

# An Enhanced Framework for Storage of Packets Securely on Cloud using Channel Quality Measure

Kannan A.  
Senior Professor  
Vellore Institute of Technology  
Vellore, India

Sukanya D.  
MTech Student  
Vellore Institute of Technology  
Vellore, India

Elakya K.  
MTech Student  
Vellore Institute of Technology  
Vellore, India

## ABSTRACT

The data which is outsourced is done based on cloud computing and there can be security reasons, the data can be compromised by performing attacks by other user and then among sensing points in the cloud. This project implements Optimized Centrality method which is energy efficient and also has good throughput. In the approach the sensing points are chosen based on residual energy and high channel quality, the sensing points which are not used in the path are then used for replication. The entire file is divided into fragments and then stored in the sensing points. The distance between the sensing points is computed by making use of T-color methods by making use of combination of (x,y). x is x position of the sensing point and y is y position of the sensing point. The proposed optimized centrality method is then compared against E-Centrality, Closeness Centrality and Between Centrality and then proved that proposed method is better with respect to delay, hops, energy consumption, efficient sensing points, in-efficient sensing points, security bytes' usage. The proposed also stores the packets by making use of DES method which is more secure as compared to AES used by compared methods.

## General Terms

Sensing point Deployment, Path Formation, Packet Division, AES, DES et. al.

## Keywords

Between Centrality, Closeness Centrality, E-Centrality, Sensing point Deployment

## 1. INTRODUCTION

The usage of information technology has been shifted to a better world with the help of cloud compute based service definitions like on-demand, network access from anywhere, distributed allocation of resources and pay as you go models. The use case can start from small enterprises to large organizations along with a minimum of individuals as well. The cost effectiveness of the cloud system is negated by security concerns existing in the application which the end implemented product must take care of. In order to keep the secure environment on the cloud all the entities involved in the complete process must be secured. When there are multiple entities and one of entity implements the high secure algorithm then the remaining entities are an easy target for an attacker to bypass and use the data through them. Hence distribution of packets across multiple sensing points in the cloud can be a better way to improve the security of the end to end application.

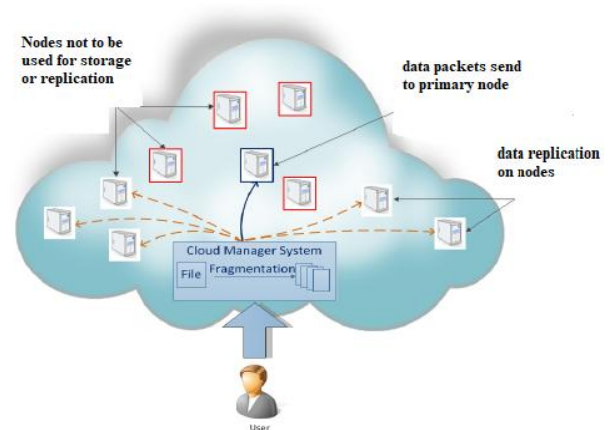


Fig 1: Architecture of the system

Fig1 shows the architecture of the system. The Cloud simulator allows the end users to model the cloud as the combination of multiple independent sensing points. Each sensing point having the responsibility for storage or replication of data. But sometimes the sensing points can be in-efficient to be used for either purposes. The data is first send to the primary sensing points which will take and then do the conversion of the entire packet into multiple independent fragments, after that the storage of the packets is done on the multiple sensing points based on certain criteria known as T-color distance or energy efficiency. Once the storage is done in order to increase the availability the data is also replicated on the efficient sensing points. The overall system decentralizes the data thereby improving the confidentiality of the packet. The Cloud manager maintains the trace of packet in the path as well as it will also store the information across the secure sensing points.

## 2. BACKGROUND

The number of interconnected servers are on a huge demand on a data center [1], but for the data center there is huge amount of cost as well as location based performance parameters involved which needs to be taken care of. The legacy systems cannot meet the bandwidth and trend factors. When the edges of a network are considered the bandwidth utilization is reduced to about 50%. there are various models which can be used at data center based on the use case which can be a legacy, switch based systems, packet delay optimized system. The Information and Computing Technology is an important block of cloud computing used in Data Center Network(DCN) [2]. The cloud framework will be used in multiple applications like agriculture, health based systems, research based search engine and analyzer along with data storage. The method will generate graph with multiple layers for different kind of DCNs, computation of failure modules

