Journal of Information Security Research

DLINE JOURNALS

Print ISSN: 0976-4143
Online ISSN: 0976-4151

JISR 2025: 16 (3)
https://doi.org/10.6025/jisr/2025/16/3/85-97

A Study of Cloud Computing Performance and Security using Full Harmonic Encryption Method

Farhan Nisar
Qurtaba University of Information Technology
Pakistan
farhansnisar@yahoo.com

ABSTRACT

Cloud Computing mean the relationship between many computer users across through a get in touch relation with other users like internet. In Cloud Computing we transmit and receive data from the internet. Cloud Computing give the liberty to Cloud Provider gives the opportunity to their user to use service as per pay model. Now days, in Cloud Performance and Security of data are major problem of Cloud Computing. In this paper, we identify the straight and forward approach to identify the system performance and security based on more secure our data as well as high availability. We also highlight providing high performance to the cloud clients and providing high level security to the Cloud user by using fully harmonic encryption techniques.

Keywords: Cloud Computing, Performance, Availability, Security, Binomial Distribution Approach for Performance Availability, Fully Homomorphic Encryption for Security, Control Mechanism, Conclusion

Received: 27 December 2024, Revised 5 April 2025, Accepted 29 April 2025

1. Introduction

Cloud computing is rising a new technique in which computer resources are available which are centralized and user can access it from remote server. Now a day, many businesses are transferring to cloud computing which is more reliable and less cost effectively. For Example yahoo and Gmail are the example of cloud services. Before discussing the Cloud Computing is using 27/7 availability, low expenditures, high automated, easy to developed and pay as peruse service model. There are three types of data in Clouds.

1. Data which is transmitted

2. Data which is stored

3. Data which is processed

The Problem in cloud is performance, availability and security issues. Availability is one of the important threat in clouds and customer cannot move his data to different service provider. The 2nd issue of availability is lock-in problem when service is out of of business. The data may be unavailable for indefinite period of time when losing data from the clouds. The performance base on application, variety of service problem and application and simulation scenarios such as e-learning software's and QoS problem can be solved in this paper. The third issue of security is secure data transfer; secure software interfaces and secures store data, user access control and data separation problem may be solve in this paper.

The Cloud Computing is more protected and more consistent. We can easily add or remove assets in Cloud computing.

In Infrastructure as a Service Faults are:

i) Network Failure mean server will be down or server problems

ii) Hardware Failure means performance will be down

In Platform as a service faults are:

i) Service Failure means System memories will be failure

ii) Configuration Failure means low transfer rate

In Software as a Service Faults are:

i) Quality of Service Failure means configuration errors

ii) Maintenance Time failure means upgrade problem failure

These services are related to Cloud Computing and solve by using the proper defense mechanism

Performance of Cloud Computing: The Cloud Computing is more famous for IT projects and mostly work are shifted on business environment. The main problem facing by Cloud users is performance issue occurs. Performance issue can be solve in many ways in which design a architectures which deal with latency sending packets from source to destination in a round trip time. We can divide the data into small chunks and share out it to all clouds. Performance depends on both downloading as well as uploading. Uploading means to encrypt the data in to small chunks while downloading mean decrypt the data into small chunks.

Availability of Cloud Computing: Cloud Computing mean something is available and ready to use by the users. It is directly proportional to reliability and performance. The high availability depends on enough redundancy. The factor which can affect the availability is human errors, software and hardware failures and machine migration from one place to another which can affect the Cloud computing availability.

Security of Cloud Computing: Security means how much your data secure from illegal users. Every client wants privacy and protected his data because most of the data contain confidential information. If the data can be accessed by Hackers then privacy and security of the data would be lost.

We can protect data from both internal and external attack and no one can alter in the data. If we can divide the data in to small chunks then security issue can be solves. If any illegal person hack some of data chunks then he cannot access the whole data easily. We can divided the data into three parts

i) Check for authenticate user only

ii) Encrypting data into secure algorithm

iii) Decrypt the data

we are using encryption and decryption mechanism to provide secure communication.

