when the two are in conflict, the person should pay more attention to the actions [10; 11].

**viii) Underlying Every Behavior is a Positive Intention**

Every hurtful, harmful, and even thoughtless behavior had a positive purpose in its original situation. Yelling in order to be acknowledged, hitting to fend off danger, hiding to feel safe. Rather than condemning these actions, we can separate them from the person's positive intent so that new, updated and more positive choices can be explored that meet the same intent [13].

**ix) People are always making the Best Choices Available to them**

Every one of us has his/her own unique personal history. Within it, we learned what to do and how to do it, what to want and how to want it, what to value and how to value it, what to learn and how to learn If what you are doing isn't working, do something else. Do anything else if you always do what you've always done, you'll always get what you've always got. If you want something new, do something new, especially when there are so many alternatives. There is no failure; there is only feedback. Successful people look at mistakes as outcomes or results, not as failure. Unsuccessful people look at mistakes as permanent and personal [15].

## 3. NLP Principles

NLP consists of a set of powerful techniques for rapid and effective behavioral modification, and an operational philosophy to guide their use. It is based on four operational principles,

1) Know what outcome you want to achieve
2) Have sufficient sensory understanding to know if you are moving towards or away from your outcome
3) Have sufficient flexibility of behavior so that you can vary your behavior until you get your outcome
4) Take action now

## 4. Analysis of NLP as a Training Technique

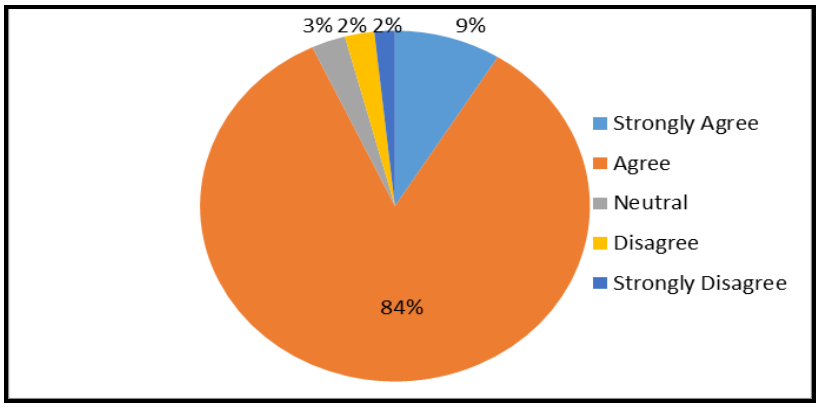
After doing a detailed literature survey of NLP studying many books undergoing NLP Practitioner certificate from two leading trainers I formed a questionnaire which is used as a basic tool to study the impact of NLP on people's life. I made some assumptions which are my hypothesis and collected the responses against them. The data collected is from various sources, leading trainers and institutes in the field of NLP training. The response of various participants have been captured and analyzed individually against various questions of questionnaire.

## 5. Graphical Evaluation of NLP Feedback

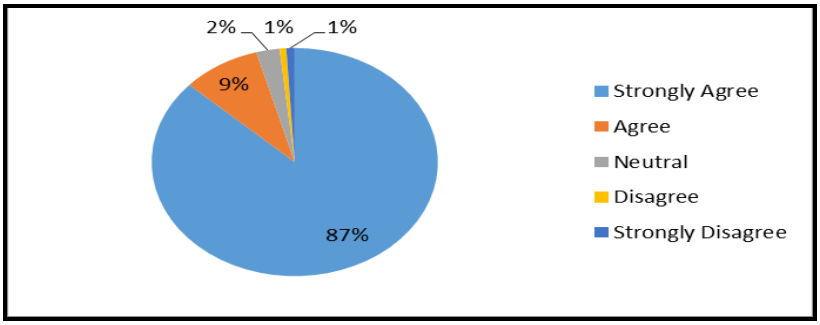
### 5.1. Responses of the Research Questionnaire Collected from Various Participants across India and a Few Abroad

| (5) | (4) | (3) | (2) | (1) |
|---|---|---|---|---|
| Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |

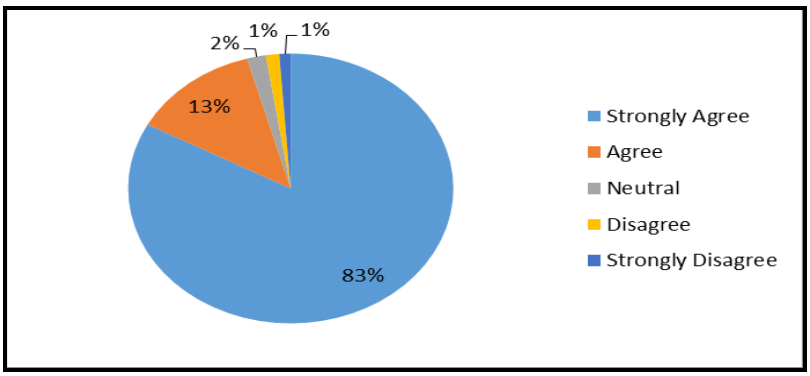
**A-1 NLP can be used in Managing Thoughts, Moods and Behavior and for Overcoming Depression.**



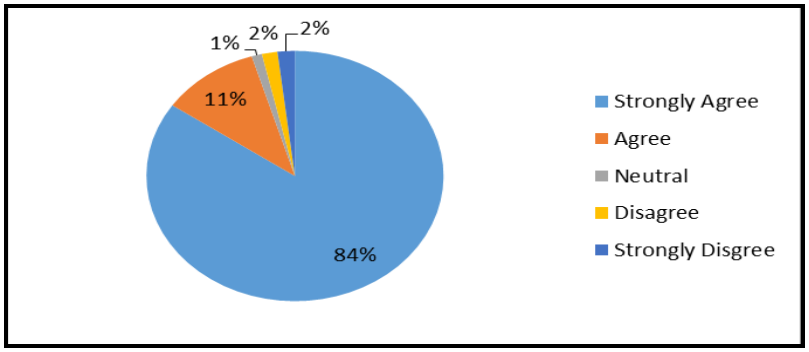

**A-2 NLP can Change Perception and can Broaden Thinking Horizon.**



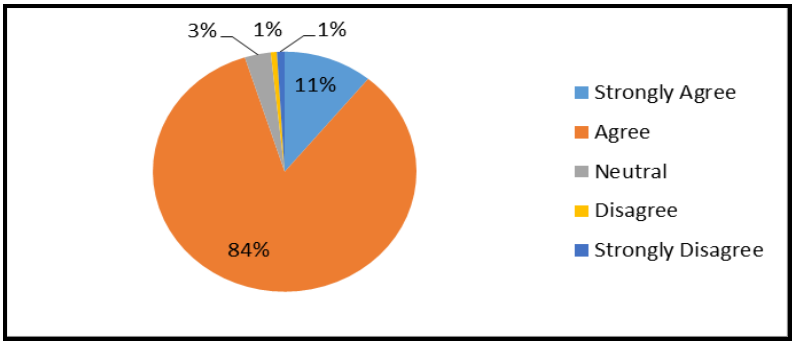
**A-3 NLP has an impact in goal setting and defining life purpose.**



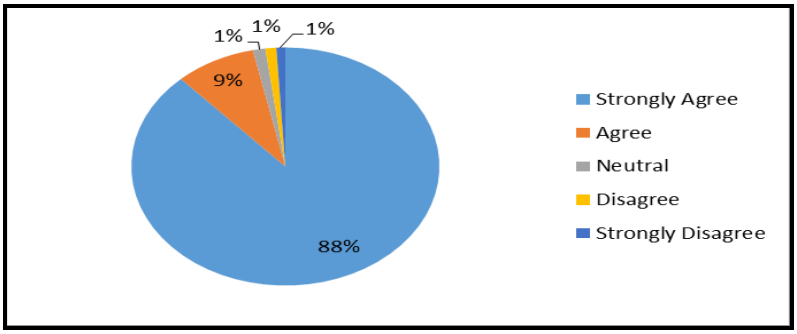

**A-4 NLP is a tool for positive transformation and Rapport building.**



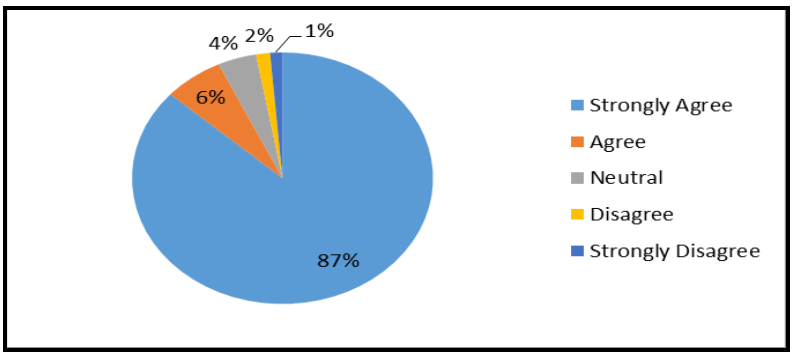

**A-5 NLP May Help in Decision Making and Conflict Management.**



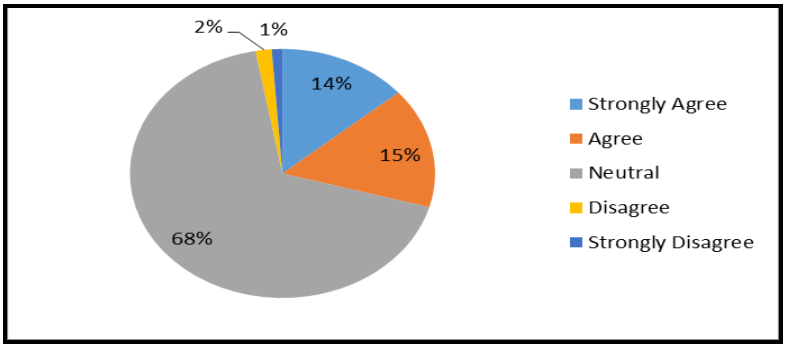

**A-6 NLP Statement 'Words can Change Minds' is true.**



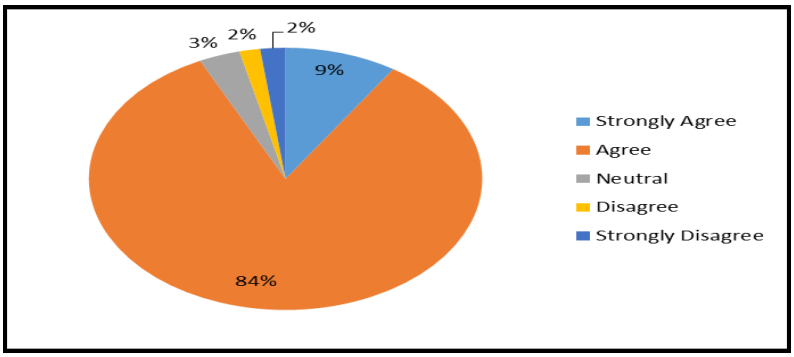
**A-7 NLP can Increase Efficiency of Individual and Organization.**



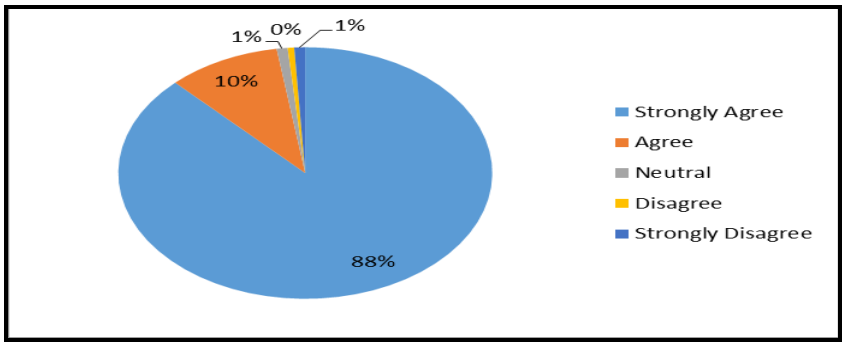

**A-8 NLP Education Should be given at School Level Itself.**




**A-9 Corporate Employees, Working Professional and Housewives should Undergo NLP Training.**

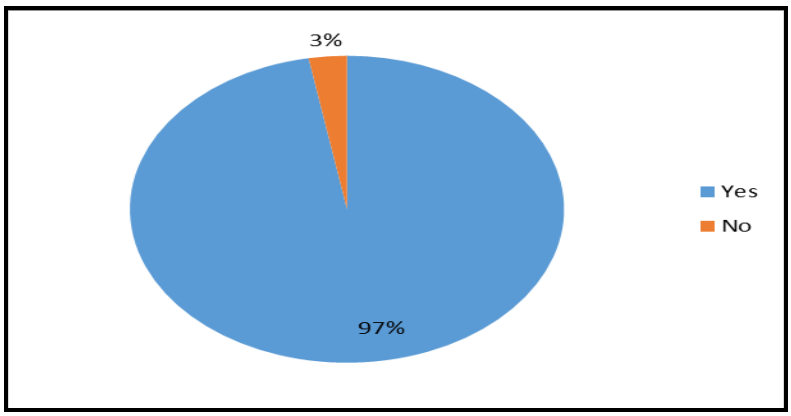



**A-10 NLP can help in Curing/Overcoming Any of Your Phobias.**

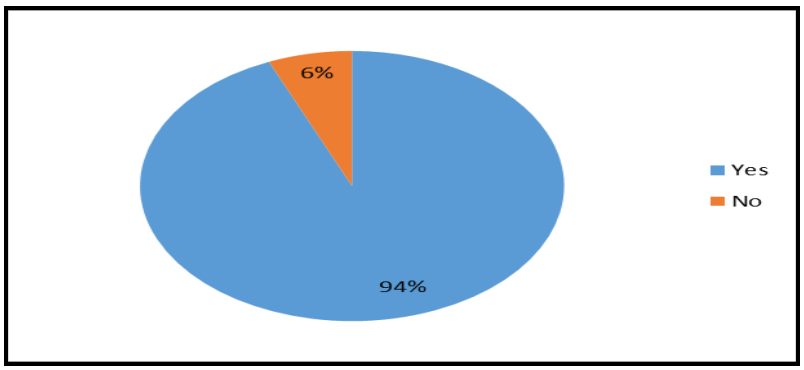


**B. Questionnaire based on Yes No Responses (1) for Yes and (0) for No.**

**B-1 Do you feel that NLP is Worth Learning?**



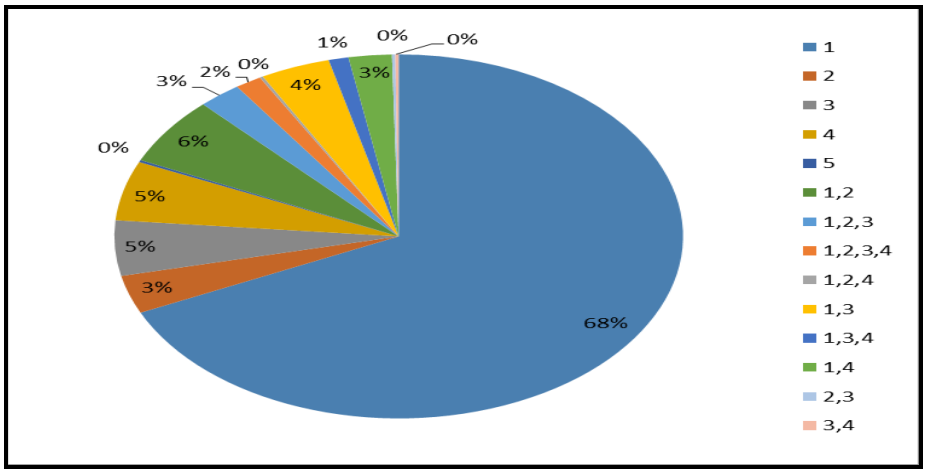

**B-2 Do you recommend this Training to Your Friends and Relatives?**




**B-3 NLP can Improve Relationship?**

(If **YES** where it can specifically be used for)

**(1)** Husband/Wife **(2)** Employer/employee **(3)** Parent/child **(4)** Teacher/Student



## 6. Summary and Conclusion

Studying the terminologies, presuppositions, principles and techniques of NLP it appears that NLP can change the way we think, react and do things. It is clearly visible from the responses that anyone who is in training, academics and the field of education should try NLP techniques in his delivery. The results which may be expected will exceed the expectations. As per the results NLP training can really act as a catalyst and as a tool for positive transformation and rapport building, increasing efficiency of an individual, managing thoughts, moods, and behavior. NLP can also be used for changing perception, broaden thinking horizon and goal setting. The analysis also gives a signal that NLP can increase efficiency of individual and organization moreover people agree that NLP education should be given at school level itself. Corporate employees, working professional and housewives should undergo NLP training to look at things with a different mindset to get different results. NLP may be used for rapport building and relationship management by couples, family, employers, employees and teachers.

NLP training techniques can be applied for increasing Sales Productivity, Positive transformation, Concentration, goal setting, removing phobias, effective communication, and mental performance. One important aspects of NLP training is to model successful people in all walks of life. Applying NLP techniques and tools, a person can become more motivated; dynamically improve work performance and boosts his/her work efficiency.

## References

[1] Anthony Robbins, 1997: *Unlimited Power: the New Science of Personal Achievement*. Free Press. 448.

[2] Richard Bandler, 1985: *Using Your Brain--For a Change*. Real People Press. 165.

[3] Richard Bandler and John Grinder, 1979: *Frogs into Princes*. Real People Press. 194.

[4] John Grinder, 1981: *Trance-Formations: Neuro-Linguistic Programming and the Structure of Hypnosis.* Real People Press. 255.

[5] Richard Bandler and John Grinder, 1983: *Reframing: Neuro linguistic Programming and the Transformation of Meaning*. Real People Press, U.S. 208.

