Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

OSNQSC: Optimized Selection Of Nodes For Enhanced Qos In Cloud Environment

Jeevitha B K[a] , Thriveni J[b] , and Venugopal K R*

*Vice-chancellor, Bangalore University, Bangalore.

[a;b] Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bengaluru- 560056

Abstract—For a cloud to be secure, all of the participating entities must be secure. The security of the cloud resources does not solely depend on an individual's security measures. The neighbouring entities may provide an opportunity to an attacker to bypass the user's defences. The data may compromise due to attacks by other users and nodes within the cloud. Therefore, high-security measures are required to protect data within the cloud. Cloud sim allows the creation of a network that contains a set of Intelligent Sense Point (ISP) spread across an area. Each ISPs will have its own unique position and will be different from other ISPs. Cloud is a cost-efficient solution for the distribution of data but has the challenge of a data breach. The data can be compromised of attacks of ISPs. This paper proposes an optimized method to find the best ISPs to place the data fragments that considers the channel quality and remaining energy of the ISPs. The fragments are encrypted before storing them. The proposed method is compared with the existing Betweenness centrality, Eccentricity and Closeness centrality methods of DROPS (Division and Replication of Data in the Cloud for Optimal Performance and Security) in terms of time, storage, throughput and energy consumption of the ISP.

Keywords- Centrality Measures, Data Fragments, Intelligent Sense Point, Optimized Method, T-Colouring.

I. INTRODUCTION

The cloud computing has altered the way of managing the infrastructure of information technology. The first aspect of the cloud is making it a powerful service for the adoption of any individual/organization. Along with the benefits of cloud such as low-cost, less maintenance and more flexibility leads to increased security burden [1]. These security concerns may occur because of the technology and offers given by the cloud's core services. To deliver the secure cloud, all of the participating entities must be secure [2]. In any given system with multiple entities, the highest level of the system's security is equal to the security of the weakest entity. Therefore, the security of the assets does not solely depend on an individual 's security measures [3]. The neighbouring entities may provide an opportunity to an attacker to bypass the user 's defences.

National Institute of Standards and Technology (NIST) has been designed for the secure adoption of cloud by the federal government to develop the standards and guidelines of cloud computing [4]. The standards should be able to migrate easily, cost-effective, and have the key elements that are required to ensure the effectiveness in the global marketplace. The NIST Cloud Computing Standards Roadmap Working Group [5] has compared

the existing standards for interoperability, performance, portability, security, accessibility standards/models/studies/use-cases/conformity assessment programs, etc, that are relevant to cloud computing. With the help of the available information, current standards, gaps, and priorities are identified.

Bernd et al., [6] introduced a security architecture that are significant to the cloud-specific vulnerabilities and provides examples of cloud-specific vulnerabilities for each architectural component. Juels et al., [7] proposed an auditing framework that describes new techniques of secure cloud data by assuring a wide range of protections. These techniques
ensure the integrity, newness to high data availability and mitigate few security concerns of enterprise resources into public clouds.

A. Motivation

in the existing methods, multiple complex paths are formed by the existing centrality methods (Betweenness, Closeness,
and Eccentricity) between source and destination ISP, thus loses the energy level drastically. The forwarding ISP in the path discovery process that is picked is based on various kinds of average distance methods of the overall path in the existing methods of centrality measures. It does not consider the energy levels of ISP that intern affects the network health. The data fragments are stored as a plain text which is not secure and the load on the ISPs is enormous.

B. Contributions

OSNQSC is proposed for outsourcing data that considers both performance and security. The method fragments and replicates the file over cloud ISPs. These ISPs are selected by considering both the capacity quality of the nodes in terms
of energy and the distance between the ISPs. Dividing the file into fragments provides confidentiality to the user's data. No meaningful information is relieved to an attacker on any successful attack on the ISP. The fragments are encrypted to
ensure the double security on the fragments of the file. And the controlled replication of the file fragments, where each fragment is replicated only once for the purpose of increase the data availability and reliability. OSNQSC achieves data integrity by assuring the user about not corrupting the data. Privacy of the data is ensured by giving access to upload the data only to authorized users.

C. Organization

The remainder of the paper is organized as follows. Section II provides an overview of the Literature Survey. Section III gives the Background Work that helped to achieve the work. OSNQSC is introduced in Section IV. Section V provides the Performance Analysis made for the work. Section VI Concludes the paper along with few future suggestions for the enhancements of the work.

II. LITERATURE SURVEY

The goal is to assure the rights of intellectual property to all the entities of the cloud i.e., data owner, environment and software merchant. Peter et al., [8] focussed on how to transfer the authority to process the data to another party on behalf of the data owner. The binding of code and data together describes the elementary controlling of access to any other entity unless it is licensed.

Increased usage of ICT produces greenhouse gases, contributing 2-3 of global emissions and keep rising each year. One of the biggest concerns is reducing cost to providers in energy consumption of the servers while maintaining the QoS and Service Level Agreements (SLA). Conor et al., [9] proposed an algorithm that schedules the incoming task, which quickly completes the highest priority task and asks as a buffer in case of losing operating servers. It either uses standard or energy-efficient servers dynamically based on the priority scheme.

Pascal et al., [10] proposed a scheduling approach that incorporates energy efficiency and network awareness methods and termed it as DENS [11]. It focuses on balancing the consumption of energy, distributing tasks between computing servers and managing the network traffic.

Data Centers (DC) have been experiencing a notable expansion of interconnected servers. Being a design issue of data center, network infrastrutute plays a crucial role in basic investment and detemining the performance parameters of the data center. Data Center Network (DCN) lacks the built-in capabilities of the data center to meet the current demands of the bandwidth. So Bilal et al., [12] have simulated by implementing the models of DCN based on the legacy architecture, switch-based, and hybrid models by monitoring the network in terms of throughput and delay. The author has considered the simulation under various network traffic patterns to verify the different DCN architecture strengths and weaknesses.

Data centers have been considered as an essential of the Information and Communication Technology (ICT) [13] sector that needs to be robust to failures, erratically to distribute the required Quality of Service (QoS) level and should satisfy Service Level Agreement (SLA). The author [14] analyses the robustness of the state-of-the-art DCNs along with the significant contributions are: (a)Multi-layered graph modeling of various DCNs; (b) Classical robustness metrics considering various failure scenarios to perform a comparative analysis; (c) Inadequacy of the traditional network robustness metrics to appropriately evaluate the DCN robustness; and (d) New procedures to quantify the DCN robustness.

Generally, communication resources have become a bottleneck problem in cloud service provisioning applications. Therefore, data replication is the encouraging solution that brings the data (e.g., databases) closer to data users (e.g., cloud applications) that reduce network delays and bandwidth usage. D Boru [15] discusses the concept of data replication in cloud data centers. The author considered both energy efficiency and bandwidth consumption of the system to improve the QoS to reduce communication delays. Sushant Goel and Rajkumar Buyya [16] have compared different replication algorithms that covers a wide range of applications under distributed storage. It also includes the system of content management that ranges from distributed Database Management Systems, Service-oriented Data Grids, Peer-to-Peer (P2P) Systems, and Storage Area Networks.

Nicolas [17] has adapted the replication techniques to improve the data availability by achieving the load balancing among the data centers at the minimal cost. The author proposed a highly available key-value store that determines the cost-efficient positions of data replicas. Mohammad [18] considers the replication process a popular tool to achieve data availability as data grids have limited storage with high computing cost. The author proposed a priority-based replication scheme that the storage accessed based on price, number of access

attempts and the current time. The resources are hired from other sites of the network when resources are not available.