Problem in Performance of Cloud Computing: The Performance of Cloud computing depend on sharing of resources and shared network are the problem of performance in Clouds. If there is once Centralized Clouds then every client want to access it active and deactivate of all the users can affect the performance of the Clouds. Another factor which is affecting the performance is Parallelize Computing which also creates a burden on network performance and load on the servers because a single input can be given and a result a single output comes out. The performance can also depend on system capability if the system cannot capable to run the application then it can also affect the performance of the Cloud users.

Problem in Availability of Cloud Computing: Availability mean system is ready to use for the clients. If the heavy load traffic of the users on the Cloud server then there is problem of availability because system cannot be accessible and resources can be used by Clients. If the Cloud provider cannot solve the issue of availability then system is not reliable and trustworthy. Other factor which affect the availability are human errors, software and hardware failures. Another factor which is also affect the availability are upgrade of software setup because when software is update then all application will be in pending state.

Problem in Security of Cloud Computing: Security is main issue in cloud computing because system cannot be secure without security. The Cloud system has centralized server which have a big risk of cloud security. Many attacks can be attempt on Cloud which in case the data will be lost. We should must need a authorized person which can control the Cloud administration and if the administrator is careless then huge amount of data lost. The cloud computing involve many stakeholder which are customers, cloud providers, service users. Each stakeholder has own task due to different involvement in cloud then security of Cloud become risky.

Solution for Performance of Cloud Computing: For performance of Cloud computing we can do optimization and parallel processing to increase the speed of performance and multiple Clients can be access the service and used the software application. We divide the data in small chunks then speed and time also be increase. By using high configuration of hardware also increase the performance. We are using multiples resources input and multiples resources output for data. For protected our data we use firewall on the network

By using Binomial Distribution approach for System Performance and Availability in Cloud Computing:

Binomial distribution approach is also known as K out n. If distribution can fulfilled the following requirements then it is refer to Binomial Distribution.

The condition can be followed as:

1) Each variable have two types of categories one is successor and other is failure.

2) It obtain X successor out of n trials.

3) Binomial distribution has fixed number of successor (n).

4) Each result is independent from one to another and doesn't effect the present result.

5) The probability for each successor will be constant.

Formula:-

$$\text{Performance } P_S = {}^nC_{k}.\, P^{k} * q^{n-k} \ \ where\ {}^nC_k = n! \,/\, k!(n-k)!$$

$$q = 1-P$$

$$\text{Reliability } R_S = {}^nC_{k}.\, P_s^{\,k} * q^{n-k} \ \ where\ {}^nC_k = n! \,/\, k!(n-k)!$$

$$q = 1 - P_s$$

Formula State:

i) n is the number of successor and must be fixed and depend on service availability.

ii) k is number of successor from n.

iii) P is probability of Cloud service availability.

iv) q is the number of failure and equal to $q = 1 - P$.

v) Successor and failure are complementary and equal to $P + q = 1$.

Entire system performance is down for 1 hour only. Software can be hang-up and deadlock occurs due to incorrect input and output for synchronization will be failed due to software application connectivity with the central server.

Successor (x) would be attempt from n service availability per hour or in minute or in a given time.

Value of $K = 0, 1, 2, 3$ and $n = 3$ is the number of trial from n and assuming 0.9 as minimum trial as a treatment.

The system Performance can be calculated as:

No of Service (k)Service Performance	Successor (n)	Treatment (0.9)	System Performance
0	3	0.9	0.001
1	3	0.9	0.0270
2	3	0.9	0.2430
3	3	0.9	0.7290