[6] NLP Comprehensive, 1996: NLP: *The New Technology of Achievement*. Steve Andreas, Charles Faulkner (Eds.). William Morrow Paperbacks. 352.

[7] Connirae Andreas and Steve Andreas, 1989: *Heart of the Mind: Engaging Your Inner Power to Change with Neuro-Linguistic Programming*. Real People Press. 263.

[8] Richard Bandler, 1992: *Magic in Action.* Meta Publications, U.S.

[9] Richard Bandler and Will Macdonald, 1989: *Insider's Guide to Sub-Modalities*. Meta Publications. 116.

[10] Richard Bandler and John Grinder, 1975: *The Structure of Magic I: A Book about Language and Therapy.* Science and Behavior Books. 225.

[11] Richard Bandler and John Grinder, 1975: *Structure of Magic.* Vol. 2. Science and Behavior Books. 198.

[12] Joseph O'Connor, 2001: *NLP Workbook: A Practical Guide to Achieving the Results You Want*. Thorsons. 304.

[13] Harry Alder and Beryl Heather, 2000: *NLP in 21 Days: A Complete Introduction and Training Programme*. Piatkus Books. 312.

[14] Anné Linden and Kathrin Perutz, 2008: *Mind Works: An Introduction to NLP: the Secrets of Your Mind Revealed*. Crown House Publishing. 288.

[15] Patrick E. Merlevede, Denis C. Bridoux and Rudy Vandamme, 2001: *7 Steps to Emotional Intelligence: Raise Your EQ with NLP*. Crown House Publishing. 400.

[16] Jeffrey Hodges, 1999: *Sports Mind: an Athlete's Guide to Superperformance through Mental and Emotional Training*. Sportsmind Institute for Human Performance Research.

[17] Connirae Andreas, 1994: *Core Transformation: Reaching the Wellspring Within*. Real People Press. 240.

[18] Robert B. Dilts and Todd A. Epstein, 1995: *Dynamic Learning*. Meta Publications. 426.

[19] Anthony Robbins, 1992: *Awaken the Giant Within: How to Take Immediate Control of Your Mental, Emotional, Physical and Financial Destiny!* Free Press. 544.

[20] Richard Bandler, 1993: *Time for a Change*. Meta Publications. 243.

[21] Charlotte Bretto Milliner, 1994: *Leaves Before the Wind: Leading Edge Applications of NLP*. Grinder, DeLozier & Associates. 220.

[22] Joseph O'Connor and Ian McDermott, 2001: *NLP & Health: Practical Ways to Harmonize Mind and Body into Harmony*. Thorsons Publishers. 240.

[23] Robert B. Dilts and Robert McDonald, 1997: *Tools of the Spirit: Pathways to the Realization of Universal Innocence*. Meta Publications. 287.

[24] Joseph O'Connor and Robin Prior, 2000: *NLP and Relationships: Simple Strategies to Make Your Relationships Work*. Thorsons. 256.

[25] Michael Hall L. and Barbara P. Belnap, 2004: *Sourcebook of Magic: A Comprehensive Guide to the Technology of NLP*. Crown House Publishing. 383.

[26] Steve Andreas, 2002: *Transform Your Self: Becoming Who You Want to be: Becoming Who You Want to Be*. Real People Press. U.S. 273.

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2016, Volume 5, Issue 1, pp. 78-82, Article ID Tech-488
ISSN 2320 – 0235

Cloud Publications

Research Article | Open Access

# A Study of Scheduling Algorithms to Maintain Small Overflow Probability in Cellular Networks with a Single Cell

**Nagarajan B.[1], Venkatesan G.[2] and Santhosh Kumar C.[1]**

[1]Department of Computer Science and Engineering, Priyadarshini Engineering College, Vaniyambadi, Anna University, Chennai, Tamilnadu, India
[2]Department of Civil Engineering, Priyadarshini Engineering College, Vaniyambadi, Affiliated to Anna University, Chennai, Tamilnadu, India

Publication Date: 9 February 2016

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-488



**Abstract** Wireless scheduling algorithms for the download of a single cell that can maximize the asymptotic decay rate of the queue-overflow probability as the overflow threshold approaches infinity. We first derive an upper bound on the decay rate of the queue-overflow probability over all scheduling policies. Specifically, we focus on the class of "α - algorithms," the base station picks the user for service at each time that has the largest product of the transmission rate multiplied by the backlog raised to the power α. The α-algorithms arbitrarily achieve the highest decay rate of the queue-overflow probability. We design a scheduling algorithm that is both close to optimal in terms of the asymptotic decay rate of the overflow probability and to maintain small queue-overflow probabilities over queue-length ranges of practical interest.
**Keywords** *Asymptotically Optimal Algorithms; Cellular System; Large Deviations; Queue-Overflow Probability; Wireless Scheduling*

## 1. Introduction

Link scheduling is an important functionality in wireless networks due to both the shared nature of the wireless medium and the variations of the wireless channel over time. In the past, it has been demonstrated that by carefully choosing the scheduling decision based on the channel state and/or the demand of the users, the system performance can be substantially improved [2].

As per the survey, most of the scheduling algorithms focus on stable throughput to the users. Consider a cellular network with a single cell. The base-station transmits to users. There is a queue $Q_i$ associated with each user i=1,2,…N.

Due to interference, at any given time, the base-station can only serve the queue of one user (refer Figure 1 and Figure 2). Hence, this system can be modeled as a single server serving N queues.

Assume that data for user arrives at the base-station at a constant rate $\lambda_i$. Furthermore, assume a slotted model, and in each time-slot the wireless channel can be in one of states.

In each state, if the base-station picks user i to serve, the corresponding service rate is $F^i_m$. Hence, at each time-slot $Q_i$, increases by $\lambda_i$, and if it is served and the channel is at state, $Q_i$ decreases by $F^i_m$. We assume that perfect channel information is available at the base-station. In a stability problem, the goal is to find algorithms for scheduling the transmissions such that the queues are stabilized at given offered loads.

For a given $\alpha \geq 1$ if the channel is in stable state, the base-station chooses the user with the largest $(Q_i)^\alpha F^i_m$. delay-sensitive applications; it is far from sufficient [1]. In this paper, we are interested in the probability of queue overflow, which is equivalent to the delay-violation probability under certain conditions. The question that we attempt to answer is the following: Is there an optimal algorithm in the sense that, at any given offered load, the algorithm can achieve the smallest probability that any queue overflows, i.e., the smallest value of $P[\max_{1 \leq i \leq N} Q_i(T) \geq B]$. Note that if we impose a quality-of-service (QoS) constraint on each user in the form of an upper bound on the queue-overflow probability, then the above optimality condition will also imply that the algorithm can support the largest set of offered loads subject to the QoS constraint.

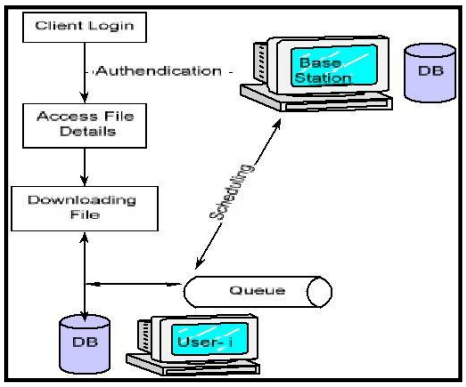



***Figure 1:*** *Service Provided Using Queues*

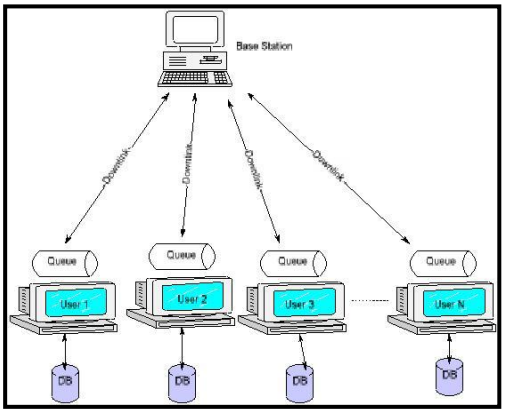



***Figure 2:*** *Dataflow Diagram*

To emphasize the dependency on α, in the sequel we will refer to this class of throughput-optimal algorithms [3] as algorithms. While stability is an important first-order metric of success, for many We use large-deviation theory and reformulate the QoS constraint in terms of the asymptotic decay rate of the queue-overflow probability as B approaches infinity. In other words we are interested in finding scheduling algorithms that can achieve the possible value of

$$\liminf_{B\to\infty} 1/B \log P\left[\max_{1\le i\le N} Q_i(0) \ge B\right]$$

Our main results are the following. We show that there exists an optimal decay rate $I_{opt}$ such that for any scheduling algorithm

$$\liminf_{B\to\infty} 1/B\log(P\left[\max_{1\le i\le N} Q_i(0) \ge B\right]) \ge -I_{opt}.$$

Furthermore, for α-algorithms

$$\liminf_{B\to\infty} 1/B\log(P^{\alpha}\left[\max_{1\le i\le N} Q_i(t) \ge B\right]) \le -I_{opt}.$$

For the above problem, it is natural to use the large-deviation theory because the overflow probability that we are interested in is typically very small. Large-deviation theory has been successfully applied to wire line networks and to wireless scheduling algorithms that only use the channel state to make the scheduling decisions.

The α-algorithms encounters a Multidimensional calculus-of-variations (CoV) problem for finding the "most probable path to overflow." The decay rate of the queue-overflow probability then corresponds to the cost of this path, which is referred to as the "minimum cost to overflow." Unfortunately, for many queue-length-based scheduling algorithms of interest, this multidimensional calculus-of-variations problem is very difficult to solve. In the literature, only some restricted cases have been solved: Either restricted problem structures are assumed (e.g., symmetric users and ON–OFF channels), or the size of the system is very small (only two users).

In this paper, we use Lyapunov function to overcome the difficulty of the multidimensional CoV problem.

The "exponential rule" can maximize the decay rate of the queue-overflow probability over all scheduling policies. The results in this paper are comparable but different. The advantage of working with the algorithms instead of the exponential rule is that the algorithms are scale-invariant (i.e., the outcome of the scheduling decision does not change if all queue lengths are multiplied by a common factor). Hence, we can use the standard sample-path large-deviation principle (LDP) instead of the refined LDP used is more technically involved.

In addition, our results highlight the role that the exponent plays in determining the asymptotic decay rate. Finally, using the insight of our main result, we design a scheduling algorithm that is both close to optimal in terms of the asymptotic decay rate of the overflow probability and empirically shown to maintain small queue-overflow probabilities over queue-length ranges of practical interest.

## 2. An Upper Bound on the Decay Rate of the Overflow Probability

We first present an upper bound $I_{opt}$ on $I_0(\lambda)$ under a given offered load λ.

This value $I_{opt}$ bounds from above the decay rate for the overflow probability of the stationary backlog process Q(t) overall scheduling policies. Then we conclude that the upper bound on the decay rate overflow rate is

$$\liminf_{B\to\infty} 1/B\log(P\left[\max_{1\le i\le N} Q_i(0) \ge B\right]) \ge -I_{opt}.$$

## 3. A Lower Bound on the Decay Rate of the Overflow

### 3.1. Probability for the α-Algorithms

To provide a lower bound that relates the decay rate of the probability to the "minimum cost to overflow" among all fluid path. For ease of exposition, instead of considering the stationary system, we consider a system that starts at time 0 (although the results can also be extended to the stationary system).

We will use the following modified queue-overflow event: {Vα(qB(t))≥ 1},

Where Vα (q) $\triangleq$ ( $\sum_{i=1}^{N} (qi)^{\alpha+1}$ ). It turns out that computing the large-deviation decay rate requires solving a CoV problem that is very difficult. The reason to use the modified overflow metric Vα ($q^B(t)$) is that the corresponding decay rate is much easier to compute and Vα($q^B(t)$) approximates the function when α is large. The function Vα (Q) is a Lyapunov function for the α-algorithm. Hence, this function may be viewed as throughput-optimal algorithm; the exponential rule is not scale-invariant.

## 4. Asymptotical Optimality of α-Algorithms

We will establish that in the limit as α→∞, the α-algorithms asymptotically achieve the largest minimum cost to overflow equal to $I_{opt.}$

To emphasize the dependence on α we use the probability distribution conditioned on Q(0)=0 under the α-algorithm.

$$\liminf_{B\to\infty} 1/B\log(P^{\alpha}\left[\max_{1\le i\le N} Q_i(t) \ge B\right] ) \le -I_{opt}.$$

As α→∞, we would expect that the α-algorithm would give more and more preference to the link with the largest queue backlog among all links with nonzero rates. If there are several links that have the same (largest) backlog, the link with the highest rate among them would be served. However, we caution that if we choose α=∞, then the resulting algorithm is the max-queue algorithm, which is not throughput-optimal for general channel models. Therefore, the above intuition does not directly lead to a stable scheduling policy.

## 5. Conclusion

In this paper, we study wireless scheduling algorithms for the downlink of a single cell that can maximize the asymptotic decay rate of the queue-overflow probability as the overflow Specifically, we focus on the class of "α -algorithms," the base station picks the user for service at each time that has the largest product of the transmission rate multiplied by the backlog raised to the power α. A key step in proving this result is to use a Lyapunov function to derive a simple lower bound for the minimum cost to overflow under "α-algorithms". This technique, overcomes the multidimensional calculus-of-variations problem. Finally, using the insight from this result, we design hybrid scheduling algorithms that are both close to optimal in terms of the asymptotic decay rate of the overflow probability and empirically shown to maintain small queue-overflow probabilities over queue-length ranges of practical interest. For future work, we plan to extend the results to more general network and channel models.

## References

[1] Venkataramanan, V.J. and Lin, X., 2007: *Structural Properties of LDP for Queue-Length Based Wireless Scheduling Algorithms.* In: Proceedings 45th Annual Allerton Conference Communications, Control, Computer, Monticello, IL.

[2] Lin, X., Shroff, N.B. and Srikant, R. *A Tutorial on Cross-Layer Optimization in Wireless Networks.* IEEE J. Sel. Areas Common. Aug. 2006. 24.

[3] Shah, D. and Wischik, D., 2006: *Optimal Scheduling Algorithms for Input-Queued Switches.* In: Proceedings IEEE INFOCOM, Barcelona, Spain.

[4] Kelly, F.P., 1991: *Effective Bandwidth at Multiclass Queues.* Queueing Systems.

[5] Shakkottai, S: *Effective Capacity and QoS for Wireless Scheduling.* IEEE Trans. Apr 2008. 53 (3) 749-761.

[6] Whitt, W. *Tail Probabilities with Statistical Multiplexing and Effective Bandwidth for Multi-Class Queues.* Telecommun. Syst. 1993. 2; 71-107.

[7] Wu, D. and Negi, R. Effective Capacity: A Wireless Link Model for Support of Quality of Service. IEEE Trans. Wireless Commun. 2003. 2 (4) 630-643.

[8] Eryilmaz, A. and Srikant, R. *Scheduling With QoS Constraints over Rayleigh Fading Channels.* In: Proceedings IEEE Conference Decision Control. Dec. 2004. 4; 3447-3452.

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2016, Volume 5, Issue 1, pp. 83-100, Article ID Tech-646
ISSN 2320 – 0235

Research Article | Open Access

# Analysis of Different Methods for Measuring the Performance of Database on Cloud Environment

**Akrati Sharma and Sanjiv Sharma**

Department of CSE/IT, MITS, Gwalior, M.P., India

Publication Date: 22 July 2016

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-646



**Abstract** Cloud computing become most adoptable technology over the past few years, it is widespread for both at organizational level or for the person who use the services that are offered in the cloud. There are several technocrats currently researched on cloud related issues and soon cloud represents the modern computing. The cloud gave the prospect for the enterprise and allowing them to center on their work by providing hardware and software solution without developing them own. Now a day the database has also moved to cloud computing so we will look into the fine points of database as a service and it's servicing. While storing data on cloud there is a need to balance the load on datacenters because if user base always sends request on single data center then it becomes overloaded so load balancing techniques are applied to manage this problem. To manage geographic distribution in terms of computing servers and data workloads a tool termed as CloudAnalyst is used which is based on cloudsim technique. CloudAnalyst helps developers with the vision of distributing applications among cloud infrastructures. Currently tool having three algorithms for load balancing round robin, throttled load balancer, equally spread current execution and the proposed algorithm is weighted round robin which works better as comparison to round robin in various aspects.

**Keywords** *Data Center; User Base; CloudSim; CloudAnalyst; Load Balancing; Round Robin; Throttled Load Balancer; Equally Spread Current Execution; Weighted Round Robin*

## 1. Introduction

Cloud computing is a field which brings a boom in the industry of technology and academics. The dependency on cloud in both the areas increases day by day. The main reasons for this popularity are the unique features and services provided by the cloud. It offers distributed services, usage of virtualized resources, sustain full realization of computing as a utility in the future [1]. With the popularity of the cloud technology, several new potentials for internet based applications become cynosure. The application models can be classified on the basis of parties who use this technology. First one is the vendors or cloud service providers who provide large scale computing infrastructure at low budget. Second one is the large-scale software systems providers, who manage large scale applications such as social networking sites and e-commerce.

These cloud services minimize costs and improve service quality to end users. With the beginning of the cloud, deployment and hosting became easy and less expensive credit goes to the functionalities of cloud like pay per usage, flexible infrastructure services, on demand self-services and many more. As per in previous era the development of such applications gaining requirement of servers with a predetermined capacity and able to handle the expected load at peak demand, installation of software infrastructure and the platform supporting the same applications. All because of this the servers were underutilized and the reason is the peak traffic occurs occasionally or at specific short time periods.