Fabre et al., [19] talk about the tolerance of any intrusion in a distributed system that the authenticated and authorized server enables a policy with a set of unrelated, untrusted sites and administrates by untrusted authorities. The author describes about some functions of distributed systems can be designed to tolerate intrusions. A prototype of the persistent
file server presented has been successfully developed and implemented as part of the Delta-4 project of the European ESPRIT program.

W.K. Hale [20] introduces the minimum-order approach to frequency assignment problems of both frequency-distance constrained, and frequency constrained optimization problems. The frequency constrained approach should be avoided if distance separation is employed to mitigate interference. A restricted class of graphs, called disk graphs, plays a pivotal role in frequency-distance constrained problems. The author introduced two generalizations of chromatic number and shows that many frequency assignment problems are equivalent to generalized graph coloring problems.

In meteorology, the cloud hook formation [21] provides a useful analogy for cloud computing. The most acute obstacles with outsourced services (i.e., the cloud hook) are security and privacy issues. The author identifies the key issues, that are believed to have long-term significance in cloud computing security and privacy, based on documented problems and exhibited weaknesses.

Subramanian et al., [22] presented a framework that enhances the security for data sharing with index-based cryptographic data slicing. This helps the individuals/organizations in removing the centralized distribution of storage and adoption of a multi-cloud storage service that assures trust.

III. BACKGROUND WORK

A. Cloud Sim

Cloud Sim is a toolkit/library from CLOUDS labs to stimulate cloud computing resources [23]. Clouds Sim does not support any actual software technology. It does not run any real-time applications, so we cannot run our projects on Cloud Sim. Cloud Sim is a library that is written purely in Java. So in order to use it, we need to write the code in Java. Cloud Sim is programmatically implemented as an extension of Grid Sim.

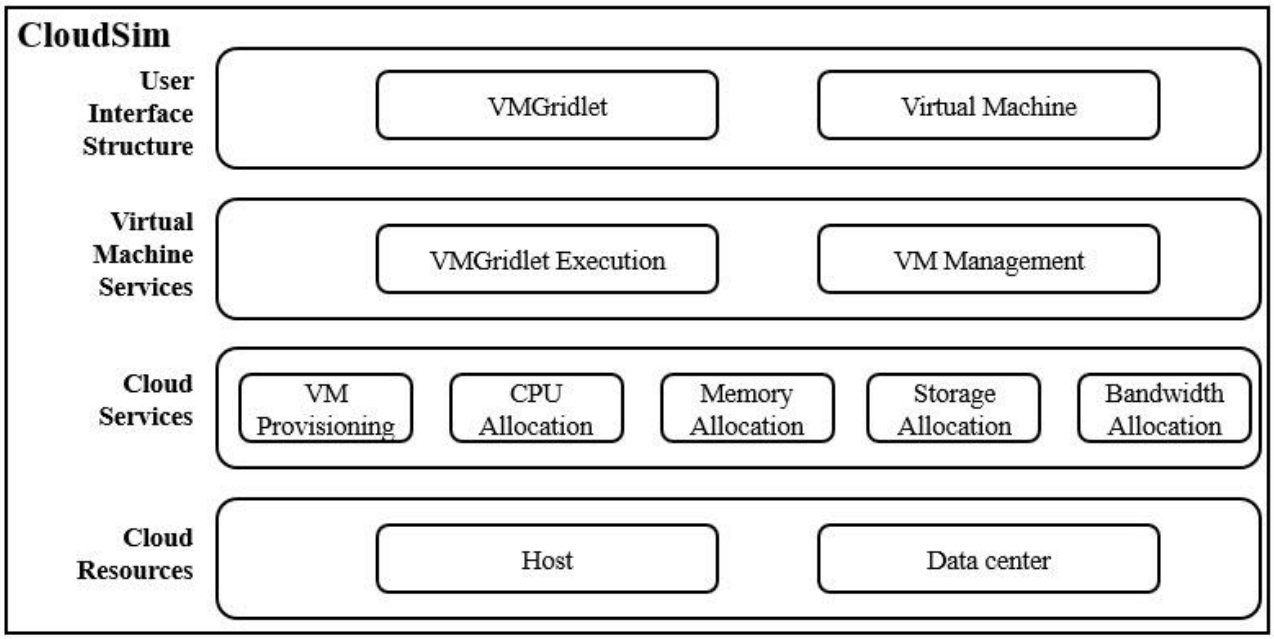

Fig. 1: Cloud Sim Architecture

Cloud computing with new technology for delivering secure and scalable computational services represented as software,
infrastructure, or platform as services. It gives access to the infrastructure that incurs payment in real currency and offers simulation-based approaches that allow the users to test their services in repeatable and controllable environment. Cloud Sim makes researchers and developers concentrate on system design issue that explore the cloud-based infrastructure and services.

Fig 1 shows the service and resources that are supported by Cloud Sim. Cloud Sim supports the functionalities of modeling and simulation of large scale data centers, servers, hosts, application containers, data center network topologies, federated clouds, user-defined policies for allocation of hosts to virtual machines and policies for allocation of host resources to virtual machines[24]. Cloud Sim provides novel support for modelling and simulation of virtualized cloud-based data center environments such as dedicated management interfaces for VMs, memory, storage, and bandwidth. It manages the initiation and execution of virtual machines, data centers, hosts, applications, and transparently manage huge system components during the simulation period.

B. Intelligent Sense Point

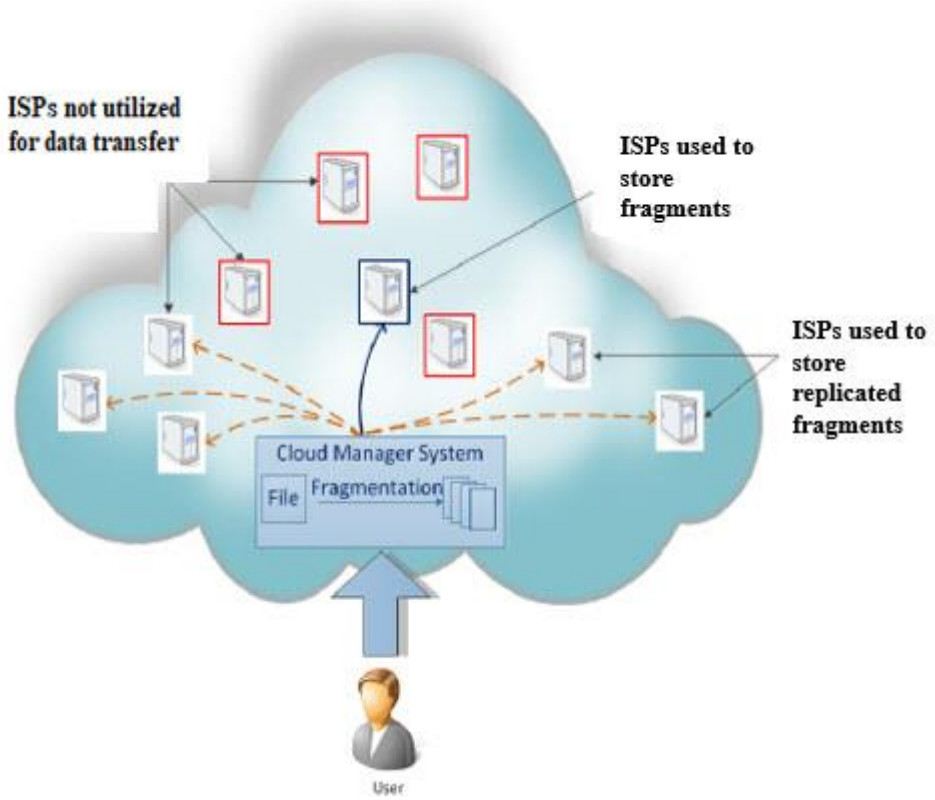

Fig. 2: Intelligent Sense Point System

Fig 2 shows the distribution of Intelligent Sense Points (ISP). The entire region is intelligently occupied by the sense points, and path is formed and data can be stored. The data can be sparse on each of the ISP and data can be replicated
on other non-participant ISPs. Multiple ISPs will be used to form the path based on T-color measure and then data is transformed into smaller fragments and stored on the path ISPs and other ISPs that are not on the path. The ISPs are randomly sparse across the area, and each ISP will have its own location. Each ISP will have unique memory, control packet sense and battery maintainer. When the ISP is used repeatedly in the path formation, then a lot of energy is lost in the process and even cannot hold the data for longer.