If $k = 0$, $n = 3$, $P = 0.9$

Here $k = 0$ successor out of $n = 3$ & the probability of successor $P = 0.9$

Step#1

$P_S = {}^nC_{k*} P^{k*} q^{n-k}$

$P_s = {}^3C_{0*} (0.9)^0 * (1-0.9)^{3-0}$

$= (3! / 0! (3-0)! * 1 * (0.1)^3$

$= (3! / 0! (3)! * 1 * 0.001)$

$= 1 * 1 * 0.001$

$P_s = 0.001$

If k=1, n=3, P=0.9

Here k=1 successor out of n=3 & the probability of successor P=0.9

Step#1

$P_S = {}^nC_{k*} P^{k*} q^{n-k}$

$P_s = {}^3C_{1*} (0.9)^1 * (1-0.9)^{3-1}$

$= (3! / 1! (3-1)! * 0.9 * (0.1)^2$

$= (3! / 1! (2)! * 0.9 * 0.01)$

$= 3 * 0.9 * 0.01$

$P_s = 0.027$

If k=2, n=3, P=0.9

Here k=2 successor out of n=3 & the probability of successor P=0.9

Step#1

$P_S = {}^{n}C_{k\,*} P^{k} * q^{n-k}$

$P_s = {}^{3}C_{2\,*} (0.9)^2 * (1\text{-}0.9)^{\,3-2}$

$= (3! / 2! (3\text{-}2)! * (0.9)^2 * (0.1)^1$

$= (3! / 2! (1)! * 0.81 * 0.1)$

$= 3 * 0.81 * 0.1$

$P_s = 0.243$

If $k = 3$, $n = 3$, $P = 0.9$

Here k = 3 successor out of n = 3 & the probability of successor P = 0.9

Step#1

$P_S = {}^{n}C_{k\,*} P^{k} * q^{n-k}$

$P_s = {}^{3}C_{3\,*} (0.9)^3 * (1\text{-}0.9)^{\,3-3}$

$= (3! / 3! (3\text{-}3)! * (0.9)^3 * (0.1)^0$

$= (3! / 3! (0)! * 0.729 * 1)$

$= 1 * 0.729 * 1$

$P_s = 0.729$

Here is the Figure in which performance can be calculated in Matlab when k=0, 1, 2, 3, n=3, P=0.9

System Reliability is related to availability in which system is available is 24/7 and service must be available in office timing from 09:00 am to 04:00 pm. The System Reliability is failed due to some error seem like this “Server has no response” or failure occurs

The causes of System Availability are:

i) System crashes or hang out

ii) Network will be jamming or any attack can be attempt

No. of Successor Service Availability	Sucessor (n)	Performance P_s	System Reliability R_s
0	3	0.001	0.997
1	3	0.0270	0.076
2	3	0.243	0.134
3	3	0.729	0.388

```
> > binopdf (0, 3, 0.9)

ans =

1.0000e-003

>> binopdf (1, 3, 0.9)

ans =

0.0270

>> binopdf (2, 3, 0.9)
ans =

0.2430

>> binopdf (3, 3, 0.9)

ans =

0.7290
```

Figure 1

The K observation out of n successor of Cloud Availability is as below:

Here $k = 0$, $n=3$ $P_s = 0.001$ & probability of 0 successor is $P_s = 0.001$

Step#2

$R_{s=}(n! / k! (n\text{-}k)! * P_s^{\,k} * (1 - P_s)^{n\text{-}k}$

$R_s = (3! / 0! (3\text{-}0)! * (0.001)^0 * (1\text{-}0.001)^3$

$R_s = (3! / 0! (3\text{-}0)! * (0.001)^0 * (0.999)^3$

$R_s = (1 * 1 * (0.997)$

$R_s = 0.997$

Here $k = 1$, $n = 3$ $P_s = 0.270$ & probability of 1 successor is $P_s = 0.270$

Step#2

$R_{s=}(\mathrm{n}! / \mathrm{k}! (\mathrm{n\text{-}k})! * \mathrm{P}_s^{\,\mathrm{k}} * (1 - \mathrm{P}_s)^{\mathrm{n\text{-}k}}$