When the above two ends are taken into account, several factors generates that affect the net assistance of cloud. These factors include distribution of user bases at different geographical areas, performance of the internet infrastructure in those geographic areas, working of user bases, and capabilities of cloud services and its behavior towards dynamic reconfiguration among others. To understand such vibrant and largely distributed environments in a controlled and reproducible manner there is a need of simulation.

In Database as a service [7] a database can be accessed by the clients via internet from the cloud. Database service provider deliver database to them when they need it or want to store their data over cloud. Cloud database is designed for creating the pool of virtualized resources so that user can select the required resource and used it. The cloud database is present on cloud so that it uses the various services of cloud and utilizing the software and hardware resources of the cloud computing service provider. The cloud database holds the data on heterogeneous data centers which is located at heterogeneous locations. This is the reason which makes cloud database structure different from the normal databases, due to this its structure become complex one. There are numerous nodes across the cloud databases for query services, so that data centers that are located in different geological areas can also be accessible. This linking of nodes on datacenters is compulsory for the access of the database over the cloud. There are several methods for accessing the database over the cloud; the user can access it via computer through the internet using 3G or 4G services.

## 2. CloudSim

CloudSim is a framework developed by the GRIDS [3] laboratory of University of Melbourne. A widespread and extensible simulation framework based on java allows flawless simulation, and perform experiment on emerging cloud computing infrastructures and application services. CloudSim [2] is just like a boon for researchers and industry based developers using this they can work on specific system design issues without worrying about the low level details of cloud based infrastructures and its services.

CloudSim consist the following features:

1) Allow modeling and simulation for large scale cloud computing infrastructure, having data centers on a single node.
2) Provide platform for modeling data centers, service brokers, scheduling, and allocations policies.
3) Presence of virtualization engine, which helps in creating and managing multiple, self-employed, and co-hosted virtualized services on a data center node.
4) Flexibility to switch between spaces and time-shared allocation of processing cores to virtualized services.

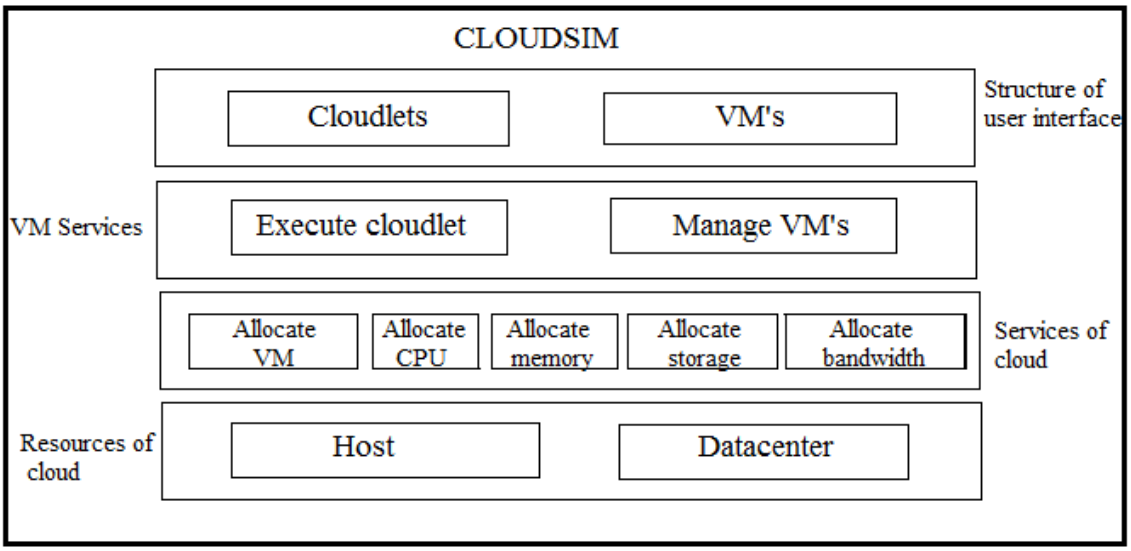



***Figure 1:*** *Components of cloudsim*

These convincing features of Cloudsim would pace the formation of new resource allocation policies and scheduling algorithms for cloud computing. CloudSim framework developed on the top of GridSim framework which is also developed by the GRIDS laboratory.

### 2.1. GridSim

GridSim [4] toolkit was developed to rectify the problem of performance evaluation related to real large scaled distributed environments in a repeatable and restricted manner. The GridSim is a Java based simulation toolkit which supports modeling and simulation of diverse grid resources. It supports multiple application models and provides some rules for creating application tasks, mapping of tasks to resources.

### 2.2. SimJava

SimJava [5] is the simulation toolkit which is incorporated in both the simulation framework CloudSim and GridSim.

## 3. CloudAnalyst

It is an easy to use tool with visualization capability. CloudAnalyst [6] separates the simulation experiment and setting up a programming exercise and allow modeler to focus on the parameters of simulation more than the procedure of programming. It allows the repetition of simulations with changes according to the parameters. Output generates graphically which is helpful in terms of analyzing the results after the simulation process. If there is any problem with the parameters of simulation like performance evaluation and accuracy of result it also rectify the same. Figure 2 consist the architecture of the simulator. Some of the features of the tool describe it more deeply:

1) It is easy to set up and execute a simulation experiment in the environment. The simulator provides an easy to use GUI which is spontaneous & inclusive.
2) The tool is easy to configurable, especially in modeling something as complex as an internet application which rely on parameters and its values. Hence there is need of rapidly changes the values of parameters according to simulation and repeat them.

3) Specialty of the tool is the representation of result in the forms of graphs, tables and charts. It is highly advantageous to summarize large amount of statistics that is collected during the simulation. It is helpful in finding the unique pattern between the output parameters and comparing them.
4) Repeatability of experiments is the striking feature of the simulator. It is important that every time when the experiment is performed it must produce same result for same parameters and different results for different ones. Otherwise the simulation becomes messy and becomes just a random sequence of events rather than a controlled experiment. There is also an option of saving the old simulation and if required in future then loaded back from the directory.
5) It is realistic simulation framework incorporated with the set of input parameters can be achieved in a few attempts. There is ease of extensions in terms of parameters on the simulator, the parameters can easily be increased or decreased according to the requirement of the simulation. Hence the simulator architecture supports extensions with minimum efforts.

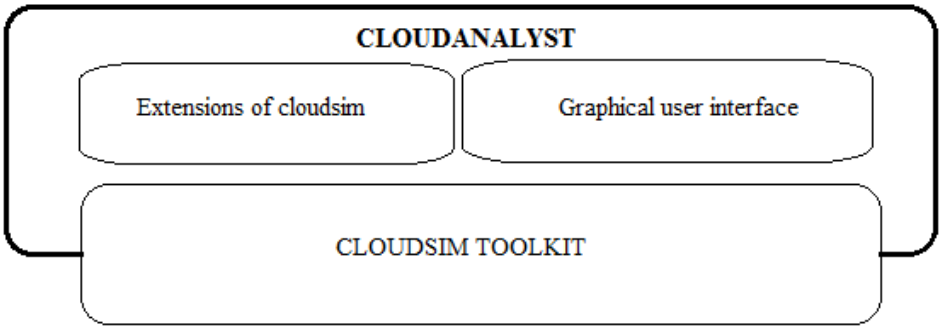



***Figure 2:*** *CloudAnalyst architecture*

### 3.1. Simulation Output of the Simulator

When experiments are performed on the simulator the generated results can be calculated with following parameters:

1) Response time of the simulation, it refers to the amount of time server takes to return the results of a request to the user. It affects by the factors like network bandwidth, number of users, number and type of requests submitted, and calculation time. Average, maximum and minimum response time is calculated
2) Response time can be calculated on the basis of regions present across all over the world and the overall effect of that usage on the data centers hosting the application.
3) Data center servicing time is calculated, it is the taken by the server to fulfill the request of the user.
4) Data center processing time is calculated of the overall simulation.
5) Cost of the simulation is calculated.
6) Time to transfer data is also taken into account.

CloudAnalyst is purely java based tool and on Java platform it using Java SE 1.6. It is designed on JavaSwing the GUI of the simulator using Swing components.

### 3.2. Load Balancing

As described in the figure that there are several datacenters (DC) and user bases (UB) are located across the world UB's are requesting for storing their data on the DC's. Now the question is arises

that on which data center the requirements of users are fulfilled. Here some conditions are occurred which is undesirable:

1) If user always sends data to a data center which is filled with request and still receiving much requests then the problem of overloading occurred due to which data centers crashed.
2) If requests always arrived on single data center then other data centers remains idle.

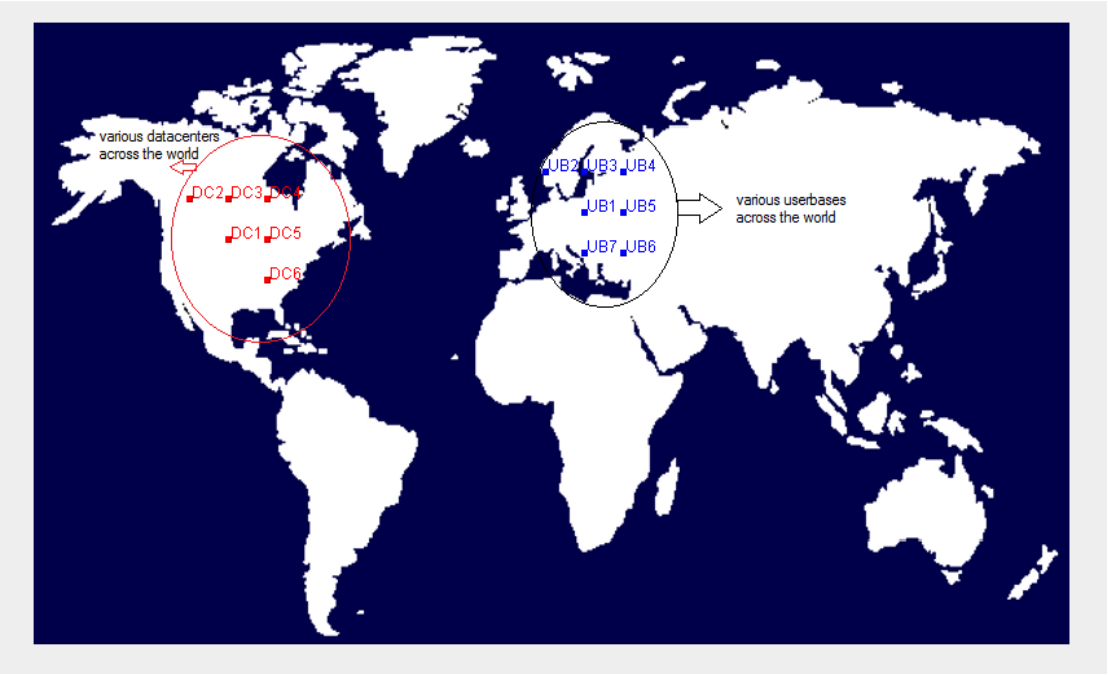



***Figure 3:*** *World map having several data centers & user bases*

To solve such problems the concept of load balancing is used. Load Balancing is a method to distribute workload on the multiple data centers or a computer cluster through network links to achieve optimal resource utilization for increasing throughput and lower down the response time. Load Balancing is used for avoiding too much overload on the resources and dividing the traffic between different data centers. Data can be sent and received without maximum delay. Load Balancing is used for lower down the total waiting time of the resources. In cloud computing load balancing are uses for maintaining the load on virtual machine and cloud resources. To perform the task of load balancing on cloud data centers a simulation environment is required that is CloudAnalyst simulator. The tool is java based and based on cloudsim.

## 4. Backgrounds & Related Work

Sivashakthi, T., Dr. Prabakaran N., [8] in 2010 gives various storage techniques for storing data in cloud. Cloud storage is regarded as a system of distributed data centers that generally utilizes virtualization technology and supplies interface for data storage. The paper includes discussion on: Implicit storage security to data in online, Public auditing with complete data dynamic support, efficient third party auditing (TPA), Way of dynamically store data in cloud, Effective and secure storage protocol. These points are described in details.

Nusrat Pasha, Dr. Amit Agarwal, Dr. Ravi Rastogi [9] in 2014 explains the working of round robin algorithm. It is the scheduling technique that uses the concept of time slices. The time is divided into multiple time slices and each node is given a specific time slice which uses the principle of time

scheduling. The resources provided to the requesting client on the basis of time slice by the of the service provider. Round robin algorithm also is incorporated in cloud databases for performing the task of load balancing on different data centers of cloud. The Round Robin algorithm does not save the state of previous allocation of a VM to a request from a given user base while the same state is saved in RR VM load balancer. The Round Robin VM Load balancer maintains two data structure. Hash Map- in which it stores the entry for the last VM allocated to a request from a given user base. VM State List- this stores the allocation status (i.e. busy available) of each VM.

Waleed Al. Shehri [10] in 2013 gives a brief about DBaaS means database-as-a-service. This is a storage technique for storing databases on cloud. A database can be accessed by the users through internet and they can use it according to their requirement. Cloud database is designed for virtualized computing environment. The cloud database is incorporated with the help of cloud computing that means using the software and hardware resources of the cloud service provider. The cloud database will become the mostly used technology for storing huge data worldwide. It is not like taking the relational database and deploys it over a cloud server. It means that adding of extra nodes according to user requirement, and maximizes database performance. It is required to distribute the data over different data centers. The database must be available 24x7 so that the user can get the data whenever he needs. The cloud database must be easily manageable and it should be less costly too. Cloud computing is helpful in recovering the information after a disaster like crashing of nodes in the database.

Gill Sukhjinder Singh, Thapar Vivek [11] in 2015 gives a brief about the load balancing and its need on cloud environment. Load Balancing is a procedure to distribute or share the load equally among all the nodes (in this case we considered it as datacenters in place of nodes) of the network. It helps the congested and under loaded nodes like if any node is having more loads (congested node) than the threshold value, then its load is transferred to the node with less loads. Thus load balancing is the best choice for performing this operation because it is a major challenge for cloud computing. Several time it may inevitable and not affordable, if any of the servers become idle in a datacenter while others are overloaded or congested in response to user demands. It means jobs require the proper assignment of servers in a datacenter and results is the higher maintenance cost of idle servers. Therefore appropriate load balancing techniques need to be applied for extra cost effective in the cloud environment.

Bhathiya Wickremasinghe [12] in 2009 presented a tool termed as CloudAnalyst used for analyzing cloud environment and it is completely based on the cloudsim technology. CloudAnalyst is a trouble-free tool with a level of visualization capability is even better than just a toolkit because it visualizes the whole world map and shows the geographic locations of data centers and user bases over there. Such a tool separates the simulation experiment set for programming exercise and enables a modeler to give attention on the simulation parameters rather than the technicalities of programming. It allows performing the experimentation process repeatedly with some small modifications to the parameters rapidly and easily. The result generated in graphical form so that result analysis becomes easier and more efficient and it enlightened the problems with the performance and accuracy of the simulation logic.

## 5. Existing Algorithms Work on Simulator

There are some algorithms which work on CloudAnalyst tool to perform load balancing. Figure 4 shows the options of such algorithms in the tool and its description are as follows:-

### 1) Round robin policy

It is one of the simplest scheduling techniques [13] that utilize the principle of time slices. Here the time is allocated in the form of slots and hand over it to the each node; it is the concept of time scheduling. Each node is given a time quantum and its operation, the resources or virtual machines are provided to the requesting client on the basis of time slice by the cloud service providers.

### 2) Throttled load balancer policy

This algorithm assures that pre- defined numbers of cloudlets are allocated to a single virtual machine at a time instant. If the number of users requests are more than that of the present number of available virtual machines at data centre. Than incoming request are arranged in the queue basis until the next virtual machines becomes available.

### 3) Equally spread current execution load policy

The jobs are submitted by the clients to the computing system. As the submitted jobs arrive to the cloud they are queued in the stack. The cloud manager estimates the job size and checks for the availability of the virtual machine and also the capacity of the virtual machine. Once the job size and the available resource (virtual machine) size match, the job scheduler immediately allocates the identified resource to the job in queue. Unlike the round robin scheduling algorithm, there is no overhead of fixing the time slots to schedule the jobs in a periodic way. The impact of the ESCE algorithm is that there is an improvement in response time and the processing time. The jobs are equally spread, the complete computing system is load balanced and no virtual machines are underutilized. Due to this advantage, there is reduce in the virtual machine cost and the data transfer cost.