C. Centrality Measures

The positioning of the nodes inside the network is termed "centrality." The features that describe the individual characteristics of the position in the network are degree (how connected it is?), clustering (how clustered its friends are?),
distance to other nodes and the centrality, influence, power, etc.

1) Betweenness Centrality: Betweenness centrality [28] measures the number of times a node lies on the shortest path between other nodes. Its roles as an intermediary, connector between the nodes. It is the shortest path that lies between two nodes along with the intermediate node. It is a measure of how often a node is a bridge between other nodes, as shown in equation 1.

$$Cb(k) = \sum\left(\frac{Pk(i,j)}{P(i,j)}\right) \quad (1)$$

where,

Pk (i, j) - Number of the shortest path between i, j and that pass through node k.

P (i, j) - Number of shortest path between i and j.

Nodes with high betweenness centrality are often important controllers of power or information.

2) Closeness Centrality: A node is said to be closer with respect to all of the other nodes within a network. Closeness
centrality [29] is the ease of reaching to other nodes and scales directly by calculating the relative distance to other nodes. It is the average length of the shortest path between the node and all other nodes, as shown in equation 2.

$$Cc(v) = \frac{N-1}{\sum d(i,j)} \quad (2)$$

where,

d (i; j) - gives the shortest path between node I and node j across all nodes and how far it is from other nodes.

N - Number of nodes.

The node with the highest closeness centrality is the closest one to all other nodes.

3) Eccentricity: The eccentricity of a node n [30] is the maximum distance to any node from a node n. A node is more central in the network, if it is less eccentric. Formally, the eccentricity can be given as in equation 3

$$e(v) = \max\ (v, a) \quad (3)$$

where

d (va); Vb) represents the distance between node va and vb.

A centrality measure based on eccentricity is given in equation 4.

$$E(v) = \frac{1}{e(v)}$$

IV. OSNQSC MODEL

OSNQSC architecture has two entities, as shown in fig 3 i.e., the cloud and the user. The user who wants to upload the data safely in the cloud. The cloud is the one that provides storage services to the user. First, the user has to register to authenticate themselves with the cloud. Then the user sends the file to be stored in the cloud. Upon receiving the data, the cloud divides the file into number of fragments using the SPLIT Method. Along with this, nodes are deployed in the cloud using T-coloring Placement process. Then the nodes should be selected to store the file fragment's using Betweenness centrality, eccentricity, Closeness centrality methods and the proposed optimized method. The fragments of the optimized method are encrypted and then uploaded it to the cloud.

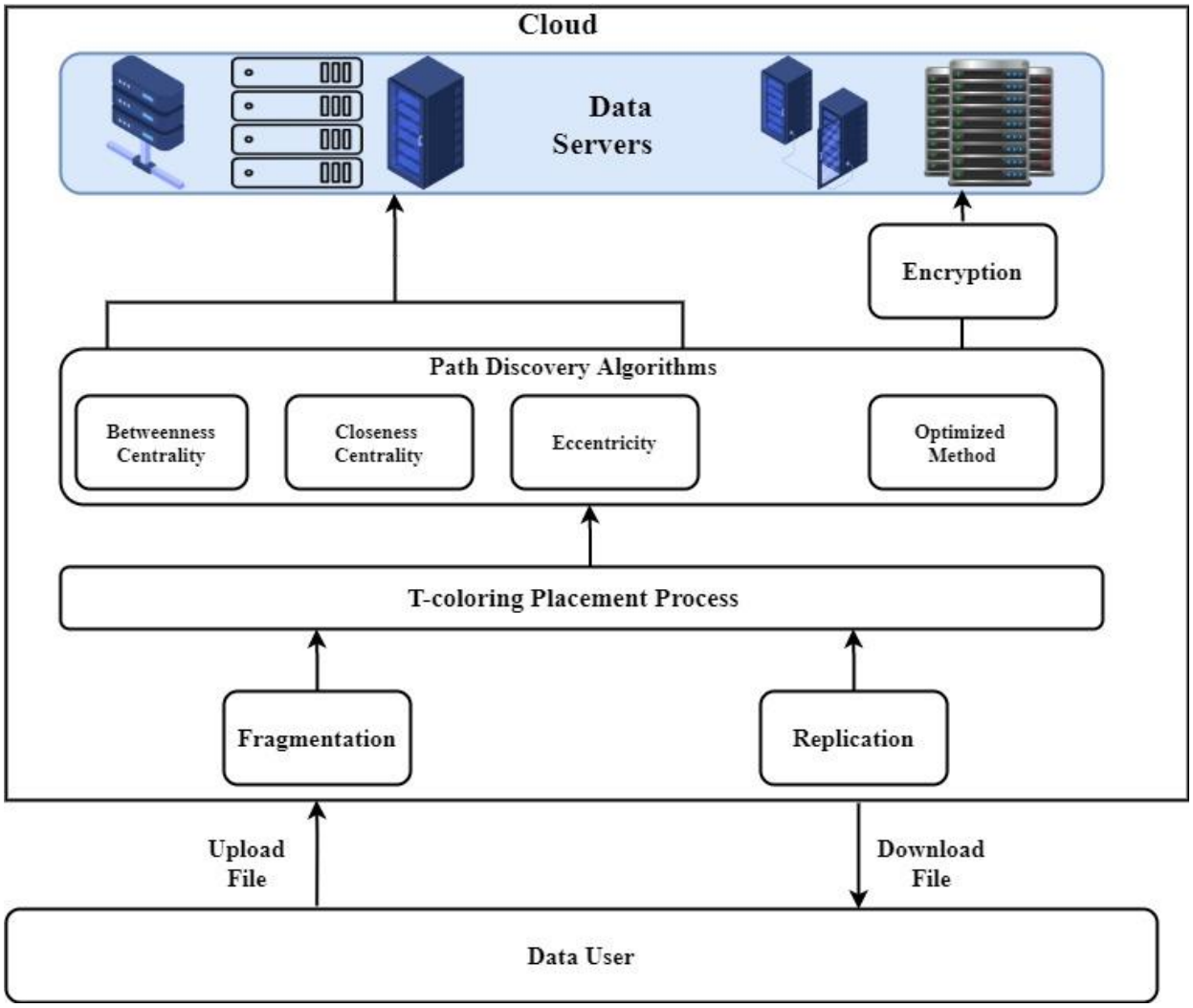

Fig. 3: OSNQSC Architecture

A. Data Fragmentation and Replication

The security of large-scale systems [25], such as cloud, depends on the security of the system as a whole and the security of individual ISPs. Data fragmentation [26] defined as breaking the data into multiple pieces to efficiently use the storage space and stored in memory. The importance of fragmentation depends on the specific storage allocation system. The file that is uploaded by the user should be in pdf format. The file is divided into multiple pages and stored in FIFO Queue. Each page is futher divided into a set of single sentences using the SPLITTER method. The dot operator uses the dot (.) symbol where the sentences end as the single fragment. Along with fragments, the fragments are replicated [27] in order to enhance the availability of the data and placed in another set of ISPs in the network.