$R_s = (3! / 1! (3\text{-}1)! * (0.0270)^1 * (1\text{-}0.270)^2$

$R_s = (3! / 0! (3\text{-}1)! * (0.0270)^1 * (0.973)^2$

$R_s = (3 * 0.0270 * (0.946)$

$R_s = 0.076$

Here k = 2, n = 3 $\mathrm{P}_s = 0.243$ & probability of 2 successor is $\mathrm{P}_s = 0.243$

Step#2

$R_{s=}(n! \,/\, k!\,(n\text{-}k)! * P_s^{\,k} * (1 - P_s)^{n-k}$

$R_s = (3! \,/\, 2!\,(3\text{-}2)! * (0.243)^2 * (1\text{-}0.243)^1$

$R_s = (3! \,/\, 2!\,(1)! * (0.059) * (0.757)$

$R_s = (3 * 0.059 * (0.757)$

$R_s = 0.134$

Here k=3, n=3 P_s=0.729 & probability of 3 successor is $P_{s=}$0.729

Step#2

$R_{s=}(\text{n}! \,/\, k!\,(\text{n-}k)! * P_s^{\,k} * (1 - P_s)^{\text{n-k}}$

$R_s = (3! \,/\, 3!\,(3\text{-}3)! * (0.729)^3 * (1\text{-}0.729)^{3\text{-}3}$

$R_s = (3! \,/\, 3!\,(3\text{-}3)! * (0.388) * (0.973)^0$

$R_s = (1 * 0.388 * (1)$

$R_s = 0.388$

Here is the Figure in which Reliability can be calculated in MATLAB when k=0, n=3, P_s is performance of each Cloud Service

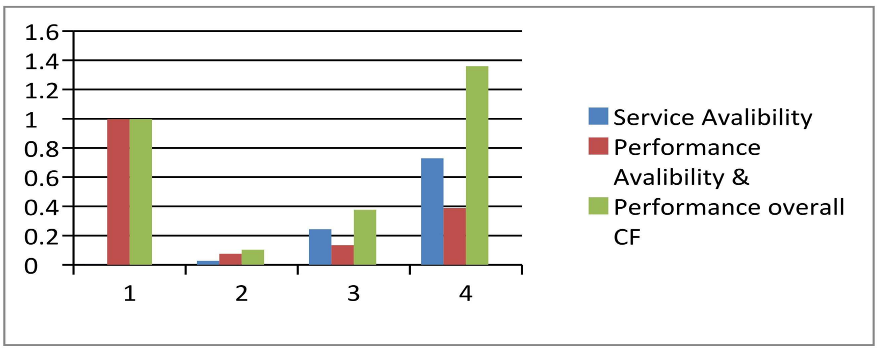
```
> > binopdf (0, 3, 0.001)
ans =
0.9970
>> binopdf (1, 3, 0.027)
ans =
0.0767
>> binopdf (2, 3, 0.2430)
ans =
0.1341
>> binopdf (3, 3, 0.0729)
ans =
3.8742e-004
```

Figure 2

For Calculating overall performance and Availability of the Cloud Service We can find a Cumulative Frequency of the Service that is highly available to the users and find out that overall Service Reliability through binomial Distribution.

Solution for Security in Cloud Computing: Security issue can be solving by dividing the data into small chunks. When we can divide our data most of data can be encrypted in to cipher text and hence increase the

S. No	Service Availability	Service Performance	Availability + Performance Cumulative Frequency
1	0.001	0.997	0.998
2	0.027	0.076	0.103
3	0.243	0.134	0.377
4	0.729	0.388	1.36



security. If any unauthorized user can access it then he get only limited information rather than the huge amount of the data Because in Cloud environment many client can access the cloud services. Then it reduce the security of the Cloud data. Security issue can also increase by mobility of the data and changing the location of data also help to reduce the security issue. Regular password changing also solving security issue. We should design an algorithm in which data can be encrypted and for hacker it can be difficult to access the data. Many big organization use Linux in which data can be secure.