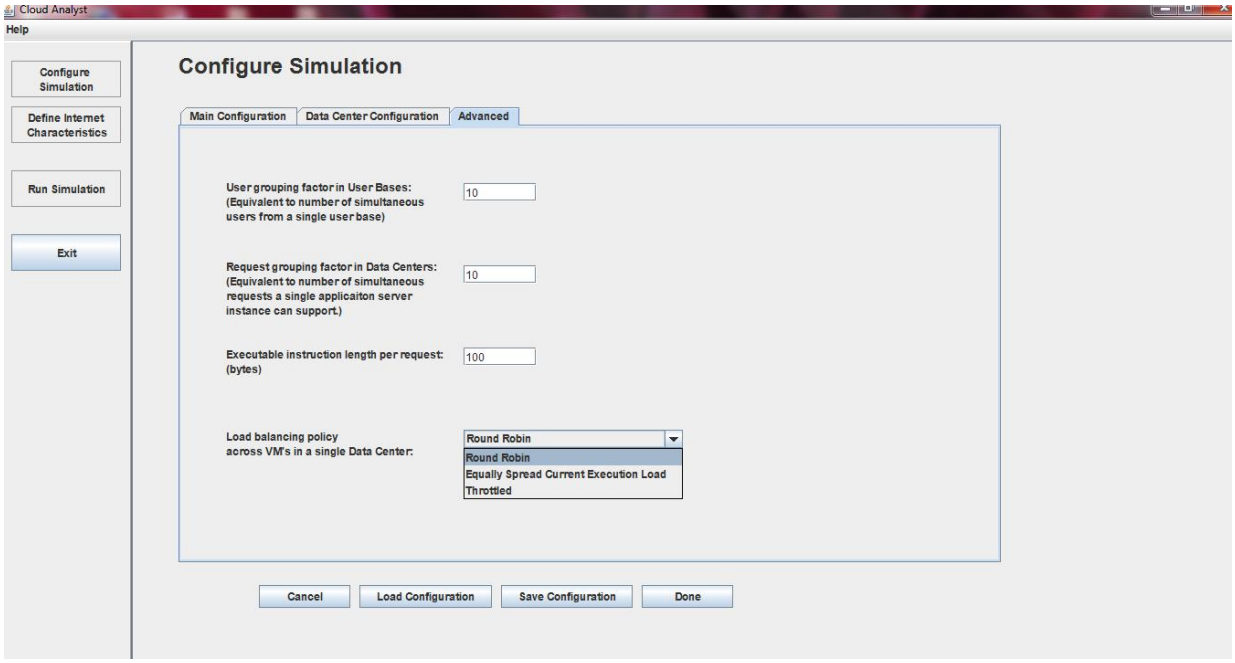



***Figure 4:*** *CloudAnalyst screen shows existing load balancing algorithm*

### 5.1. Proposed Algorithm for Performing Load Balancing

For performing load balancing besides these algorithms one more algorithm is used which is the enhanced version of round robin algorithm that is the weighted round robin algorithm. Weighted round robin perform better load balancing as compare to round robin policy. Figure 5 shows the incorporated option of weighted round robin algorithm in the tool. In round robin policy the virtual machines (VM) are allocated to the data centers for particular time slice. If there are total 5 data centers then 2ns (approx.) time slice is allocated to every data center. It means that every data center uses VM for 2ns; it doesn't matters that whether any data center is needy for VM. This problem is solved in weighted round robin algorithm, in weighted round robin algorithm a weight is assigned to every data center; more weight shows more requirement of VM. The data center having more weight the VM first allocate to that data center.

In terms of load sharing we can say that suppose there are 5 data centers and user want to store its data on data center then using weighted round robin policy a weight is assigned to each data center. Weight is decided on the basis of request arrives on the data center, like if a data center DC1 filled with the request and it does not have enough capacity to handle more request then a weight assigned to DC1 is less and another data center DC2 having enough space to handle request than its weight is more as compare to DC1 hence there are more chances that next request arrives on DC2 due to its weight. It decreases the chances of overloading and crashing of data centers

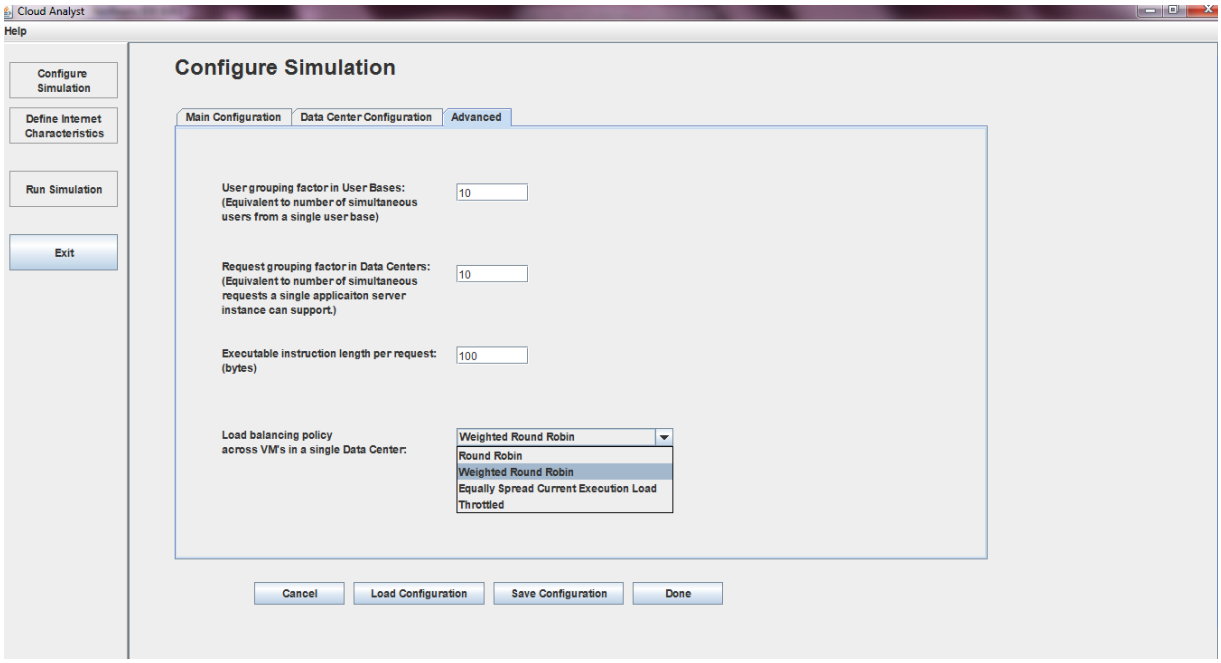



***Figure 5:*** *CloudAnalyst screen shows proposed load balancing algorithm*

## 6. Result Analysis

There are several measures on the basis of which it is proved that the outcome generated through weighted round robin policy is better than that of round robin policy. Load balancing task can be performed in a better way via using weighted round robin algorithm.

### 6.1. Response Time

Response time refers to the amount of time server takes to return the results of a request to the user. It affects by the factors like network bandwidth, number of users, number and type of requests submitted, and calculation time.

$$\text{Tresponse} = ((n/r - T_{calculation}) /1000) \text{ ms} \ldots\ldots\ldots (1)$$

n: number of concurrent users
r: number requests/sec the server receives
$T_{calculation}$: calculation time
With the response time various service broker policies are also taken into account:

The traffic routing between user bases and data centers is controlled by a service broker that decides which data center should examine the requests from each user base. The CloudAnalyst uses three types of service brokers which help in implementing the different routing policies.

### 6.2. Closest Data Center Policy

In this case one has to search quickest path to the data center from a user base according to network latency. The service broker will have to search the data center for the user which is at the least distance from particular user base and route user traffic to the closest data center according to transmission latency. Figure 6 shows the calculation of response time using closest data center policy in round robin algorithm whereas Figure 9 shows the same with weighted round robin policy which generates better results.

### 6.3. Optimized Response Time Policy

In this policy the service broker dynamically monitors the performance of all data centers and manages the traffic to the data center. It estimates to give the best response time to the user at the time when user quires. Figure 7 shows the calculation of response time using optimal response time policy in round robin algorithm whereas Figure 10 shows the same with weighted round robin policy which generates better results.

### 6.4. Reconfiguring Dynamically with Load Policy

This is an extended version of proximity based routing. The service broker is having additional responsibility of scale up the deployment of applications based on the load it is suffering from. This problem is solved by increasing or decreasing the number of virtual machines allocated in the data center. Figure 8 shows the calculation of response time using reconfigure dynamically with load policy in round robin algorithm whereas Figure 11 shows the same with weighted round robin policy which generates better results.

On the basis of this the results shown are as follows:

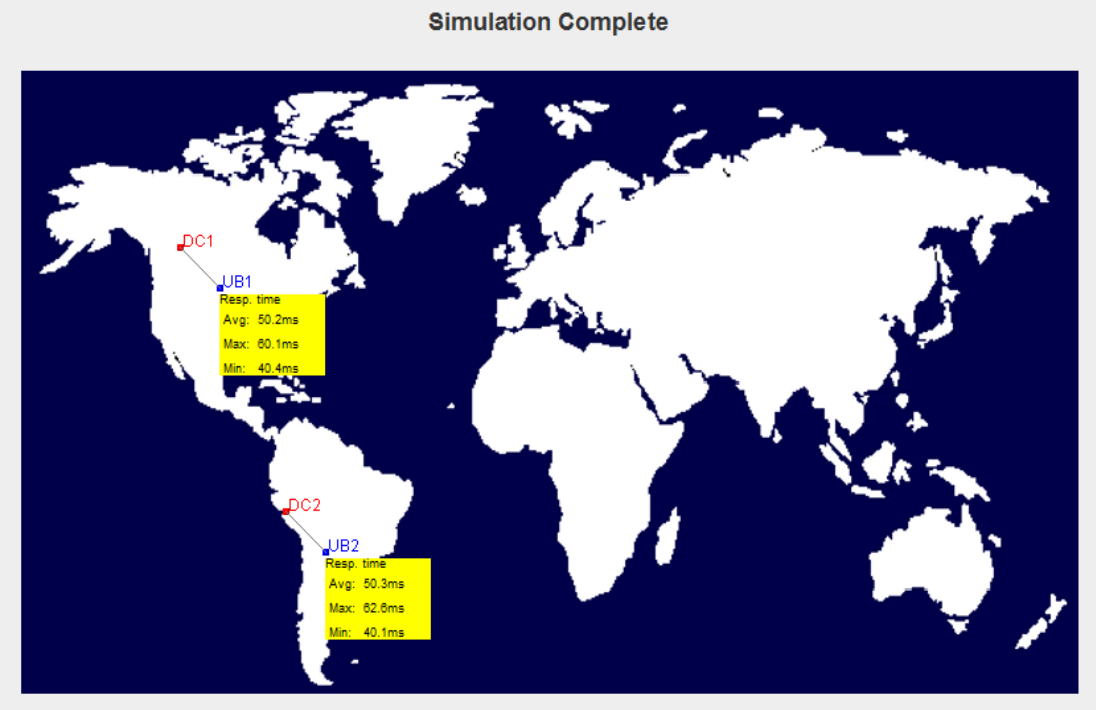



***Figure 6:*** *Calculation of response time using closest data center policy via round robin algorithm*

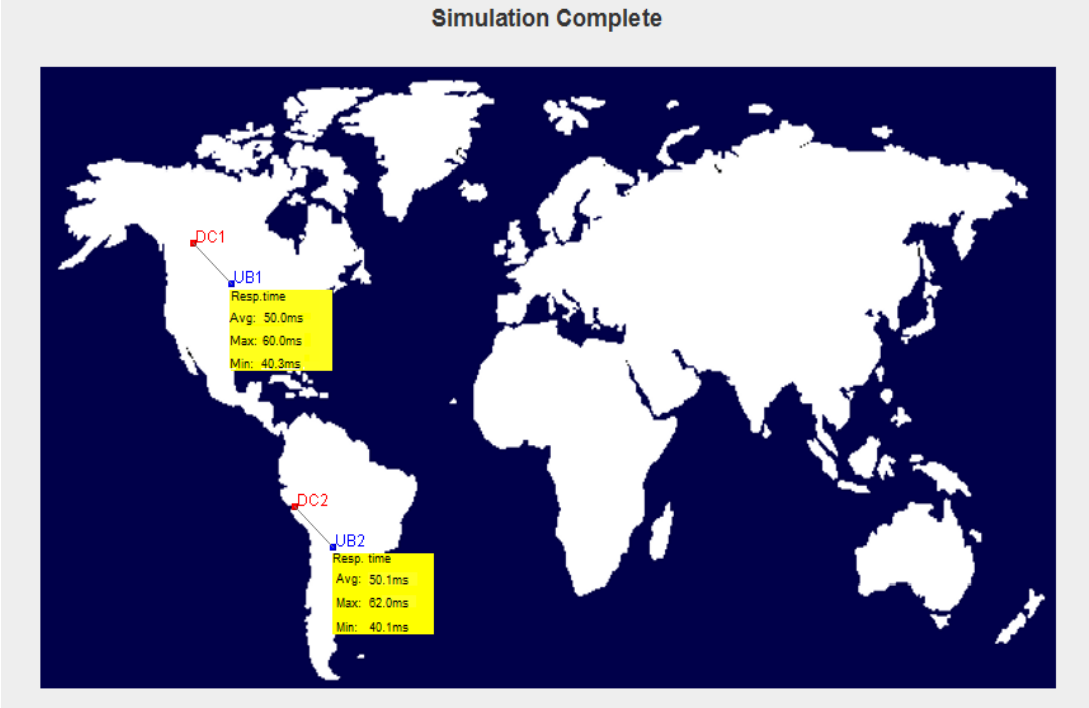



***Figure 7:*** *Calculation of response time using optimal response time policy via round robin algorithm*

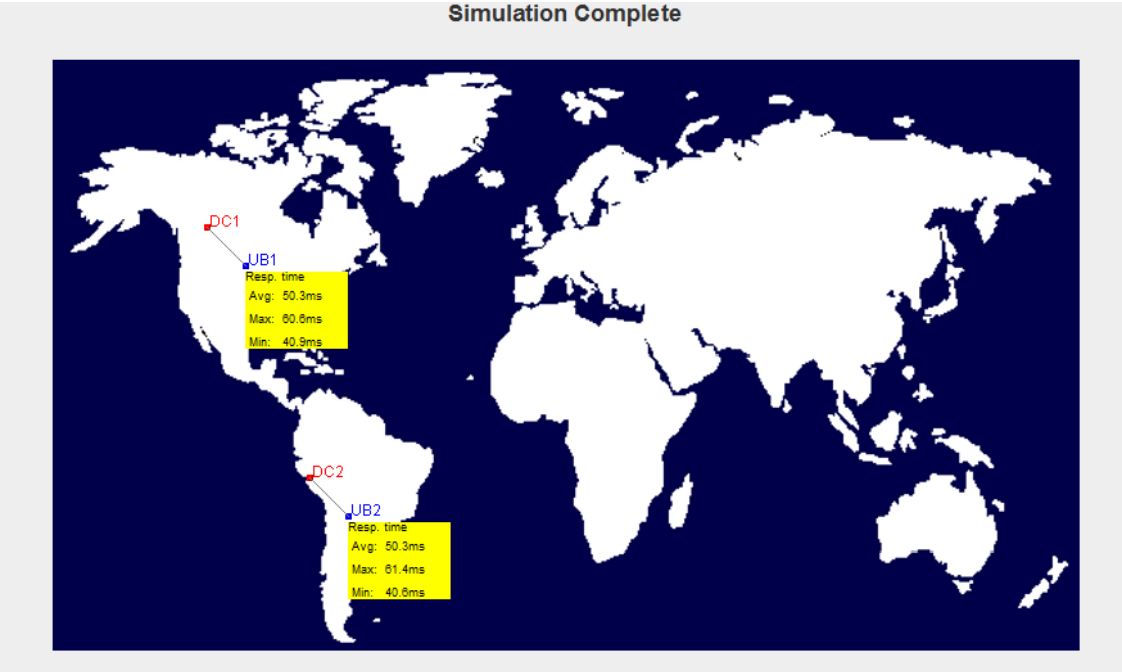



***Figure 8:*** *Calculation of response time using reconfigure dynamically with load time policy via round robin algorithm*