B. T-coloring Placement Process

T-coloring is responsible for placing the ISP in a region of bounded limits on the cloud. Each ISP will have its own unique location. The location of two the ISPs cannot be the same as well. Fig 4 shows an example of how ISPs are positioned for a set of iterations. The ISP location can change for each iteration, and each iteration position is presented in different colors for all 25 ISPs within the boundary range of 25*25 and the same is depicted in Fig 4.

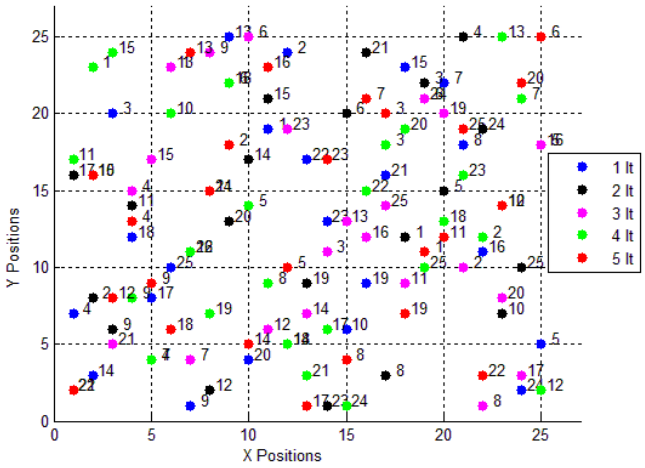

Fig. 4: Position of ISPs for the set of Iterations

TABLE I: T-Color Placement Process

Input: N_{ISP} , ha_{start}, ha_{end}, va_{start}, va_{end}.
Output: T-coloring Placement Matrix TCPM.

begin

Step 1: Initialize l = 1, l = 1-> N_{ISP} .

Step 2: Find the first dimension for the ISP in the area under coverage ha_{start}, ha_{end}. The dimension must satisfy the condition.

$ha_i = ha_v$ for any ha_v which satisfies

$ha_{start} \leq ha_v \leq ha_{stop}$ and $ha_v \neq ha_{ah}$

Step 3: Find the second dimension for the ISP in the area under coverage va_{start}, va_{end}. The dimension must satisfy the condition.

$va_i = va_v$ for any va_v which satisfies

$va_{start} \leq va_v \leq va_{stop}$ and $va_v \neq va_h$.

Step 4: The complete set is formed using (I; (ha_i; va_i)).

Step 5: Save the Ith data of Matrix as shown in Table II.

Step 6: l = l + 1

Table I shows the algorithm of T-color Placement Process of Node position in which ISP are distributed within the cloud by taking the number of nodes NISP required to deploy in the cloud, minimum x position, maximum x position, minimum y position and maximum y position. Position of node is generated randomly between xmin to xmax and ymin to ymax and information is stored in (i; xpos; ypos) until all the nodes are placed in the network.

TABLE II: Node position

Node	Position
i	(ha_i, va_i)

C. Path Discovery Algorithms

In order to place the fragments of the file, best ISPs should be selected in the network based on the following path discovery algorithms, such as Betweenness Centrality, Closeness Centrality, Eccentricity, and Optimized method.

1) Optimized method: The optimized method is responsible in finding the best nodes to place the fragments of the file. This method flows in a different phases.

Multiple Path Formation Phase: This phase will first find the initiators from which the path formation can be triggered and maintained. The number of paths formed will be equal to the number of initiators. From each initiator to the destination ISP, the path is formed after that the actual source ISP will be appended. The multiple-path formation algorithms is summarized in Table III. The cover ISPs are the set of ISPs within the transmission range. The step d is an indication of having the Individual Path Method for the single path formation and can find the optimization value based ISP along the path is summarized in Table IV. Each of the path is found by making use of individual path find method.

TABLE III: Multiple Path Optimized Method

Input: **Ncovernodes, covernodeset, transrange, source ISP and Destination ISP.**
Output: Multiple path traces between source ISP and destination ISP.

begin
Step 1: Initialize l = 1, l = 1-> NISP .
Step 2: Pick the lth cover ISP from covernodeset.
Step 3: Find the path between the lth cover node to the destination ISP using Individual Path Optimized Method.
Step 4: Append the actual path.
Step 5: Find the overall optimization value for the path.
Step 6: Repeat the process until paths have been found.
end

TABLE IV: Individual Path Optimized Method

Input: Source ISP, Destination ISP, Transmission Range, Energy Transmission, Energy Amplification, Distance between ISP, Environment Factor, Live period.
Output: Single path between source ISP and destination ISP.

begin
Step 1: The cover set ISPs for the source ISP are found out.
Step 2: Check whether destination ISP is present in cover set ISP, if yes the process is stopped.
Step 3: If the cover set of ISPs does not have the destination ISP, then channel quality is measured of all the cover set links.
Step 4: The link which has the highest channel quality is chosen as the next forward ISP.
Step 5: The ISP participating in the link undergoes the process of energy dissipation, and the battery level for participating ISPs will come down.
Step 6: The value of the live period is reduced by a factor of 1.
Step 7: Check the value of the live period and if it is not the same process of step 1 to step 7 is done until the destination is reached. If the live period reaches until zero, then the short path method is triggered as described in Table V.
end

The Multiple Path Formation is done by using each intermediate ISP as the source ISP. The cover set of ISPs from the source ISP are found. If the cover set has destination ISP, then the path is found. If cover set ISPs do not have the destination ISP, then channel quality is calculated as shown in equation 5 and 6.

$$\text{ChQua} = \left|\frac{\text{MeSignal}}{1.02} + 16.62\right| \quad (5)$$

where,

Me Signal - Measure Signal,
Ch Qua - Channel Quality Measure.

The Me Signal can be defined as follows

$$\text{MeSignal} = \frac{\frac{\text{Tp}}{\text{Pl}}}{\text{NoSbNf}}\ \text{GPM} \quad (6)$$

where,

TP - Transmission Power Measure,
PL - Path Loss,
No – $1{,}38*10^{-23}*290$,
SB - Signal Bandwidth,
NF - Noise Figure,
GPM - Gain power Measure.

Table V shows the algorithm that describes the shortest path among multiple paths. These multiple paths are generated from multiple path formation phase. If the cover set ISPs have the destination ISP, then the process is stopped. Suppose cover set does not contain destination ISP. In that case, the distance between links is measured with respect to destination, and the minimum distance is measured to find the next forward ISP is chosen, which corresponds to the lowest distance. The process is completed until the destination ISP is reached to get the path. After all the paths are formed, the path with the highest overall channel quality is chosen to store the data fragments.

D. Encryption

The encryption of the data fragments is done by generating the cipher and the secret key. The cipher will depend upon the file being encrypted along with the size of the file. The encryption is performed by converting data into bytes of binary data then XOR operation is performed between cipher, secret key, and data fragments. This process is repeated thrice
so that compression is achieved, and then data is stored on the ISPs present in the best path. The replication of file fragments is different on different ISPs. Energy Dissipation Method: The energy consumption in the T-color depends on the distance measure using ISPs, transmission value, and amplification value. The dissipation of energy is given by the equation 7,

$$\text{Edis} = 2 * \text{Edatatx} + \text{Egenvaldmdelta} \quad (7)$$

where,

Edis - Energy for dissipation of ISP.
Edatatx - Energy for data transmission.
dm - distance measure.
Delta - attenuation factor.