By using fully Homomorphic Encryption Approach for System Security in Cloud Computing: The homomorphic Encryption Algorithm which is used to encrypt and decrypt the data. The homomorphic encryption is very expensive application. It depends on three steps:

1) Data Protection: The data can be transmitted in cipher form to the cloud user and divide into small chunks and data will be securely transmitted and even the cloud administrator or provider cannot be read that encrypted data.

2) Data Progression: Fully homomorphic encryption make a trust between third party and the customer who use the Cloud services and convert direct data in to encrypted form and another user can decrypt it.

3) Cipher Text Reclamation: Cipher text can retrieve by cipher text method directly. For the privacy of the data multiplication and addition function can be used without changing the plain text.

i) Encryption Algorithm: The homomorphic encryption parameters are p, q and r, where x is positive all large odd numbers, y represent all large positive even numbers. P and Q are use as key generation for the data security phase and r is any random encryption of the data text when selected.
For text m, calculate as:

$$C = m + 2r + P^*Q$$

$$\text{Encrypt: Plain Text} \rightarrow \text{Cipher Text}$$

Where C is the Cipher text and m is representing the data then we will get the cipher text

ii) Decipher Algorithms:
The homomorphic encryption in which cipher text convert back to its original plain text.

$$m = (c \text{ mod } P) \; mod \; 2$$

Because p and q are less then $(m + 2r)$ then C mode P will be (m+2r) and it must be keep in mind that decryption can be done from many to one.

$$m = (m + 2r) \; mod \; 2$$

$$\text{Encyption}^{-1} = \text{Decrypt : Cipher} \rightarrow \text{Plain Text}$$

Verification of Homomorphic Encryption Algorithm:
i) The Homomorphism Addition Verification:
Suppose we have two group of data as m_1 and m_2 to convert it in to cipher text as follows:

Cipher $\text{Text}_1 = (\text{Data}_1 + \text{Codeword}_1)$
$C_1 = m_1 + 2r_1 + P * Q_1$
Cipher $\text{Text}_2 = (\text{Data}_2 + \text{Codeword}_2)$
$C_2 = m_2 + 2r_2 + P * Q_2$

For Plain text
Encryption (m_1) + Encryption (m_2) = Encryption $(m_1 + m_2)$
$m_3 = m_1 + m_2$
Cipher Text_3 = Cipher Text $_1$ + Cipher Text $_2$
$C_3 = (C_1 + C_2) = (m_1 + m_2) + 2(r_1 + r_2) + P(Q_1 + Q_2)$
Here P is much less than from the $(m_1 + m_2) + 2(r_1 + r_2)$
$C_3 = (C_1 + C_2)$ mode $P = (m_1 + m_2) + 2(r_1 + r_2)$

This algorithm can satisfy the security issues and provide most secure service to their Customers using addition property.

ii) The Homomorphism Multiplication Verification:
Suppose the plain text will be as follow

Cipher $\text{Text}_1 = (\text{Data}_1 + \text{Codeword}_1)$

$C_1 = m_1 + 2r_1 + P * Q_1$

Cipher Text$_2$ = (Data$_2$ + Codeword$_2$)

$C_2 = m_2 + 2r_2 + P * Q_2$

For Plain text

Encryption (m_1) * Encryption (m_2) = Encryption (m_1 * m_2)

$m_4 = m_1 * m$

Cipher Text$_4$ = Cipher Text $_1$ * Cipher Text $_2$

$C_4 = C_1 * C_2 = (m_1 + 2r_1 + P * Q_1) * (m_2 + 2r_2 + P * Q_2)$

$= m_1 m_2 + 2r_2 m_1 + m_1 PQ_2 + m_2 2r_1 + 4r_1 r_2 + 2r_1 PQ_2 + m_2 PQ_1 + 2r_2 PQ_1 + P^2 Q_1 Q_2$

$P\{PQ_1Q_2 + Q_2(m_1 + 2r_1) + Q_1(m_2 + 2r_2)\}$

As we know that Here P is much less than from the $(m_1\, m_2) + 2\,(r_1 r_2 + rm_2 + r_2 m_1)$ $C_4 = C_1 * C_2$ mode $P = m_1 m_2 + 2\,(2r_1\, r_2 + r_1\, m_2 + r_2\, m_1)$

This algorithm can satisfy the security issues and provide most secure service to their Customers by using multiplication property.