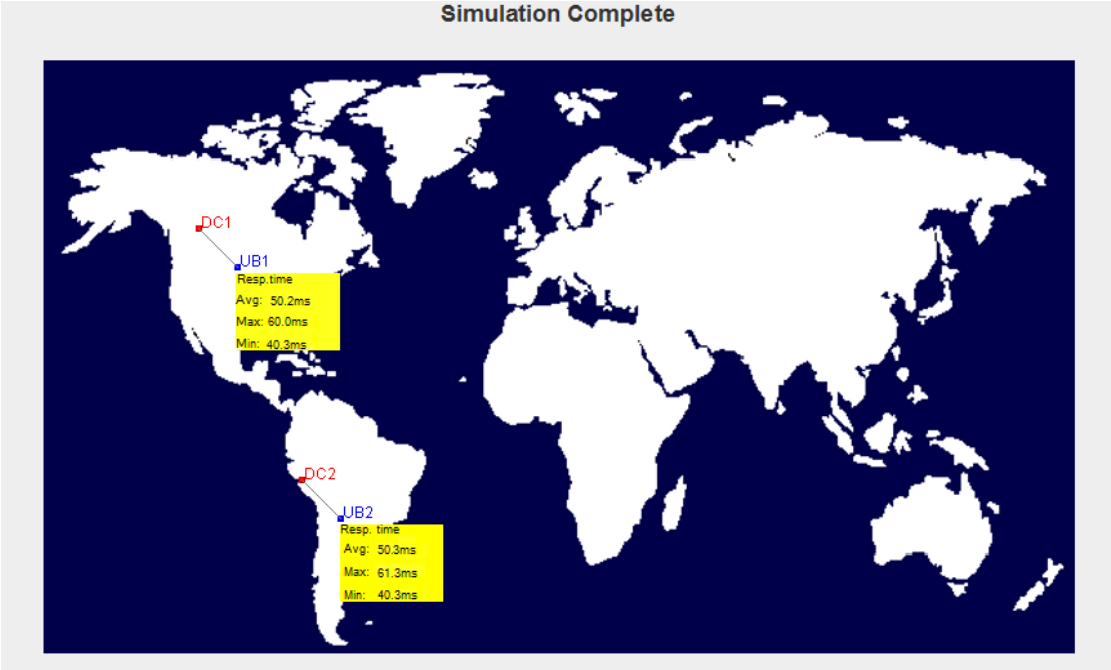



***Figure 9:*** *Calculation of response time using closest data center policy via weighted round robin algorithm*

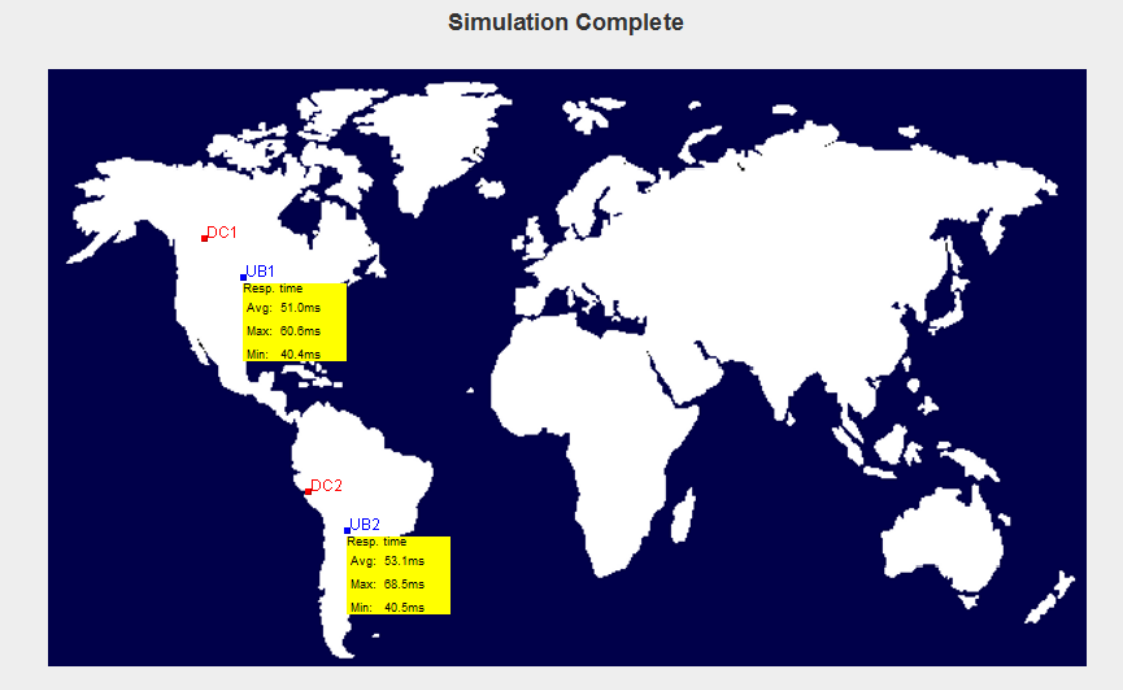



***Figure 10:*** *Calculation of response time using optimize response time policy via round robin algorithm*

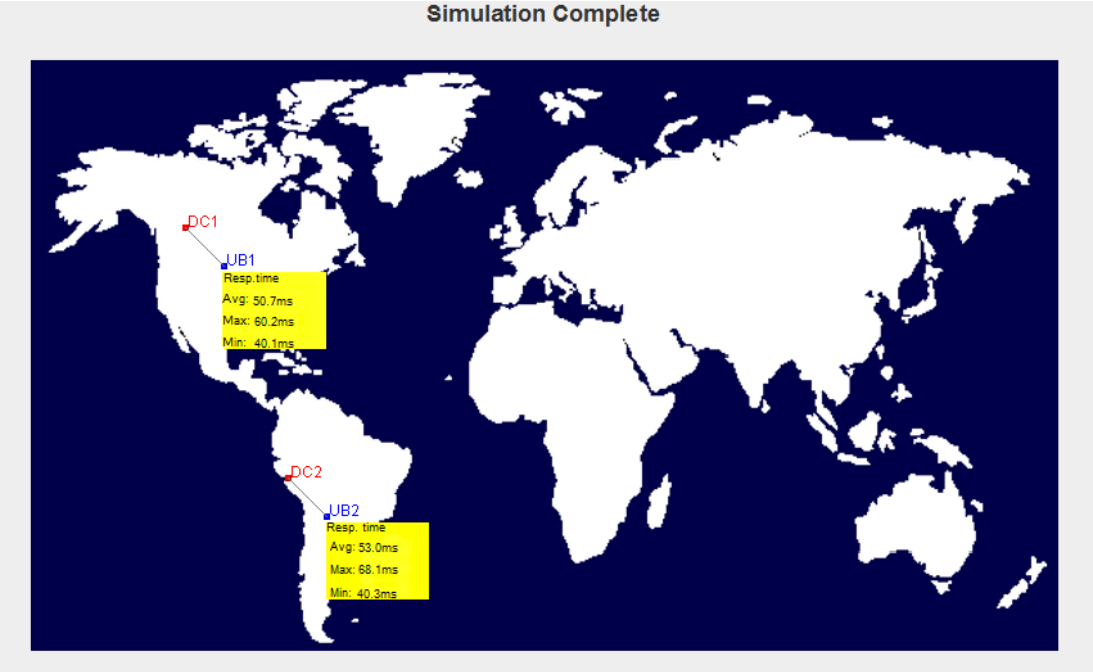



***Figure 11:*** *Calculation of response time using reconfigure dynamically with load policy via weighted round robin algorithm*

### 6.5. Response Time on the Basis of Regions

In the CloudAnalyst the world is divided in to 6 regions which consist 6 main continents in the world. The other main entities like user bases and data centers belong to following regions. This geographical consortium is used to preserve a level of realistic ease for the large scaled simulation being attempted in the CloudAnalyst. Figure 12, Figure 13, Figure 14, show the comparison between

two user bases of RR and WRR algorithm at average, maximum and minimum scale using ORT, CDC, and RDWL policies simultaneously. Approximate users according to CloudAnalyst per region.

***Table 1**: Approximate user according to CloudAnalyst per region*

| Region | CloudAnalyst region Id | Users |
|---|---|---|
| North America | 0 | 80 million |
| South America | 1 | 20 million |
| Europe | 2 | 60 million |
| Asia | 3 | 27 million |
| Africa | 4 | 5 million |
| Oceania | 5 | 8 million |

### 6.5.1. Results

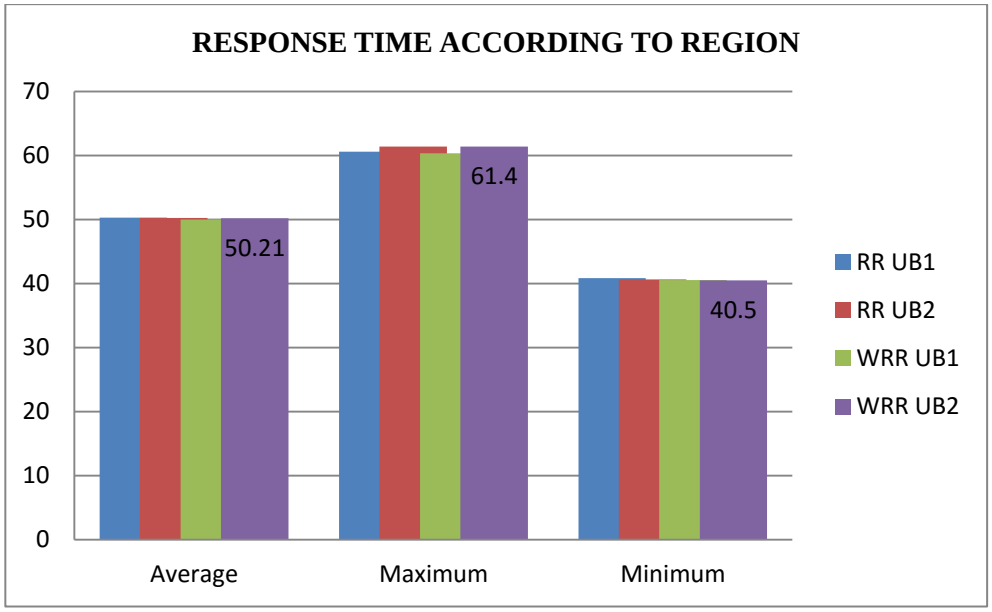



***Figure 12:** Optimise response time*

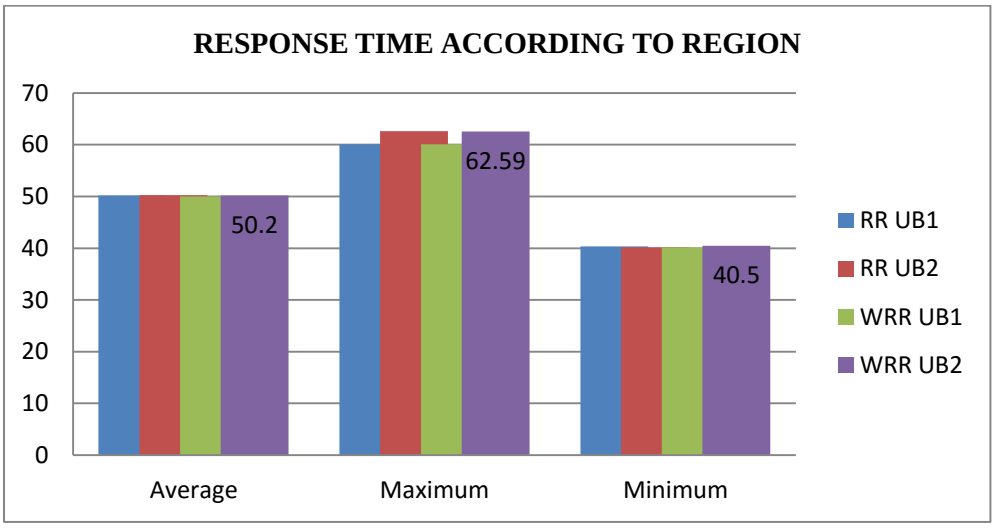



***Figure 13:** Closest data center*

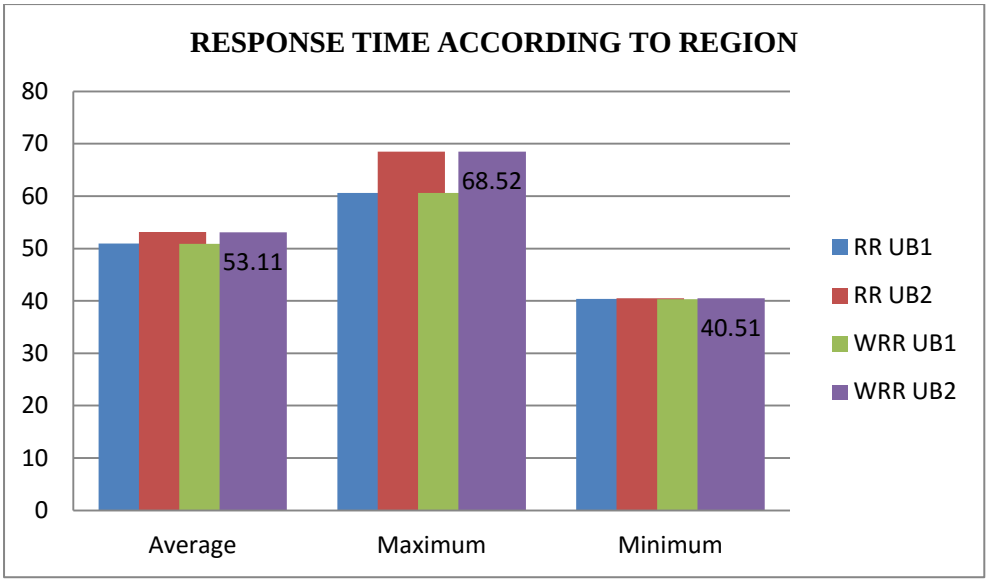



***Figure 14:*** *Reconfigure dynamically with load*

### 6.6. Data Center Processing Time

Once the requests are received at the Data Center Controller it may again sub divided the requests in a single Internet Cloudlet in to multiple sub Internet Cloudlets based on the 'DC Request Grouping Factor'. Each of these sub cloudlets are then assigned to virtual machines by the load balancer and the new request is completed only when all the sub cloudlets are processed and returned to the controller. But this total duration is the time for processing all the requests in the internet cloudlet. If the data center controller waits till this point to send back the response to the user base then the final response recorded by the user base is the total processing duration plus the transmission delay for a single request. Therefore the data center controller is designed to send back the response to the original request on the receipt of the first response sub cloudlet. Figure 15, Figure 16, Figure 17, show the data center processing time of RR and WRR policies at average, maximum or minimum scale using CDC, ORT and RDWL policies simultaneously.

$$T_{DCP} = T_P + T_{Delay} \ldots\ldots\ldots\ldots \quad (2)$$

Where $T_{DCP}$ is data transfer processing time, Tp is processing time, $T_{Delay}$ is the delay time.

$$T_{Delay} = T_{Latency} + T_{Transfer} \ldots \quad (3)$$

Where $T_{Latency}$ is the network latency and $T_{Transfer}$ is the time taken to transfer the size of data of a single request (D) from source location to destination. $T_{Latency}$ is taken from the latency matrix (after applying Poisson distribution on it for distributing it) held in the Internet Characteristics.

$$T_{Transfer} = D/B_{W(Per\ user)} \ldots\ldots\ldots (4)$$
$$B_{W(Per\ user)} = B_{W(Total)}/N_r \ldots\ldots\ldots (5)$$

Where $B_{W(Total)}$ is the total available bandwidth (held in the Internet Characteristics) and $N_r$ is the number of user requests currently in transmission. The Internet Characteristics also keeps track of the number of user requests in-flight between two regions for the value of $N_r$.

Figure shows the graphs of data center processing time with different cloud server broker policies:-

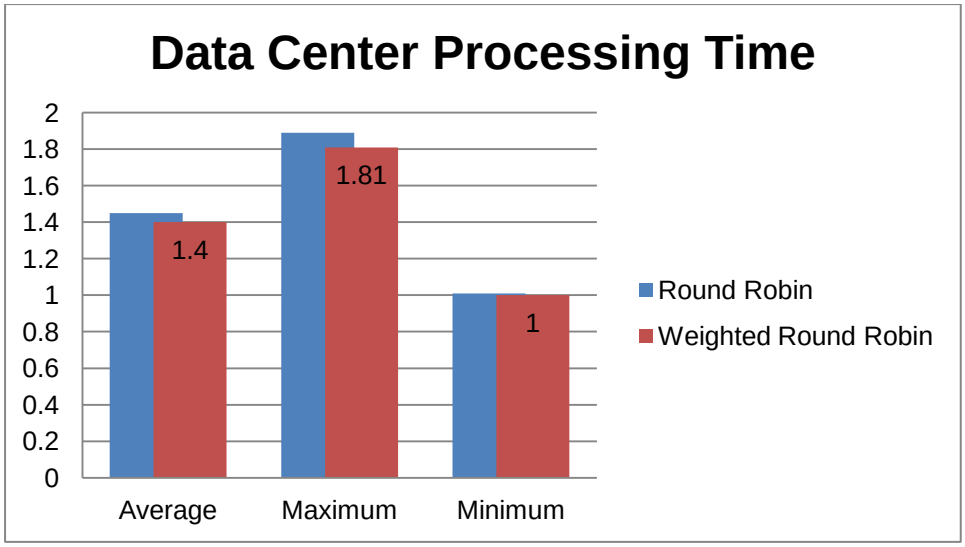



***Figure 15:*** *Closest data center technique*

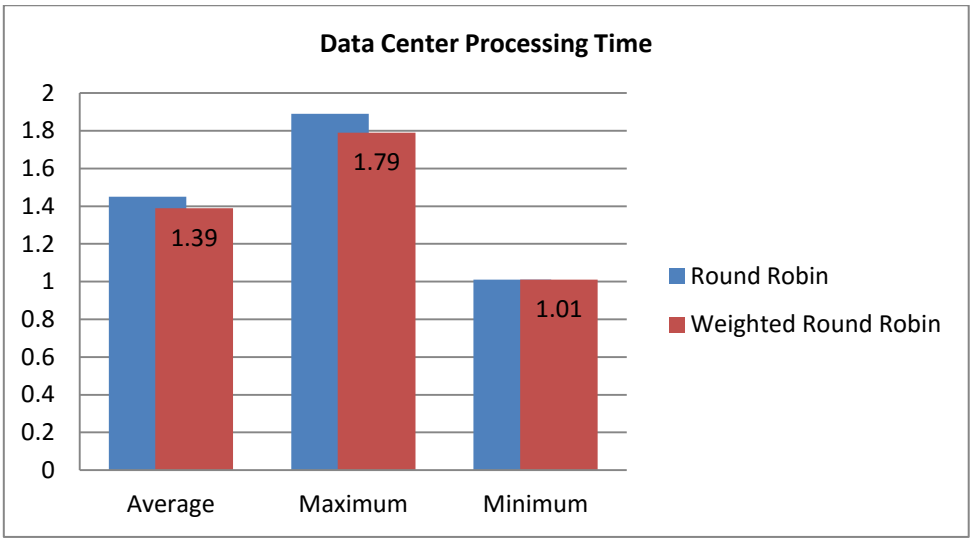



***Figure 16:*** *Optimise response time technique*

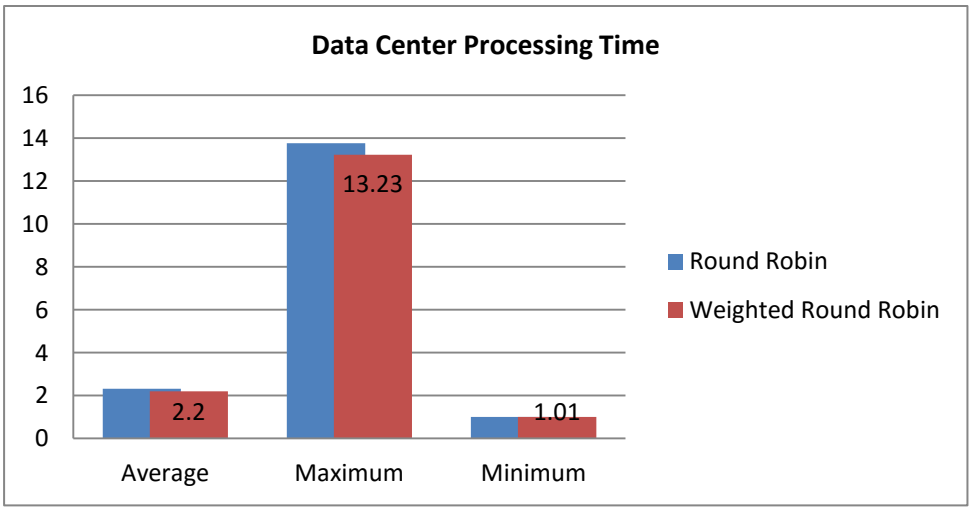



***Figure 17:*** *Reconfigure dynamically with load technique*

### 6.7. Data Center Request Servicing Time

Data center request servicing time can be defined as the time taken by the server to fulfill the request of the user. Figure 18, Figure 19, Figure 20, show the data center request servicing time of RR and WRR policies at average, maximum or minimum scale using CDC, ORT and RDWL policies simultaneously.