The ISP will lose its energy after participating in the path, and then the new energy level for ISP can be determined as shown in equation 8.

$$NEisp = O\ Eisp \square Edis \quad (8)$$

where,

N Eisp - new energy level for ISP.
O Eisp - Old energy level for ISP.
Edis - Energy for dissipation.

V. PERFORMANCE ANALYSIS

The performance metrics used while analysing the performance of the proposed method are:

1. Path Discovery Time: It is the time taken to discover the ISPs. The path will have the number of ISPs that takes the shortest path in the proposed method.
2. Hop Count: It is defined as the number of intermediate ISPs between the source and destination ISP.
3. Energy Consumed: It is defined as the energy utilized by the ISPs while discovering the ISPs.
4. Routing Overhead (RO): It is defined as the overhead that occurs while discovering the ISPs. The routing overhead is calculated using the equation 9.

$$RO = \frac{2*no\_of\_hops}{no\_of\_datafragments} \quad (9)$$

5. Total Upload Time: It is the total time taken to upload the file.
6. Total Download Time: It is the total time taken to download the file.
7. Throughput: It is calculated by taking the size of the file to the time taken to place the file.

This section describes the result analysis of the proposed method and compared it with existing methods. Table VI
shows the parameters that are considered for the analysis.

TABLE VI: Experimental Input

Name of the Input Parameter	Value
Number of Intelligent Sensing Point	50
Minimum one Dimension X end Point	1
Maximum one Dimension X end Point	100

Minimum one Dimension Y end Point	1
Maximum one Dimension Y end Point	100
Distance Measure between ISPs for Random Placement	25
Energy for all Intelligent Sensing Points	9999mj
Energy required for Transmission data	20mj
Energy required for Generation data	10mj
File uploads	10-500KB
Initiator Intelligent Sensing Point	2
Destination Intelligent Sensing Point	50

The Data user should authenticate himself by registering in cloud by using various fields. Two different users cannot have same email or username, otherwise registration will fail. The nodes are deployed in the cloud using Cloud Sim Simulator. These nodes are considered as Intelligent Sense Point. The registered user will initialize the ISPN, energy level initialization of all the algorithms, find the path between the initiator ISP and destination ISP. Store the data fragments across different ISPs, and download the file securely whenever required.

The performance of the OSNQSC method is compared with the existing DROPS [31] methods. The behaviour of the algorithms is studied by changing the file size between 10kb to 500kb with a constant number of ISP.

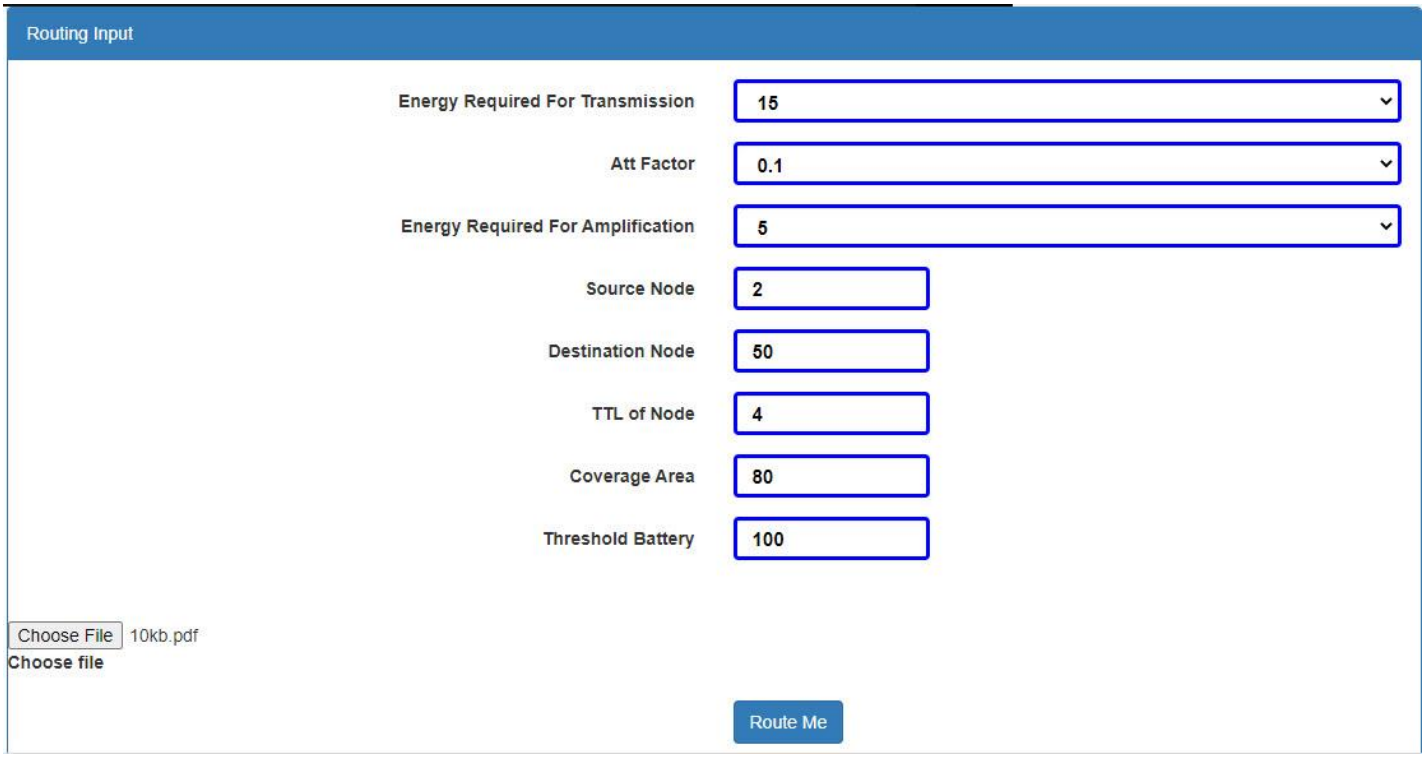

Fig. 5: Path Discovery Input

Fig 5 shows the screen-shot of the output where the inputs are given to find the paths of the ISP to store the fragments. The input is considered as the energy required for transmission, attenuation factor, the energy

required for amplification, source and destination node, TTL value, threshold battery, and the file to be uploaded.

OPTIMIZED	70BC8BB7A373C4B6872BD3C0...	Jeevitha	[2, 4, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48]
CLOSENESSCENTRALITY	70BC8BB7A373C4B6872BD3C0...	Jeevitha	[2, 8, 9, 6, 10, 7, 11, 14, 13, 4, 12, 5, 3, 1, 17, 18, 20, 16, 15]
BETWEENCENTRALITY	70BC8BB7A373C4B6872BD3C0...	Jeevitha	[2, 6, 7, 4, 1, 3, 5, 9, 12, 15, 14, 11, 10, 13, 17, 20, 18, 21, 24, 23, 26, 25, 28, 22, 19, 16, 8]
ECENTRALITY	70BC8BB7A373C4B6872BD3C0...	Jeevitha	[2, 6, 5, 3, 4, 1, 7, 8, 11, 9, 14, 15, 13, 17, 16, 20, 18, 12]

Fig. 6: Selection of ISPs by Path Discovery Algorithms

Fig 6 shows the selection of different ISPs by the path discovery algorithms and selecting the shortest path to ISP to place the files' fragments. Different ISPs are selected by the path discovery algorithms. OSNQSC uses the optimized method to select the ISP, which is depended on the energy level of each ISP along with the shortest method to discover the ISP. But the existing centrality methods concentrates only on the distance between the ISPs. Based on this, Fig 7 shows the time taken to discover the path of the ISPs and select the shortest path to place the fragments of the file. Different file placements will have different paths with different ISPs. Compared to DROPS [31] methods, OSNQSC takes much less time to discover the ISPs.