Control Mechanism:

i) The new user can add itself in cloud storage system through proper mechanism that enhance to reduce the Security Risk in Clouds.

ii) The Client can enter, delete, download and upload data to the cloud through proper mechanism that also reduces security Risks.

iii) The Server can monitor the user activity and make a log in database

iv) Client can also retrieve the data through the Proper mechanism Which also reduce the security risk in Cloud.

Security Solutions	Desktop (user) Windows 7	Server (Application Platform) Windows 2008	User Application
OS Hardened (not required services or ports to be blocked)	Yes	Yes	No
Antivirus, Malware, Spyware	Yes	Yes	No
Vulnerability assessment and fixing for OS/App	Yes	Yes	Yes
Patch Management (updates)	Yes	Yes	Yes
Access Control	No	No	Yes
Segregation of Duties	No	No	Yes
Auditing	No	No	Yes

Table 1. Security Measure Adopted for Cloud and Network in Real Time Industries

Conclusion

In this paper we can study the different characteristics of cloud services. We can also discuss performance availability and Security problem and how they can solve. Performance depends on uploading and downloading in a mean time. We can solve it by binomial distribution technique. We can also resolve the availability issue in Cloud when we upgrade software or network jamming then we check that our system is in idle condition or not and we get the high availability. We can also solve security mechanism by using homomorphic approach to convert any data into decrypted form and cannot understand by other users. This mechanism is still safe for users.

References

[1] Rivest, R., Adleman, L., Dertouzos, M. (1978). On data banks and privacy homomorphisms [M]. *NewYork: Academic Press, 169—180.*

[2] Heiser, Jay., Nicolett, Mark. (2012). Assessing the Security Risksof Cloud Computing *[EBOL]*(2008—6—3)[12—28]. www.gartner.com id=685308.

[3] Gentry, C. Fully homomorphic encryption using ideall attices [M] *New York Association for Computing Machinery2009169—178.*

[4] Bedra, A. (2010). Getting started with Google App engine and clojure [J]. *IEEE Internet Computing*, 14(4), 85-88.

[5] Gens, F., IT cloud services user survey, pt.2: top benefits & challenges [EB/OL]. http://blogs.idc.com/ie/?p=210, 2012-12-01.

[6] Wikipedia. (2009). Side kick data loss [EB/OL]. http://en.wikipedia.org/wiki/ 2009_Sidekick_data_loss, 2012-12-0

[7] Sonehara, N., Echizen, I., Wohlgemuth, S. (2011). Isolation in cloud computing and Privacy-Enhancing technologies [J]. *Business & Information Systems Engineering,* 3(3), 155-162.

[8] Talbot, D. (2010). Security in the ether [J]. *Technology Review,* 113(1), 36-42.

[9] Zissis, D., Lekkas, D. (2012). Addressing cloud computing security issues [J]. *Future Generation Computer Systems, 28(3), 583-592.*

[10] Klems, M., Coben, R., Kaplan, J, et al. Twenty-one experts define cloud computing [EB/OL]. http://cloudcomputing.sys-con.com/node/ 612375/print, 2012-12-05.

[11] Foster, I., Zhao, Yong., Raicu, I., et al. (2008). Cloud computing and grid computing 360-degree compared [C]. *Grid Computing Environments Workshop*. GCE '08, 2008: 1-10.

[12] Vaquero, L M., Rodero-merino, L., Caceres, J., et al. (2009). A Break In The Clouds: Towards A Cloud Definition[J]. *Acm Sigcomm Computer Communication Review,* 39(1): 50-55.

[13] Wikipedia. Cloud computing [EB/OL]. *http://en.wikipedia.org/wiki/ Cloud_Computing, 2012-12-05.*