$S = \frac{B}{C}$.....(6)

Where S is the service request time, B is the busy time of the server and C is the completion time of the user's task.

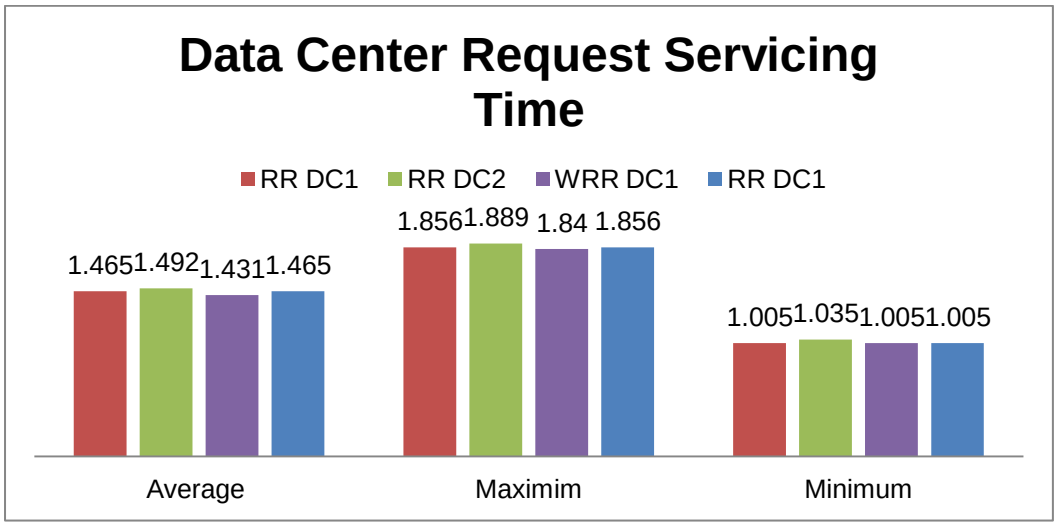



***Figure 18:*** *Closest data center*

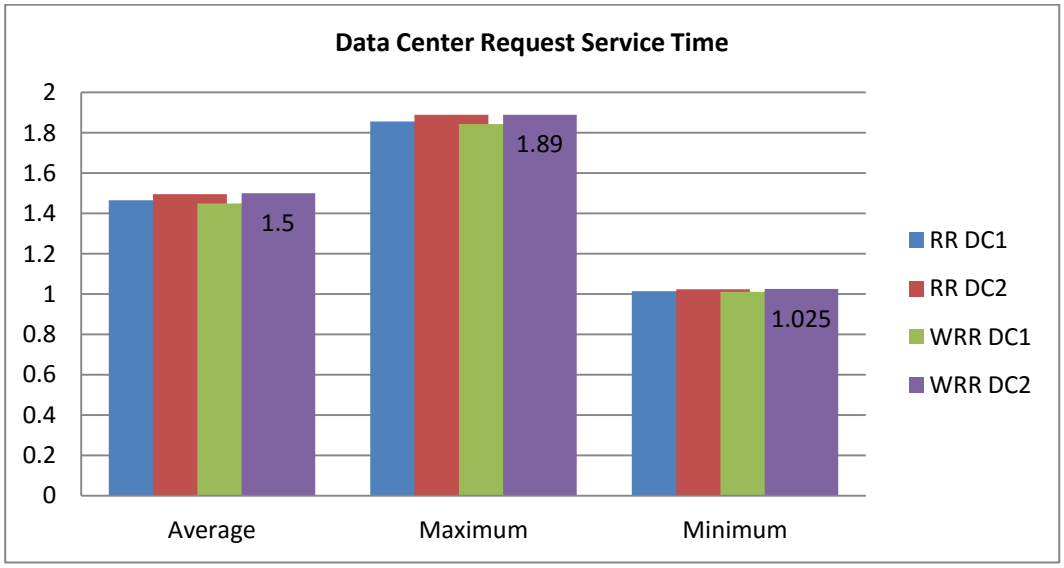



***Figure 19:*** *Optimise response time*

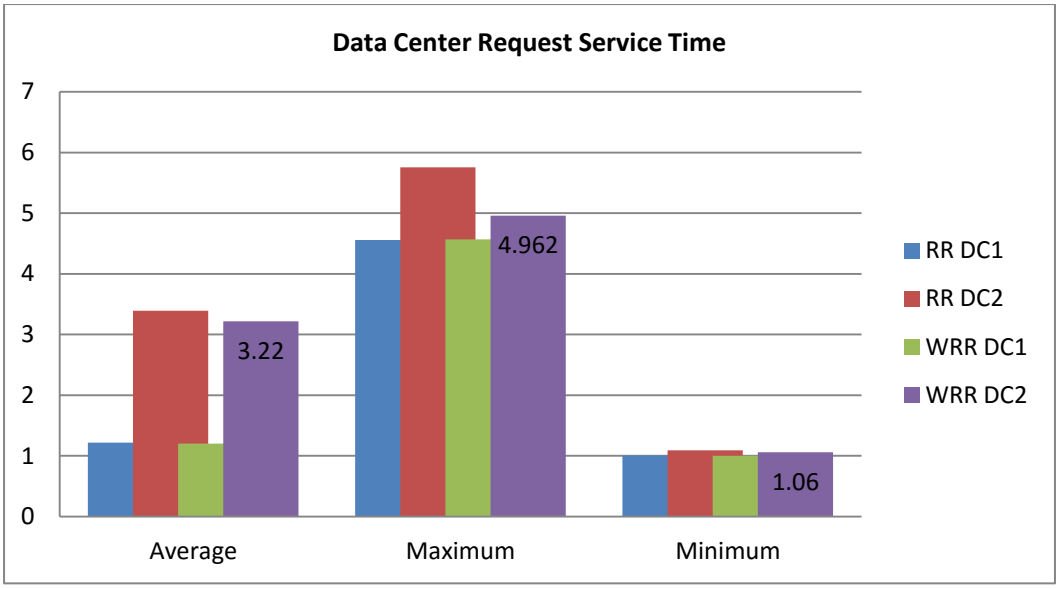



***Figure 20:*** *Reconfigure dynamically with load*

## 7. Conclusion

At last it is concluded that the adoption of cloud is good from the several aspects. It's good to take resources on rental bases rather to buy it and best thing is that one has to pay only for the amount of time for which he used such resources. One more technology of cloud is focused here that is DBaaS (database-as-a-service). It is beneficial to store the data on cloud database because personal systems are not enough spacious to store such huge amount of data there. In this case cloud database is one of the options to store their data. There are less chances of data loss in cloud databases as comparison to the normal database or we can say that cloud databases are robust in the case of disaster or data loss.

Also the information about cloudsim based tool CloudAnalyst is incorporated here. The tool is used for performing simulation using various policies. It maps the world wide data and connects several data centers to user bases. It also performs the task of load sharing in the case of overloading. There are three algorithms used in the simulator for performing the task of load sharing round robin policy, throttled load balancer policy and the equally spread current execution policy fourth one is the proposed algorithm for performing the task of load balancing on cloud database that is the weighted round robin policy. If we comparing the result of algorithms then the response time of round robin policy is smaller amongst all. With the service broker policy of closest data center it produced better results. Although the experiments performed only on two datacenter or five virtual machines and the generated result having minor difference from the previous one. But these changes must be taken into account and with some improvements or future understandings it could produce better results.

## References

[1] Buyya, R., Yeo, C.S., and Venugopal, S. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. Proc. of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC 2008, IEEE CS Press, Los Alamitos, CA, USA), 25-27, Dalian, China, Sept. 2008.

[2] Buyya, R., Ranjan, R., and Calheiros, R.N. Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities. Proc. of the

7th High Performance Computing and Simulation Conference (HPCS 09), IEEE Computer Society, June 2009.

[3] Buyya, R. and Murshed, M. GridSim: A Toolkit for the Modeling and Simulation of Distributed Resource Management and Scheduling for Grid Computing. *Concurrency and Computation: Practice and Experience*. 2002. 14; 1175-1220.

[4] Buyya, R. and Murshed, M. GridSim: A Toolkit for the Modeling and Simulation of Distributed Resource Management and Scheduling for Grid computing. *Concurrency and Computation: Practice and Experience.* 2002. 14 (13-15) 1175-1220.

[5] UOE (University of Edinburgh). Institute for Computing Systems Architecture. Simjava. 2009. http://www.dcs.ed.ac.uk/home/hase/simjava

[6] Bhathiya Wickremasinghe. CloudAnalyst: A CloudSim-based Tool for Modelling and Analysis of Large Scale Cloud Computing Environments. MEDC Project Report. Sep 2009.

[7] Pizzete, L. and Cabot, T., 2012: Database as a Service: A Marketplace Assessment. Retrieved 23rd November from http://www.mitre.org/work/tech_papers/2012/11_4727/cloud_database_service_dbaas.pdf.

[8] Sivashakthi, T. and Prabakaran, N. A Survey on Storage Techniques in Cloud Computing. *International Journal of Emerging Technology and Advanced Engineering*. 2013. 3 (12) 125-128.

[9] Nusrat Pasha, Amit Agarwal, and Ravi Rastogi. Round Robin Approach for VM Load Balancing Algorithm in Cloud Computing Environment. *International Journal of Advanced Research in Computer Science and Software Engineering.* 2014. 4 (5) 34-39.

[10] Waleed Al. Shehri. Cloud Database as a Service. *International Journal of Database Management Systems*. 2013. 5 (2) 1-12.

[11] Gill Sukhjinder Singh and Thapar Vivek. Implementation of a Hybrid Load Balancing Algorithm for Cloud Computing. *International Journals of Advanced Technology in Engineering and Science.* 2015. 10 (2) 73-81.

[12] Wickremasinghe Bhathiya, Rodrigo N. Calheiros, and Buyya Rajkumar. Cloud Analyst: A CloudSim Based Visual Modeler for Analyzing Cloud Computing Environments and Applications. Distributed Computing Project, CSSE Dept. University of Melbourne, 2009.

[13] Gupta Ruhi. Review on Existing Load Balancing Techniques of Cloud Computing. International *Journal of Advanced Research in Computer Science and Software Engineering*. 2014. 4 (2) 168-171.

**Cloud Publications**
International Journal of Advanced Computer Science and Information Technology
2020, Volume 6, Issue 1, pp. 101-114
ISSN 2320–0235, Crossref: 10.23953/cloud.ijacsit.461

Research Article

# Comparison of Back Propagation, Long Short-Term Memory (LSTM), Attention-Based LSTM Neural Networks Application in Futures Market of China using R Programming

**Wang Shuangao[1], Liu Yi[1], Rajchandar Padmanaban[2,3], Mohamed Shamsudeen[4] and Subalakshmi R[5]**

[1]Business School, China University of Political Science and Law, Xueyuan Road Campus: 25 Xitucheng Lu, Haidian District, Beijing, China
[2]NOVA Information Management School (NOVA IMS), Universidade Nova de Lisboa, Campus de Campolide, Lisbon, Portugal
[3]Forest Research Centre, School of Agriculture, University of Lisbon, Tapada da Ajuda,, 1349-017 Lisbon, Portugal
[4,5] University V.O.C. College of Engineering, Anna University Thoothukudi Campus, 7th Street West, Bryant Nagar Main Road, Thoothukudi, Tamil Nadu, India.

Correspondence should be addressed to Wang Shuangao, *wangshuangao@outlook.com*

Publication Date: 14 May 2020

**DOI:** https://doi.org/10.23953/cloud.ijacsit.461



**Abstract** Artificial neural network is widely used in the financial time series, but Long short-term memory (LSTM) neural network is rarely used in the futures market in China. In this paper, the LSTM neural network is studied by using futures data. The daily trading data of four groups of futures such as silver, copper, lithium and coking coal from December 2014 to December 2018 are used as the training object to make short-term prediction of the closing price. By comparing the Back Propagation (BP) neural network, general multi-layer LSTM neural network, and using the attention mechanism optimization LSTM contrast test, the result of the experiment shows that the futures price trend forecast time sequence, attention mechanism to promote significant effect of time sequence, and LSTM combined effect, by adjusting the parameters setting, using the improved LSTM neural network for time series prediction accuracy is higher, better generalization ability.
**Keywords** *LSTM Neural Network; Futures Forecasting; Attention Mechanism; Financial Engineering*

## 1. Introduction

Forecasting stock and futures prices is an interesting and difficult task for many analysts and academics, and because of the inherent complexity and dynamics of such price movements, improving their accuracy is particularly difficult (White, 2002). In the past few decades, economists have tried to predict stock and futures markets using linear measurement tools (AR, MA, ARIMA) and nonlinear algorithms (ARCH, GARCH, neural network) (Padmanaban and Karuppasamy, 2018).

In recent years, a small number of scholars began to study the application of data mining methods

to the stock market. Compared with the traditional measurement method, neural network has better prediction performance and learning performance in financial time series, and has more comparative advantages (Gencay, 1996). For the domestic stock market, a large number of scholars use various optimized BP neural networks to predict the stock market price and trend. With the further development of computer technology, some domestic scholars began to use Long Short Term Memory (LSTM) neural network for stock market prediction (Rajchandar, 2012). However, there are relatively few researches on the price prediction of futures market using neural network, and few researches on domestic futures market using LSTM neural network. The scale of futures market is huge, and there is still a large space for neural network research (Hinton, 2012).

In 1988, H. White used the neural network to study the daily stock return of IBM, which was the world's first prediction study on time series using machine learning. However, he failed to achieve the expected effect, because the model got into the problem of local minimum value in the training process, that is, the gradient explosion. Grudnitski used the basic neural network to predict the gold futures price in 1993, mainly to verify the applicability of neural network, and found that the prediction ability of neural network was better than the traditional data model (White, 2002). In 1996, German scholar Gencay used forward neural networks and perceptron to make an empirical analysis of Dow Jones industrial average index, which was mainly based on average data analysis, and the prediction effect was good (Gencay, 1996). In 2004, G. Peter Zhang used the method of combining ANN neural network with ARIMA traditional time series algorithm to accurately prove that the neural network was more accurate than the results obtained by ARIMA in nonlinear data analysis (Grudnitski and Osburn, 1993). In 2004, Shaikh and Iqbal used the neural network method to reveal the difference between implied volatility and temporal volatility to study the price changes of standard & poor's 500 index futures (Hamid and Iqbal, 2010); Hamid and Zakaria used four BP neural networks to predict the price of Iranian crude oil. On the whole, the optimized BP model was more effective than the ARIMA model. The larger the amount of training data, the more accurate the effect. Jan-chung Wang using a general equilibrium model to forecast the Taiwan stock market, in the model to join the market after the stochastic interest rate and market volatility, found that the prediction effect of this method than the general equilibrium pricing model prediction effect is strong, Jan-chung Wang also found that using the EWMA model with GARCH (1, 1) model method of combining the forecasting error of the futures market volatility than other models (Visalatchi and Padmanaban, 2012).

This paper summarizes the typical literatures on the prediction of non LSTM neural network model of futures as follows: by combing the related literatures on the prediction of futures price, it is found that the main prediction methods for futures can be roughly divided into two categories: one is to predict through GARCH and its modified model; the other is to comprehensively use other models, such as principal component analysis method, on the basis of neural network, to overcome the problem. The limitation of neural network improves the accuracy of prediction. For the price prediction using neural network, Yu Wen uses CNN LSTM neural network to analyze the secondary financial market data (Hochreiter and Jurgen Schmidhuber, 1997). Compared with the traditional simple statistical methods and some other neural network methods, such as logistic regression, convolutional neural network (CNN) is a more effective analysis of financial secondary market (Monishiya and Padmanaban, 2012). The market price is predicted in a relatively short period of time, and the prediction for a longer period of time is significantly improved, which is 10% higher than the simple statistical method and 5% higher than other neural networks (Dashti and Hamid, 2011). Using neural network to forecast futures, generally using LSTM combined with other methods. Yishun Liu (2019) found this model combines the VMD (variation pattern decomposition) method and LSTM (long-term short-term memory) network, constructs the prediction model, and forecasts the prediction trend and the inverse neural network model (BPNN) (Qiu and Akagi, 2016).

Leiji forecasts the price of carbon futures based on ARIMA CNN LSTM model. Chenhao Wang (2018) established a model to predict the high and low price of soybean futures through LSTM

neural network (Rajchandar and Bhowmik, 2017). Although the volume of China's futures market is huge, but generally speaking, there are few comparative studies on the futures market using neural network in China (Baek and Kim, 2018). Moreover, there are many problems in data selection range, model applicability and so on. In this paper, the LSTM based on the attention mechanism is compared with LSTM and BP neural network, which has some innovations.