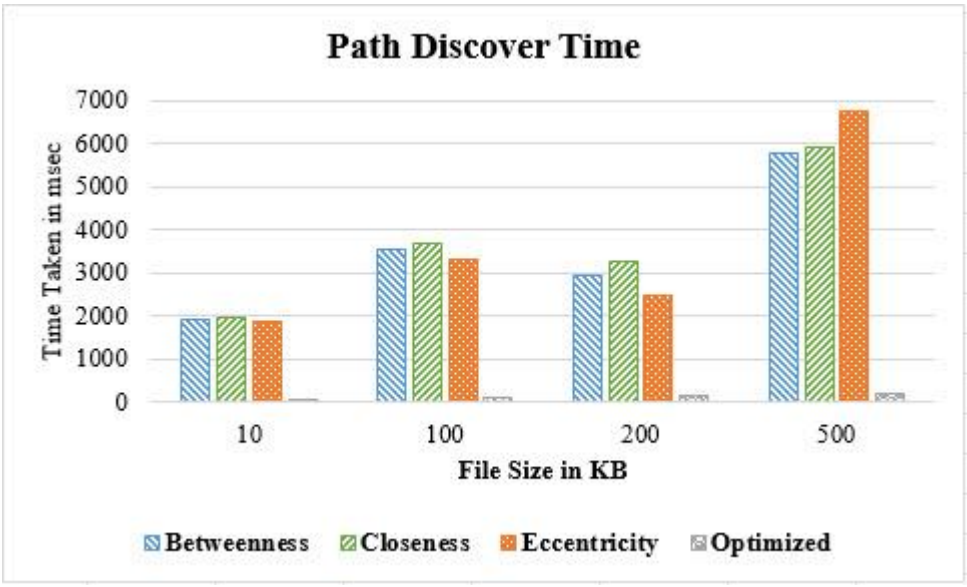

Fig. 7: Path Discovery Time

Fig 8 shows the comparison of hops count. Compared to existing methods of DROPS [31], OSNQSC takes much fewer hops because the existing centrality measures undergo back forth propagation to get the next storing ISP while discovering the intermediate ISPs in the network. Therefore, the existing algorithms may visit an already visited ISP in the
discovery process whereas, the proposed optimized method does not visit the ISP twice. Hence the existing method takes
much fewer hops compared to the existing method.

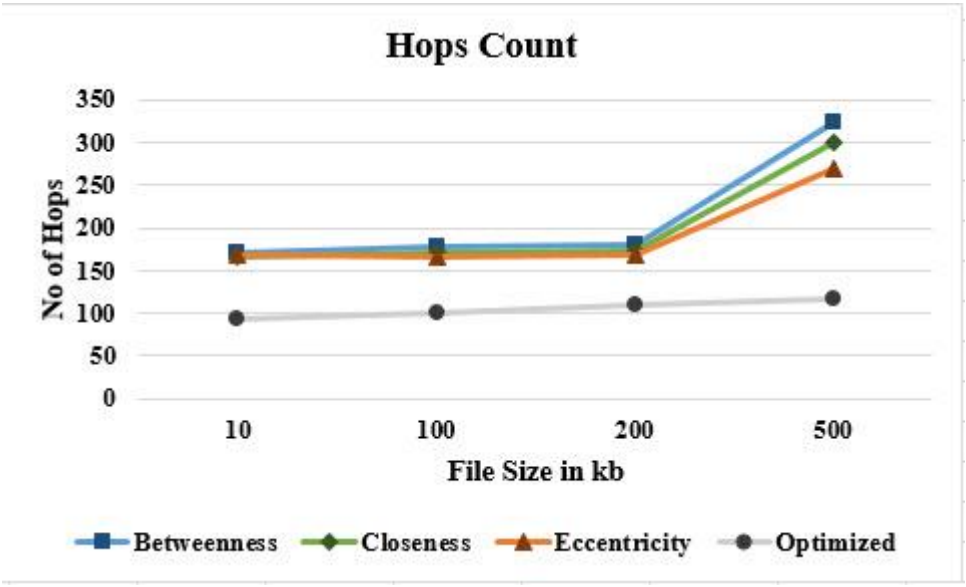

Fig. 8: Hops Count

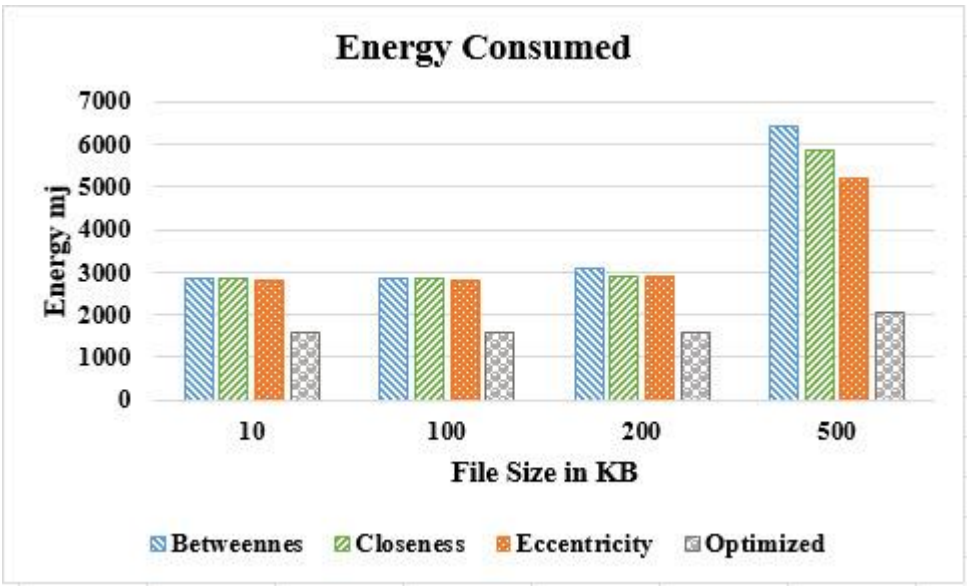

Fig. 9: Energy Consumed

Fig 9 shows the energy consumed to discover the ISP. It is the energy wasted while discovering the ISPs. The existing centrality measure repeats the already visited ISP to get the distance between all the ISPs. So it consumes more energy
during this back forth propagation. In contrast, the optimized method uses the ISPs based on the higher energy capacity
and less distance between initial ISP and destination ISP and won't visit the already visited ISP. The increase in number
of hops leads to energy consumption. Hence the proposed algorithm consumes less energy compared to the existing DROPS method.

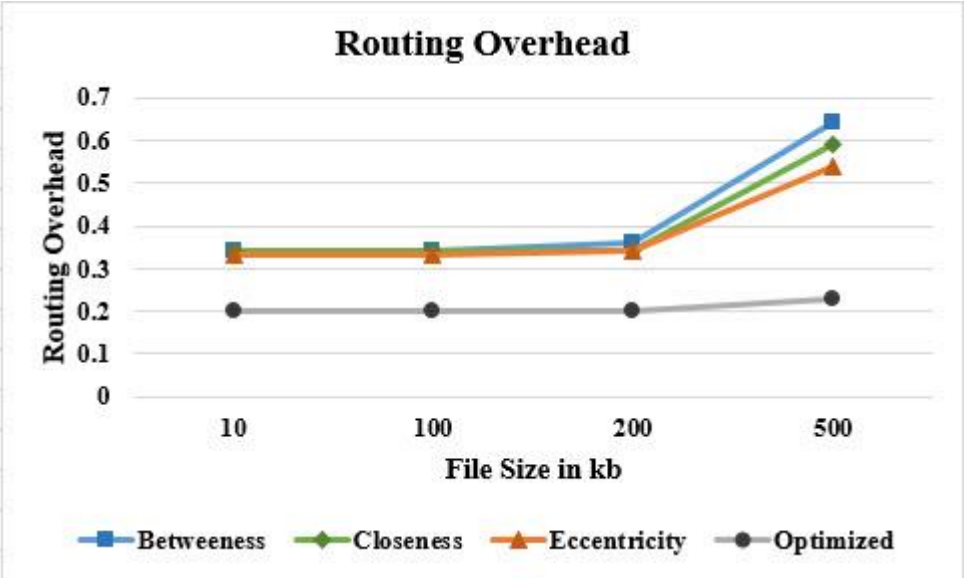

Fig. 10: Routing Overhead

Fig 10 shows the routing overhead that occurs while finding the ISP. The increase in the number of hops increases the energy consumption that leads to increase in overhead while selecting the ISPs as it depends on the efficiency in discovering the ISPs in the network. This intern results in wastage of bandwidth. Existing DROPS [31] methods use more bandwidth in terms of routing. Hence, the optimized method has less routing overhead than the DROPS methods.

TABLE VII: Comparison of Total Upload Time of Betweenness Centrality, Closeness Centrality, Eccentricity, and Optimized Method

Size in KB	Upload time in ms			
	Betweenness	Closeness	Ecentricity	Optimized
10	40177.13	40176.13	40178.13	40148.13
100	380240.86	380239.86	380241.85	379938.51
200	373558.18	373557.18	373559.18	373263.5
500	370120.75	370119.75	370121.75	369826.21

Fig. 11: Total Upload Time

Fig 11 shows the total time taken to upload a file. The graph is plotted based on the values, shown in Table VII. The total upload time includes ISP selection, file fragment time, placing fragments in choosen ISP, encrypting the fragments the file without any encryption. As the file size increases, the time taken to upload the file increases. The OSNQSC takes less time to discover the ISPs that intern results in less time to upload the file.

As per the graph, there is no much difference between all the algorithms. This is because of the encryption in the proposed OSNQSC method where the encrypted time is added along with the ISP discover time before uploading. Storage is utilized efficiently as the fragments are encrypted so that storage space consumed will be less compared to existing system, as shown in Table VIII.

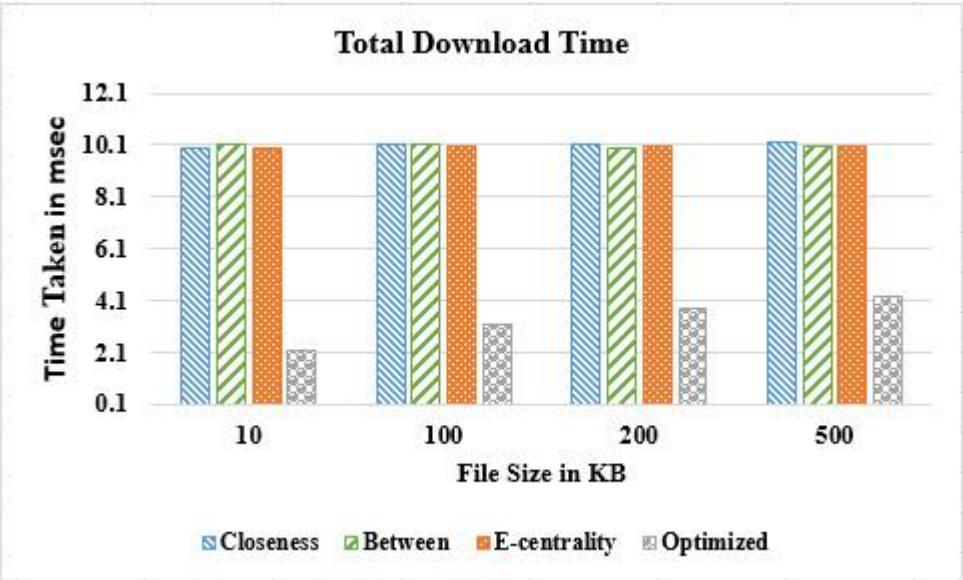

Fig. 12: Total Download Time

TABLE VIII: Comparison of File Size in Bytes

Existing System	Proposed System
10000	9335
100000	95388
200000	189770
500000	462564

Fig 12 shows the total time taken to download the file. The graph is plotted based on the values, shown in Table IX. The
total download time includes the time to retrieve the fragments from the ISPs, decrypt and download as a single file. As the file size increases, the time taken to download the file increases. OSNQSC takes less time compared to the existing DROPS methods.

TABLE XI: Comparison of Total Download Time of Betweenness Centrality, Closeness Centrality, Eccentricity, and Optimized Method

Size in KB	Download time in ms			
	Betweenness	Closeness	Ecentricity	Optimized
10	10.01	10.12	10.01	2.14
100	10.11	10.15	10.02	3.16
200	10.11	10.01	10.07	3.80
500	10.22	10.08	10.05	4.24

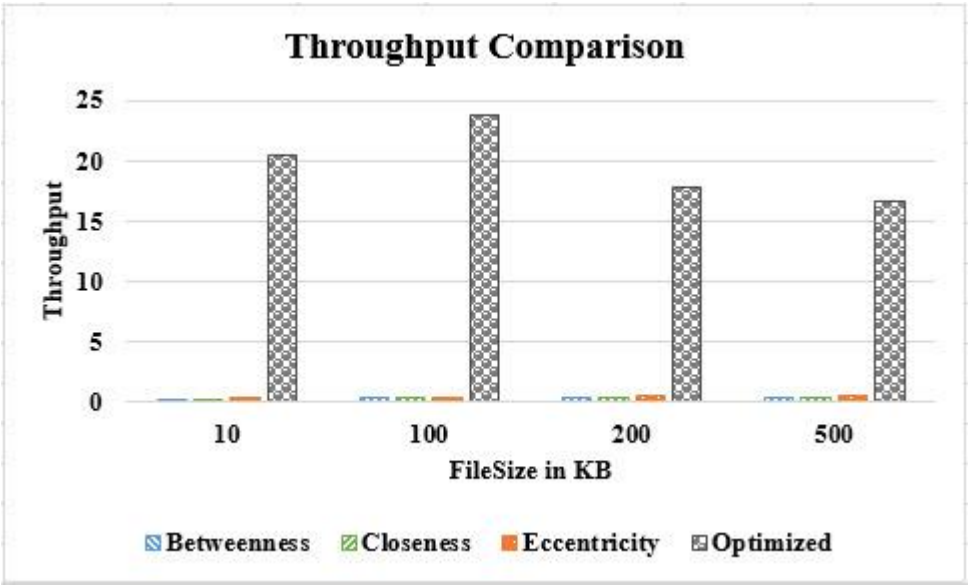

Fig. 13: Throughput Comparison

Fig 13 shows the comparison of the throughput of the path discovery algorithms. It is the time taken to store the file in the cloud. OSNQSC takes the best and shortest path ISPs to place the fragments of the file. Thus the proposed method takes much less time to upload the file that intern increases the throughput compared to the existing centrality measures.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, OSNQSC method is proposed, a cloud storage security scheme that collectively deals with securely storing the file by fragmented it into a number of fragments and stored on the best ISPs of the network. T-color method is used to deploy the ISPs randomly in cloud with the help of Cloud Sim. The ISPs are discovered by the path discovery algorithms of both existing and proposed methods, and best ISPs are selected. OSNQSC uses the encryption in order to provide double security along with dividing the file fragments. Due to this, even if a single ISP is attacked by the hacker, the data will not be revealed as the data is dividing and placed in different ISPs, which is deployed randomly in the cloud. The optimized method concentrates on both the distance and energy level of ISP whereas the existing methods concentrates only on the distance between the ISPs and do not think of energy levels of the ISPs. This helps to compare the performance of the existing Betweenness centrality, Closeness Centrality, and eccentricity of the DROPS methodology [31] with the proposed OSNQSC and efficient in terms of time, storage, throughput, and energy.