## 2. Introduction to the Model Principle

### 2.1. Model Principle

LSTM is a special RNN (Recurrent neural network) Recurrent neural network. In 1997, Sepp Hochreiter and Jurgen Schmidhuber proposed LSTM algorithm (Hochreiter and Jurgen Schmidhuber, 1997). The recurrent neural network (RNN) is a time-depth neural network capable of processing sequence data. Since the significant disadvantage of RNN is "insufficient memory length", that is, it is unable to remember too far back or too far forward, the selection of hidden layer weight has a great impact on the learning and training process (Venkatesan and Padmanaban, 2012). If the weight is small, the gradient will disappear. Since the error gradient can be accumulated in the update, if the weight is large, it will become a very large gradient, which will result in a large update of the network weight, which will make the network unstable and eventually lead to "gradient explosion", which will result in unconvergence (Rumelhart and David, 1986). In order to deal with the gradient problem existing in RNN, the LSTM model of "peep hole connection" will be used for reference in this study. The advantage of the LSTM model is that it is better for processing and predicting time series events with long intervals and delays (Fakhruddin and Mahalingam, 2018). The reason for this is that the basic unit of its short and long memory network consists of one or more memory blocks and three adaptive multipliers, namely the input gate, the output gate and the forgetting gate (see Figure 1). Through the three gates to achieve the preservation and control of information. The process of studying and predicting the futures time series is shown in the following Figure 1:

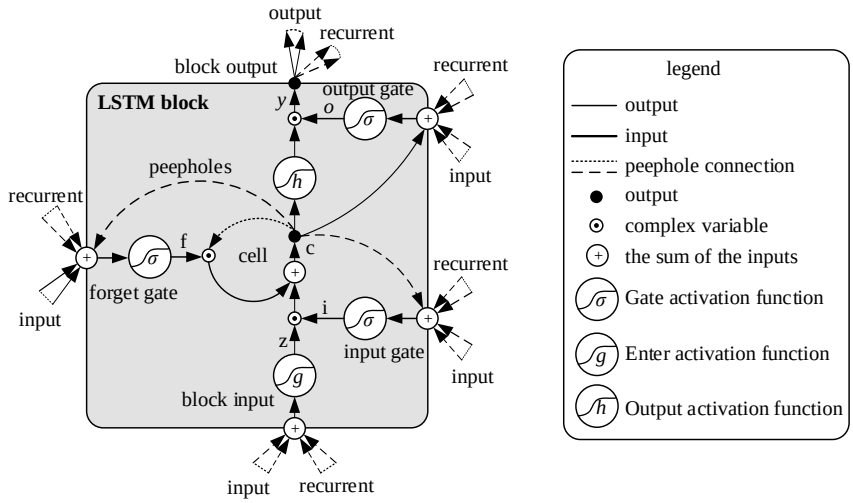



***Figure 1:*** *Schematic diagram of LSTM model, made by the author*

### 2.2. LSTM Related Formulas

The relevant mathematical formulas in this paper are obtained according to Ren Jun's research and appropriately revised on this basis (Wen and Yuan, 2018). The input data is set as X, and Zc is the current state value of the neuron Cell. Each Cell is updated at time t and LSTM. The condition of the input gate is as follows:

$$Z_l^t = \sum_{i=1}^{l} w_{il} x_i^t + \sum_{hh=1}^{H} w_{hl} y_h^{t-1} + \sum_{c=1}^{C} w_{cl} Z_c^{t-1} + b_i \quad (1)$$

In formula (1), the variable with subscript l is related to the input gate. The first term is the input of the external unit, and the third term is the input from the dashed part of the Cell. The second term with the subscript h is a generic term, because both the elements and the hidden nodes in the LSTM model can be interconnected, so a portion of the external input can also be represented by it, where it represents the bias vector of the input gate $b_i$. For forgotten doors gate is as follows:

$$Z_\phi^t = \sum_{ii=1}^{l} w_{i\phi} x_i^t + \sum_{h=1}^{H} w_{h\phi} y_h^{t-1} + \sum_{c=1}^{C} w_{c\phi} S_c^{t-1} + b_\phi \quad (2)$$

### 2.3. BP Neural Network Model

BP neural network is Rumelhart & McClelland two people first proposed in 1986, it is a special kind of multilayer forward neural network, BP algorithm is to solve the multi-layer forward neural network weights optimization and proposed, is characterized by forward signal transmission, error back propagation, is currently the most widely used in neural network learning algorithm of a class of the diagram above is a typical BP neural network. Where, is the input of the input layer, and is the weight between the JTH node of the hidden layer and the node of the input layer. $x_1 \mathrm{L}\ x_i \mathrm{L}\ x_n$ $w_{1j} \mathrm{L}\ w_{ij} \mathrm{L}\ w_{nj}$. (Figure 2)

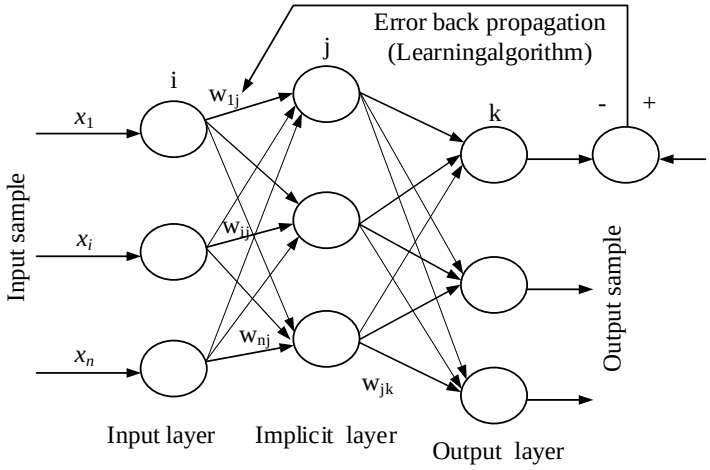



***Figure 2:*** *BP model diagram*

The BP neural network algorithm in this paper refers to the research of Hongwei Ding, and its steps are as follows:

1) Initialization weight and threshold value: the random initialization interval is [-1,1], and a threshold value is set for each cell.
2) propagation forward from the input layer

Input calculation formula of hidden layer:

$$I_j = \sum_{i=1}^{n} W_{ij} O_i + \theta_j \quad (3)$$

Where, is the threshold value of the JTH neuron in the hidden layer.$O_j$ The actual output calculation formula of the hidden layer:

$$O_j = f(I_j) = \frac{1}{1+e^{-I_j}} \quad (4)$$

Where, f is the excitation function. In the same way, the output value of the output layer can be obtained. The derivation steps are omitted.

### 2.4. LSTM based on Attention

Attention mechanism means to focus on something and get more Attention. The attention mechanism in deep learning is supposed to pay more attention to certain factors when processing data. In a broad sense, attention is an integral part of the network architecture, responsible for managing and quantifying interdependencies:

- Between the input and output elements (general note)
- In the input element (self care)

In this paper, the most important part of LSTM optimization strategy is the addition of the attention mechanism, whose motivation is to consider the different input time series and their different influences on the predicted output. In order to realize this kind of network, softmax function is added to the time sequence dimension of the input end to calculate the weight of attention, as shown in equation (5):

$$weights = \text{soft}\max(Input) \quad (5)$$

After the weights are obtained, they need to be applied to the input to assign different weights to the timing of the input, so as to make the prediction better.

$$output = weights * (Input) \quad (6)$$

## 3. Empirical Method

This article uses R programming and Python to process the data and generate training diagrams.

### 3.1. Data Preprocessing

The raw data of silver, copper and lithium futures in this paper are from Shanghai futures exchange, and the raw data of coking coal futures are from Dalian Commodity Exchange. Since the original futures data are discontinuous or missing due to the stop of trading and so on, this paper standardized the data with excel. The data set is the daily trading data combination of December 16, 2014, December 17, 2018 for a total of 4 years. The sample form after data preprocessing is shown in the following Table 1:

***Table 1:*** *original data styles (silver AG for example)*

| Date | Opening price | Highest price | Lowest price | Closing price | Before the settlement price | Settlement price |
|---|---|---|---|---|---|---|
| 20141216 | 3650 | 3667 | 3503 | 3525 | 3682 | 3615 |
| 20141217 | 3602 | 3602 | 3434 | 3465 | 3615 | 3477 |
| 20141218 | 3434 | 3520 | 3418 | 3496 | 3477 | 3472 |

| | | | | | | |
|---|---|---|---|---|---|---|
| ... | ... | ... | ... | ... | ... | ... |
| 20181217 | 3550 | 3550 | 3500 | 3508 | 3524 | 3511 |

### 3.2. Parameter Setting

Learning rate is one of the most important over parameters for deep neural network adjustment. The learning rate is too low, the training is more reliable, and the optimization is too time-consuming, because each step toward the minimum loss function is small. However, if the learning rate is too high, the training may not converge. The amount of weight change can be so large that the optimization passes the minimum and the loss function becomes worse. The number of iterations is the number of times the neural network learns on the training set, and is also the number of times the weight item is updated. In general, the selection of the number of iterations is mainly to make the training loss value of the neural network close to or reach the minimum. When more training times are given, the result of the neural network is no longer greatly improved, and the value nearby is the number of iterations. In general, the three most important parameters, training set, learning rate and iteration times, constitute the input parameters of the prediction function in the neural network.

The structural parameters of BP and LSTM models are designed as follows: the number of independent variables is consistent with the number of neurons; each layer of input and output is available; the division of time points is consistent with the number of model layers; the input is input one by one in accordance with the time sequence. In order to prove the effect of the model, this study tested the closing price, the highest price and the lowest price respectively. Namely, the opening price, the lowest price, the highest price, the trading volume, and the closing price and other five independent variables (parameters).

In this study, BP and LSTM models were used to predict the closing price on the 8th day with 7 transaction days. The partition proportion of the data set is: 85% of the data blocks are used for training, and the remaining 15% are tested in chronological order. The network parameters of BP model are designed as follows. (1) Correction rate: 0.1; (2) number of hidden layers: 1100; (3) learning rate: 0.05; (4) iteration: 1000;

The network parameters of LSTM model are designed as follows: (1) the number of the two hidden layers is: 50,100; (2) learning rate: 0.005; (3) time steps: 30; (4) number of iterations:200. LSTM parameters after adding CNN convolution and Attention: (1) the number of hidden layers is: 128,64; (2) time steps 6;(3) number of iterations: 200.

## 4. Analysis of Experimental Results

### 4.1. Model Training Effect

The goal of training (learning) is to set the learning rate as 0.005, and the output error will become smaller and smaller after the iterative training through the neural network until the error is stable in a small interval. The learning rate of the following four futures is set at 0.005, the total number of iterations is 200, and the proportion of data set training and testing is 85%:15%. The image reflects
the convergence of four different training errors in the data set training. The blue line represents the training situation, the yellow line represents the test situation, and the index of the vertical coordinate is the sum of squares of errors. The abscissa represents the number of iterations of the neural network. The loss function of model training is MSE.

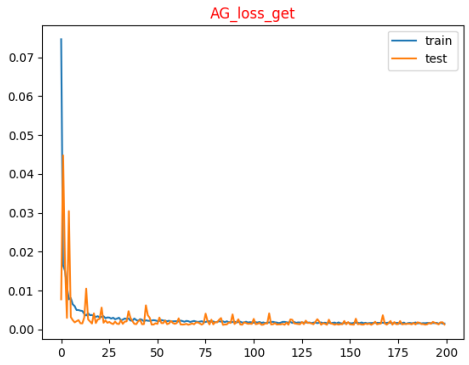



***Figure 3:*** *Silver training renderings*

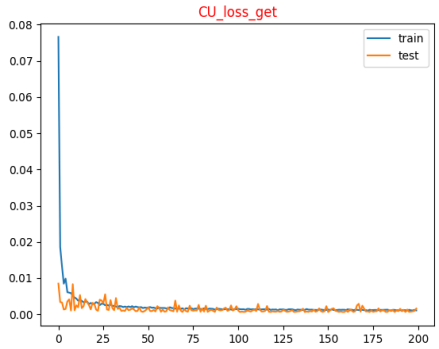



***Figure 4:*** *Copper training renderings*

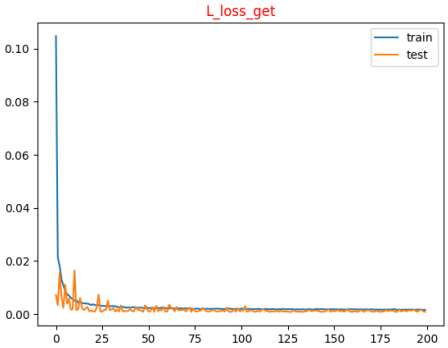



***Figure 5:*** *Lithium training effect diagram*

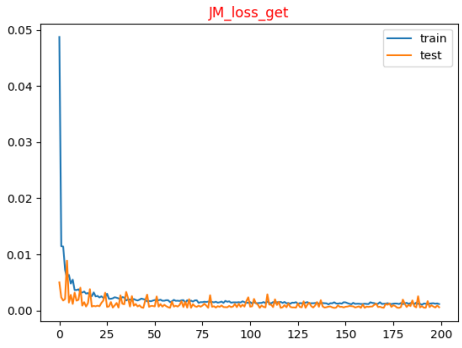



***Figure 6:*** *Coke training effect diagram*

The general LSTM training effect is shown in the Figure 3, 4, 5, 6. It can be seen that silver stays stable after 50 iterations, copper stays stable after 25 iterations, lithium stays stable after 25 iterations, and coke stays stable after 50 iterations.

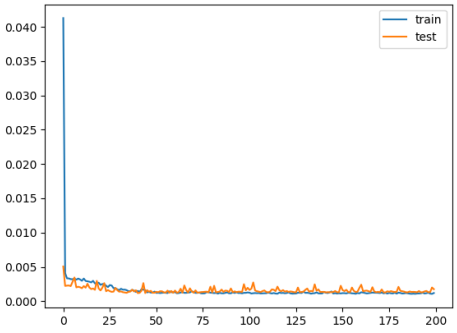



***Figure 7:*** *Training effect of silver closing price*

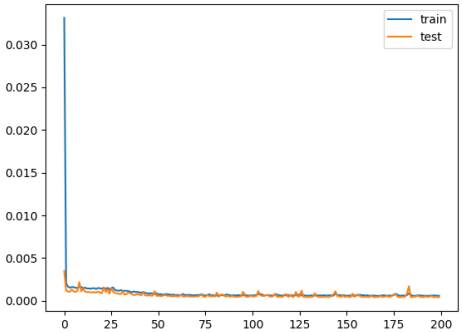



***Figure 8:*** *Training effect of copper closing price*

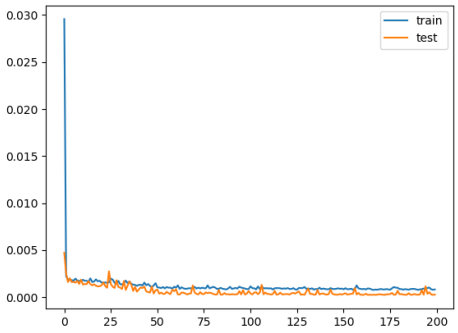



***Figure 9:*** *Training effect of coking coal closing*

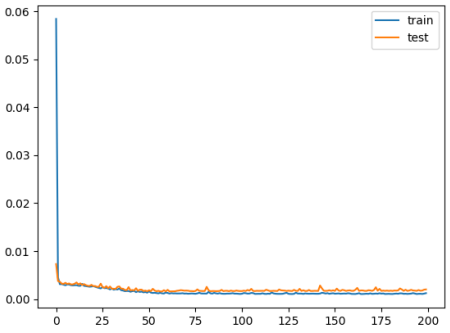



***Figure 10:*** *Training effect of lithium closing price*

The training effect of LSTM model based on the adaptive learning rate based on attention is shown in the Figure 7, 8, 9 and 10. According to the LSTM learning and training based on the above four futures closing prices, the image converges rapidly when the average number of iterations is within 25. The training of the model in the data set can make the error of the neural network converge rapidly to the range of (0,0.1).

Learning from the general training, the number of iterations are within 100 images to achieve rapid convergence, model in the training data set, can make the error of the neural network is fast convergence in (0,0.1) interval, in the number of iterations is lower than 50 times of model prediction error was rapidly decreases, that model has fast convergence characteristics, all futures prediction and stability in the lower interval training error, show that model is stable. In general, the model after further optimization has good applicability and stable prediction performance.

### 4.2. Comparative Analysis of the Prediction Effect between BP and LSTM

The graph comparison and analysis of the predicted results are shown in the following legend. The x-coordinate in the Figure 11, 12, 13, 14, 15 and 16 represents the number of iterations, and the y-coordinate is the error value and the futures price, respectively. The yellow curve represents the actual value and the blue curve represents the predicted value.

The prediction results after BP and LSTM neural network training (taking silver and copper as an example for comparison): the left side is BP's prediction results, and the right side is LSTM's prediction results. It can be seen that the LSTM's silver prediction results are very good, and the copper prediction results are also good, slightly separated from the actual value.