OSNQSC can be further improved by using of genetic algorithms to make the nodes sleep and then update energy levels so their overall lifetime can be maintained. The compression techniques can be used to further compress the file to achieve the storage. The data which is uploaded by the user is not shared with any other user so that sharing feature can also be added to share the file with authorized users.

REFERENCES

[1] Jeevitha B K, Thriveni J, and Venugopal K R, “Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey”, International
Journal of Computer Applications, vol. 156, issue. 12, pp. 16-27, December 2016.
[2] Keiko Hashizume1, David G Rosado, Eduardo Fern´andez-Medina, and Eduardo B Fernandez, “An Analysis of Security Issues for Cloud Computing”,
Journal of Internet Services and Applications, vol. 4, no. 5, 2013.
[3] L. M. Kaufman, “Data Security in the World of Cloud Computing,” IEEE Security and Privacy, vol. 7, no. 4, pp. 61-64. 2009.
[4] M. Hogan, F. Liu, A.Sokol, and J. Tong, “NIST Cloud Computing Standards Roadmap”, NIST Special Publication, July 2011.
[5] Michael D. Hogan, Fang Liu, Annie W. Sokol, and Tong Jin, “NIST Cloud Computing Standards Roadmap”, NIST Information technology and Computational science, August 2011.
[6] B. Grobauer, T.Walloschek, and E. Stocker, “Understanding Cloud Computing Vulnerabilities”, IEEE Security and Privacy, vol. 9, no. 2, pp. 50-57,
2011.
[7] A. Juels and A. Opera, “New Approaches to Security and Availability for Cloud Data”, Communications of the ACM, vol. 56, no. 2, pp. 64-73, 2013.
[8] Stefan Rass, and Peter Schartner, “Towards using Homomorphic Encryption for Cryptographic Access Control in Outsourced Data Processing”, Seventh International Conference on Cloud Computing, Grid and Virtualization, pp. 7-13. 2016.
[9] Conor McBay, Genard Parr and Sally McClean, “Energy Saving in Data Center Servers using Optimal Scheduling to Ensure QoS”, Seventh International Conference on Cloud Computing, Grid and Virtualization, pp. 57-60. 2016.
[10] Dzmitry Kliazovich, Pascal Bouvry and Samee Utiab Khan, “DENS: Data Center Energy-Efficient Network-Aware Scheduling”, Cluster Computing,

pp. 65-75, 2011.
[11] Shruthi Dadhich and Vibhakar Pathak, “An Approach to Optimal Strategy for Energy Efficiency in Cloud System”, International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 5, issue. 6, pp. 1097-1101, June 2017.
[12] K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, “Quantitative Comparisons of the State of the Art Data Center Architectures”, Concurrency and Computation: Practice and Experience, vol. 25, no. 12, pp. 1771-1783, 2013.
[13] Claudio Fiandrino, Dzmitry Kliazovich, Pascal Bouvry and Albert Y. Zomaya, “Performance Metrics for Data Center Communication Systems”, IEEE 8th International Conference on Cloud Computing, pp. 98-105, 2015.
[14] Kashif Bilal, Marc Manzano, Samee U. Khan, Eusebi Calle, Keqin Li, and Albert Y. Zomaya, “On the Characterization of the Structural Robustness
of Data Center Networks”, IEEE Transaction on Cloud Computing, vol. 1, no. 1, pp. 1-14, 2013.
[15] D. Boru, D Kliazovich, F. Granelli, P. Bouvry, and A. Y Zomaya, “Energy-efficient Data Replication in Cloud Computing”, IEEE Transaction on Cloud Computing, vol. 1, no. 1, pp.64-77, 2013.
[16] Sushanth Goel and Rajkumar Buyya, “Data Replication Strategies in Wide Area Distributed Systems”, pp. 1-27, http://www.cloudbus.org/papers/DataReplicationInDSChapter2006.pdf.
[17] Nicolas Bonvin, Thanasis G Papaiannou and Karl Aberer, “Dynamic Cost-Efficient Replication in Data Clouds”, ACM Workshop on Automated Control for Data Centers, June 2009.
[18] Mohammad Samadi Gharajeh, “A Dynamic Replication Mechanism in Data Grid based on a Weighted Priority-based Scheme”, i-manager’s Journal on Cloud Computing, vol. 6, no. 1, pp. 9-13, January - June 2019.
[19] Y. Deswarte, L. Blain, and J. Fabre, “Intrusion Tolerance in Distributed Computing Systems”, Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, pp. 110-121, May 1991.
[20] W.K. Hale, “Frequency assignment: Theory and applications”, Proceedings of the IEEE, vol. 68, no.12, pp. 1497-1514, December 1980.
[21] Wayne A. Jansen “Cloud hooks: Security and Privacy Issues in Cloud Computing”, 44th Hawaii International Conference on System Sciences,
pp. 1-10, Jan 2011.
[22] K. Subramanian and F. Leo John, “ Dynamic Data slicing in Multi Cloud Storage using Cryptographic Techniques”, World Congress on Computing
and COmmunication Technologies (WCCCT), pp. 159-161, 2017.
[23] http://www.cloudbus.org/cloudsim/
[24] Rodrigo N. Calheiros, Rajiv Ranjan, Cesar A. F. De Rose and Rajkumar Buyya, “Cloud Sim: A Novel Framework for Modeling and Simulation of Cloud Computing Infrastructure and Services”, Distributed, Parallel, and Cluster Computing, April 2009.
[25] Asma H. Al-Sanhani, Amira Hamdan, Ali B. Al-Thaher, and Ali Al-Dahoud, “A Comparative Analysis of Data Fragmentation in Distributed Database”, 8th International Conference on Information Technology (ICIT), pp. 724-729, May 2017.
[26] A. Suganya, R. Kalaiselvi, “Efficient Fragmentation and Allocation in Distributed Databases”, International Journal of Engineering Research and Technology, vol. 2, issue. 2, pp. 1-7, January 2013.
[27] Anca-Georgiana Fodor and Ion Lungu, “Implementation of Fragmentation and Replication Methods in Distributed Systems”, Journal of Information
Systems and Operations Management, pp. 373-383, 2016.

[28] https://towardsdatascience.com/graph-analytics-introduction-andconcepts-of-centrality-8f5543b55de3
[29] https://sites.google.com/site/networkanalysisacourse/schedule/anintroduction-to-centrality-measures
[30] Francis Bloch, Matthew O. Jackson, and Pietro Tebaldi, "Centrality Measures in Networks", Elsevier SSNR Publishing, June 2019.
[31] Mazhar Ali, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, and Albert Y. Zomaya, "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security", IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 303-315, April-June 2018.