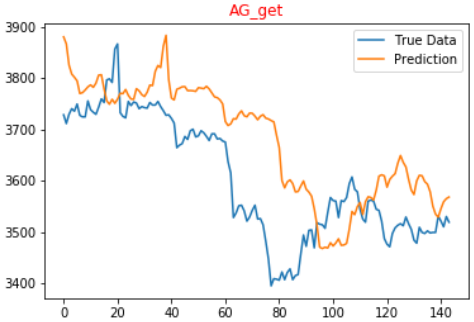



***Figure 11:*** *Silver BP prediction*

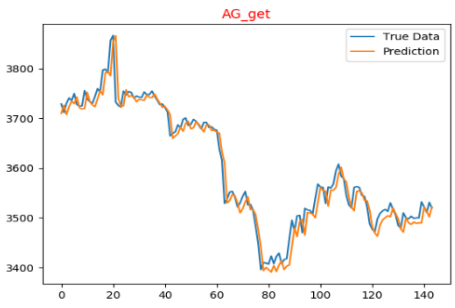



***Figure 12:*** *Silver LSTM prediction renderings*

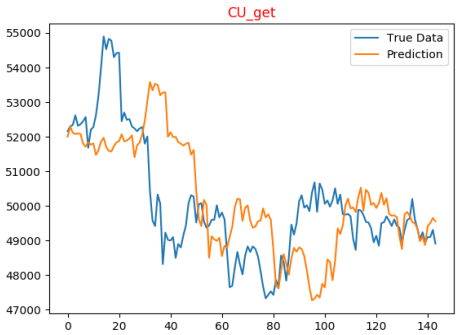



***Figure 13:*** *Copper BP prediction effect*

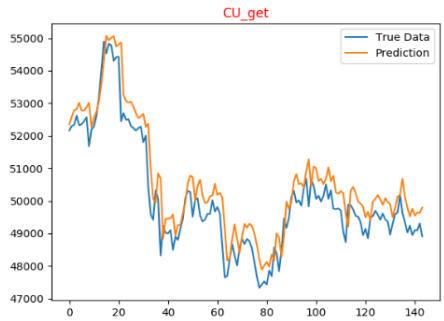



***Figure 14:*** *Copper LSTM prediction*

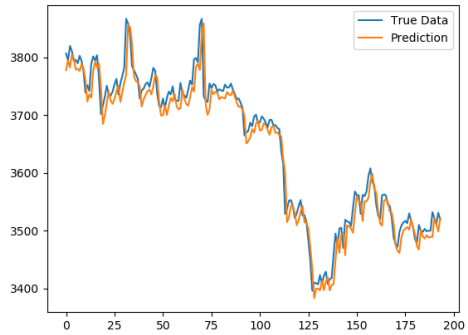



***Figure 15:*** *Optimization of LSTM effect for sliver*

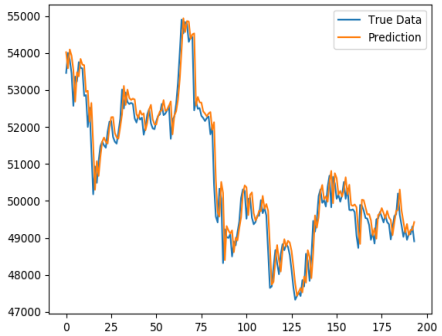



***Figure 16:*** *Optimization of LSTM effect for copper*

By comparing BP neural network and data set training, the fitting result is not ideal, indicating that BP neural network is not a special time series of data for prediction. In addition, the study also predicted the lowest and highest prices of all futures. In the case of copper and silver, it can be seen from the forecast and the actual trend chart that the prediction effect is very good for the peak price of silver (AG_low).The lowest price of copper (CU_low) and the highest price of silver (AG_high) result in a better prediction effect, and the prediction of the highest price has deviation. By observing the curves of the above four futures prediction results and comparing the prediction results with the actual trend, it can be clearly found that the predicted output of LSTM model on the four futures prices is basically consistent with the real output on the overall trend.

### 4.3. Model Prediction Accuracy Analysis

In the evaluation research of accuracy, the evaluation index of regression algorithm, namely root mean square error (RMSE), is used to evaluate the accuracy of prediction. The root mean square error is also known as the standard error, which is the square root of the loss function for linear regression. You take the true value, the predicted value, and then you square it and average it, and then you take the square root. Intuitively, MSE is equivalent to putting the loss function on the test set to see the loss value. Due to the limitation of the number of observations, the best value is usually used to replace the real value. The advantage of the square root error is that it is very sensitive to the very small or very large errors in the measurement, and the precision of the measurement can be well reflected. In the RMSE calculation formula, the value on the Y test set is the actual value, and Yi is the output value of the neural network.

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(Y_i - Y)^2}{n}} \quad (7)$$

When the size of RMSE value reflects the size of the predicted result deviating from the actual result when multiple measurements of a variable are made, that is, the higher the measurement

accuracy is, the smaller the RMSE will be. The Table 2 shows the RMSE results when four futures varieties are predicted.

***Table 2:*** *Comparison of root mean square error of LSTM neural network in futures price prediction*

| varieties | silver | copper | Coking coal | lithium |
|---|---|---|---|---|
| RMSE | 0.0125 | 0.0208 | 0.0219 | 0.0233 |

MAE=average absolute error (MAE) is another loss function used for regression models. MAE is the sum of the absolute value of the difference between the target value and the predicted value

$$MAE = \frac{1}{m}\sum_{i=1}^{m} | h(x^i - y^i) | \qquad (8)$$

***Table 3:*** *Comparison of the average absolute error of LSTM neural network in the prediction of futures prices*

| Varieties | Silver | Copper | Coking coal | Lithium |
|---|---|---|---|---|
| RMSE | 0.0111 | 0.0159 | 0.0181 | 0.0119 |

As can be seen from the above table, RMSE of copper, coking coal and lithium futures is larger than that of silver, and the RMSE of silver is 0.017. The predicted value is the most consistent with the graph of the real value, with almost no separation, and the prediction accuracy is the highest.

In order to further explore the reason why RMSE and MAE are not the same futures, we further analyzed the original data of silver, copper and lithium. The following four charts show the raw data distribution of futures. It can be clearly seen that the distribution of the original data of silver is relatively regular and concentrated, and the overall figure is closer to the normal distribution, while that of coking coal is poor in terms of distribution regularity, and the data distribution is more dispersed. The lowest and highest values of lithium

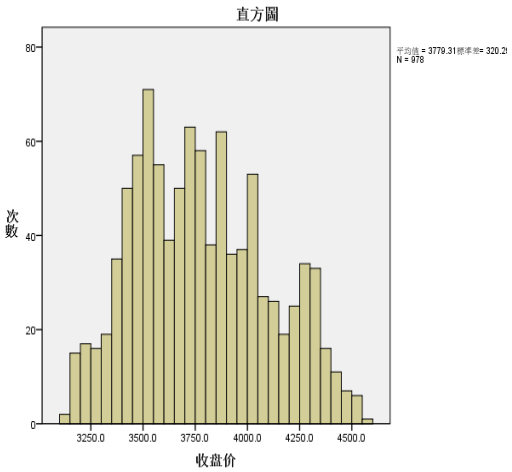



***Figure 17:*** *Histogram of silver original data*

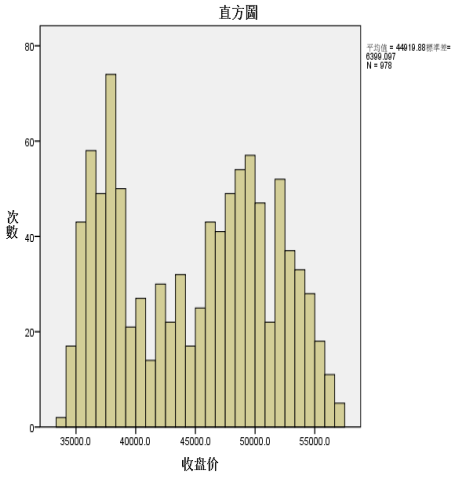



***Figure 18:*** *Box diagram of copper original data*

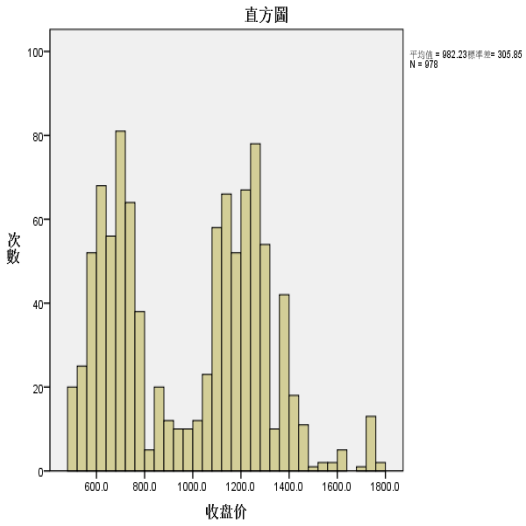



***Figure 19:*** *Box diagram of raw data of coking coal*

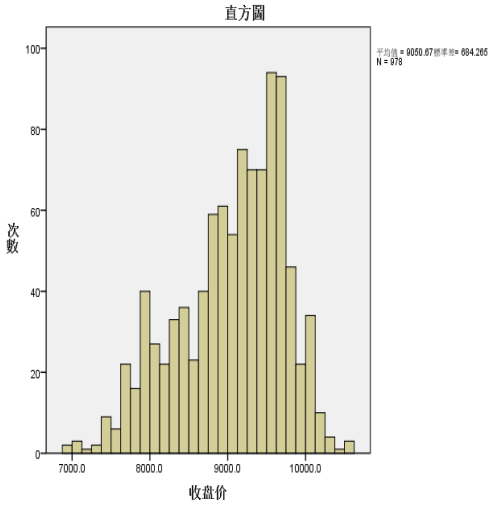



***Figure 20:*** *Distribution histogram of raw data of lithium*

The RMSE value of lithium is the largest among the four futures, and its predicted value is the most discrete with the actual result, and the prediction effect is the worst. The difference between the maximum value and the minimum value of lithium is prominent. RMSE is more sensitive to outliers, and the above results are consistent with the principle of RMSE.MAE of coking coal is the largest, that is, the absolute average value is the largest, which means the dispersion degree of coking coal is large.

Through the distribution of the original data, it also shows that the LSTM neural model has different prediction effects on different futures, which is related to the model and the dispersion degree of the distribution of individual futures data. The LSTM neural network model in this study has a root-mean-square error value in the range of (0,0.1) for the prediction of the future price trend, which fully shows that the prediction accuracy is very high, and the model is applicable to the future price with good performance and significant prediction effect.

## 5. Conclusions and Prospects

All BP neural networks applied in stock market prediction belong to the theoretical category of static neural networks. Such neural networks have no memory function and are excessively dependent on the current input. Therefore, static neural networks cannot well reflect the dynamic characteristics of stock and futures markets. LSTM neural network increases the horizontal connection between the hidden layer units, has the characteristics of memory and the influence of internal time sequence. As an RNN with memory and feedback type, LSTM neural network is a type of dynamic neural network. Compared with the original model, a hidden layer is added to improve the performance of LSTM model in predicting financial time series. The LSTM dynamic neural network is suitable for the high noise, nonlinear and unstable random price time series in the market.

For gradient problems of RNN and neural network fitting problem, the empirical use data normalization and dropout method to modify the model, dropout by adjusting the LSTM model parameters (not modifying the objective function) under the same conditions, through the contrast experiment, found that the modified LSTM model has better generalization ability, don't rely too much on some local characteristics, such as silver futures has better prediction effect.

The study by optimizing the LSTM model for time series prediction calculation of the biggest problems are often a fitting, and this article very good correction of this problem, due to network

with multiple hidden layer structure, better able to learn the characteristics of futures data in the past, and be able to find out the relationship between the time series, also can use selective memory function, and do dig deep to the internal laws of the futures price. The experimental results show that no matter the closing price, the lowest price or the highest price, the results of this study are satisfactory.

In the time series prediction, uses convolution to further optimize. The size of the convolution kernel in the convolution layer is 3*3, the number of the convolution kernel is 4, and Max pooling is added to the output of the convolution kernel. However, the empirical results show that LSTM attention has a better effect, indicating that convolutional neural network is not necessarily the optimal choice for time series, while parameter adjustment is more effective. Of course, it is possible that this is the reason why the author chose only one type of convolution. In the next article, the author will further verify the convolution optimization.

The distribution of the original data directly determines the prediction accuracy of the model for the futures data. The model optimization in this study improves the applicability of the model to the new sample data by adjusting the parameters rather than the objective function. Therefore, in order to make good use of this model and obtain good returns in financial practice, it is suggested that futures varieties with the characteristics of relatively concentrated and regular distribution of the sorted original data should be selected. For futures with poor data distribution regularity, it may take too long to train the model, and the prediction effect may not be as good as expected.

Influence the cause of the futures prices is diverse, the change of the futures market is complex, both macroeconomic factors, also has the market supply and demand factors, and both parties speculative factors, so the market traders can't rely too much on technology, and to see the problem from the intrinsic nature of the economy. LSTM neural network also has its own disadvantages. In the current situation, machine learning cannot predict the long-term trend and cannot include all the influencing factors.

The selection of the overall data quantity is limited, and the results of the study, after the training model of effective for individual products, also hard to adapt to more varieties of futures market, this also is the common problem facing all the neural network, this study only discuss the forecasting accuracy and stability, not to the model in the case of applicability of futures to do deep research, so still have considerable space to further research.

Futures market, there are many factors that affect the direction of the trading price, so it is difficult to predict. The advantages of LSTM neural network model, such as the rapidity, determine the ability to quickly analyze a huge amount of data to achieve real-time prediction results, while the stability reflects the reliability of the model. These application characteristics are very important for price prediction and will have a great impact on the future returns of investors. It can be predicted that artificial neural network has wide application space in futures and stock market prediction.

## References

Baek, Y., and Kim, H.Y. 2018. ModAugNet: A new forecasting framework for stock market index value with an over fitting prevention LSTM module and a prediction LSTM module. *Expert Systems with Applications*, 113, pp.457-480.

Dashti, R.A.S.E., Hamid, M., and Zakaria, F. 2011. Forecasting Iranian crude oil price using artificial neural network and arima models. *Journal of Social Policy*, 7(3), pp.382-383.

Fakhruddin, B., Mahalingam, R., and Padmanaban, R. 2018. Sustainable development goals for reducing the impact of sea level rise on mangrove forests. *Indian J. Geo-Marine Sci.*, 47(10),

pp.1947-1958.

Gencay Ramazan. 1996. Non-linear prediction of security returns with moving average rules. *Journal of Forecasting*, 15(3), pp.165-174.

Grudnitski, G., and Osburn, l. 1993. Forecasting S&P and gold futures prices: An application of neural networks. *Journal of futures Markets*, 13(6), pp.631-643.

Hamid, S.A., and Iqbal, Z. 2004. Using neural networks for forecasting volatility of s & p 500 index future sprices. *Journal of Business Research*, 57(10), pp.1116-1125.

Geoffrey E. Hinton, Nitish Srivastava, Alex Krizhevsky, Ilya Sutskever, Ruslan R. Salakhutdinov. 2012. Improving neural networks by preventing co-adaptation of feature detectors. *https://arxiv.org/abs/1207.0580*

Hochreiter, Sepp, and Jurgen Schmidhuber. 1997. Long short term memory. *Neural Computation,* 9(8), pp.1735-1780.

Monishiya, G.B., and Padmanaban, R.C. 2012. Mapping and change detection analysis of marine resources in the tuticorin and vembar group of island using remote sensing. *Int. J. Adv. Forest Sci. and Management*, 2(2), p.132.

Padmanaban, R., Bhowmik, A.K., and Cabral, P. 2017. A remote sensing approach to environmental monitoring in a reclaimed mine area. *ISPRS Int. J. Geo-Information*, 6(12), doi:10.3390/ijgi6120401.

Padmanaban, R, Bhowmik, A.K., and Cabral, P. 2019. Satellite image fusion to detect changing surface permeability and emerging urban heat islands in a fast-growing city. *PLoS One*, 14(1):e0208949.

Padmanaban, R. 2019. A remote sensing approach to the quantification of local to global scale social-ecological impacts of anthropogenic landscape changes. *https://www.semanticscholar.org/paper/A-remote-sensing-approach-to-the-quantification-of-Padmanaban/b9bb88620d546bdd5837c834445c8deff7c7020d*

Padmanaban, R.C. 2012. Integrating of Urban Growth Modelling and Utility Management System using Spatio Temporal Data Mining. *Int. J. Adv. Earth Sci. Eng,* 1, pp.13-15.

Padmanaban, R., Karuppasamy S., and Narayanan R. 2018. Assessment of pollutant level and forecasting water pollution of Chennai coastal, TamilNadu using R. *Indian J. Geo-Marine Sci.* 47(7), pp.1420-1429.

Padmanban, R, and Painho, M. 2017. Urban Agent Based Model of Urban SlumDharavi, Mumbai, *International Journal of Earth Sciences and Engineering*, 10(6), pp.1110-1117.

Qiu, M., Song, Y., and Akagi, F. 2016. Application of artificial neural network for the prediction of stock market returns: the case of the Japanese stock market. *Chaos, Solitons & Fractals*, 85, pp.1-7.

Rajchandar, P. 2012. Modelling the Transformation of Land use and Monitoring and Mapping of Environmental Impact with the help of Remote Sensing and GIS. *Int. J. Adv. Altern. Energy Environ. Ecol.* 1, pp.36–38.

Rajchandar, P., Bhowmik, A.K., Cabral, P., Zamyatin, A., Almegdadi, O., and Wang, S. 2017. Modelling Urban Sprawl Using Remotely Sensed Data: A Case Study of Chennai City, Tamilnadu. *Entropy*, 19(4), p.163.

Rumelhart, David E., Geoffrey E. Hinton, and James l. McClelland. 1986. A general framework for parallel distributed processing. Parallel distributed processing: Explorations in the microstructure of cognition, 1, pp.45-76.

Venkatesan, G., and Padmanaban, R. 2012. Possibility Studies and Parameter Finding for Interlinking of Thamirabarani and Vaigai Rivers in Tamil Nadu. *India. Int. J. Adv. Earth Sci. Eng.* 1(1), pp.16–26.

Visalatchi, A., and Padmanaban, R. 2012. Land use and land cover mapping and shore line changes studies in Tuticorin coastal area using remote sensing. *Int. J. Adv. Earth Sci. Eng*. 1, pp.1-12.

Wang, J. 2010. Stock Market Volatility and the Forecasting Performance of Stock Index Futures Journal of Forecasting, 28(4), pp.277-292.

Wen, Y., and Yuan, B. Use CNN-LSTM network to analyze secondary market data. Proceedings of the 2nd International Conference on Innovation in Artificial Intelligence. 2018, pp.54-58.

White. Economic prediction using neural networks: the case of IBM daily stock returns. IEEE 1988 International Conference on neural networks.

Zhang, G. Peter. 2003. Time series forecasting using a hybrid ARIMA and neural network model. Neurocomputing, 50, pp.159-175.