and generation of robustness metrics. The computing resource pool is provided as a service end point in cloud computing [3]. The communication between resources is hard in few use cases for the cloud based systems. In order overcome this challenge replication of packets is coming as a good technique. The advantage of using such system is delay improvement and bandwidth improvement. The method makes use of energy efficiency along with bandwidth as a metric for Quality of Service. The confidentiality, integrity and data availability are important for a cloud based system [4]. An intrusion aware approach is responsible to prevent any access which effects the three factors. The system will achieve this by using a checker which can give physical access to only part of the application. Different servers which have an additional layer of security which are intrusion resistant are used to generate and implement security blocks for web sites. The cloud computing has multiple flags which are sensitive in nature those are risk, threat and vulnerability [5]. The understanding and processing of the risk factor is important for handling the cloud related vulnerabilities and can make use of security based reference architecture. The combination of distance frequency measure with optimization [6] is used to avoid interference. Disk graphs technique with chromatic number along with assignment of frequency are used to obtain generic graph for the coloring problems. Cloud computing makes it easy for the information technology companies by reducing the cost of ownership [7]. It helps the end to end applications to assign dynamic storage and computing resources. The major concern for such systems is that of security. The combinations of multi-tenancy, dependency of layers along with elasticity is used to generate security aware cloud systems. The cyclones have features like bent back front, cloud head [8] which are separated from the main polar front. A hook is created which will surround warm air with the cold air. The important issues for the cloud based hook are security along with privacy. The cloud can be secured by making use of protective layer which will achieve high data availability [9] by making use of audit based system. The system will provide visibility on the operations performed by the tenant, run integrity and freshness checks on each operation. This will improve the trust level of the overall system. The distributed technology is used to have set of independent virtual machines [10] with each machine assigned to a specific customer. Silver line is a method which will provide isolation of data for cloud based system. The information will be propagated from files to processes and Amazon S3 will also follow the same approach. hierarchical along with filtering of data is performed by making use of policy.

### 3. PROPOSED SYSTEM

The proposed system has multiple services like registration, login, T-color sensing point placement method, multiple path formation, individual path formation based on channel quality, file upload, divide the file into fragments and distribution of file data into the sensing points in the best path along with replication of data on the efficient sensing points.

#### 3.1 T-Coloring Method Details

The T-Color method is responsible for placing the sensing points in the cloud system network. Number of Sensing points, Minimum x position, Maximum x position, Minimum y position & Maximum y position will act as an input, first we generate the Sensing point Id Starting with a value as '1'. Next the Generate of X position of Sensing points randomly between  $x_{min}$  to  $x_{max}$  is performed followed by Generate

of Y position of Sensing points randomly between  $y_{min}$  to  $y_{max}$ . The storage of the information in the format of a set  $(i, x_{pos}, y_{pos})$  The increment the Sensing point ID is performed and then process is repeated until all sensing points are placed in the network. The T-color method can be summarized in Fig2

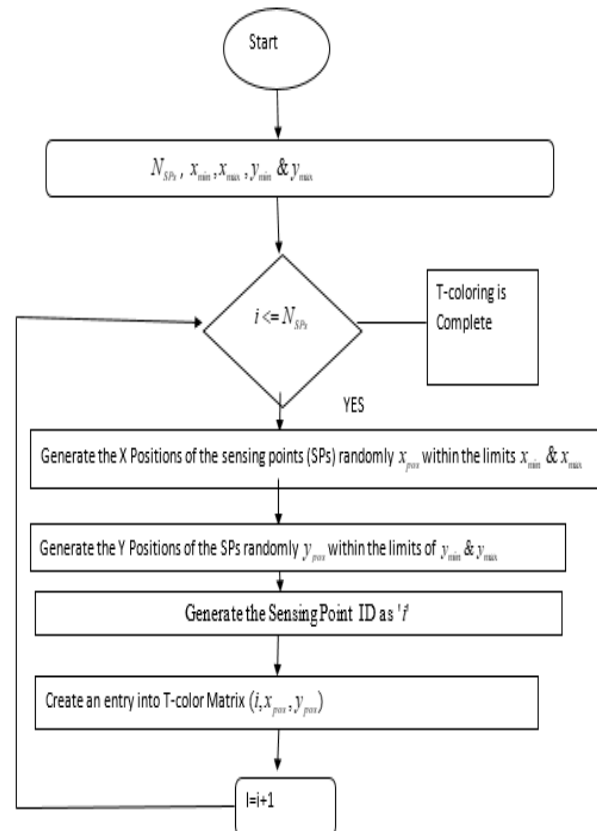
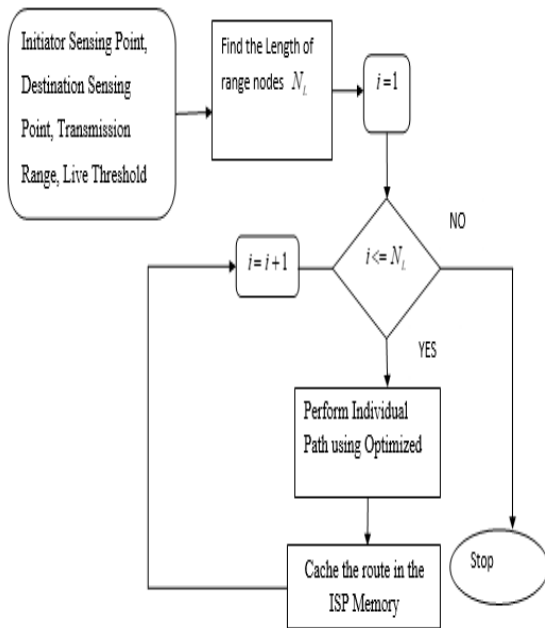


Fig 2: T-Color Method for Sensing Points (SPs) Placement

#### 3.2 Optimized Multi Path Method

The Optimized Multi Path Method is responsible for finding the multiple paths between the initiator sensing points (ISP) to the destination sensing point (DSP). The paths are also cached after each run into the ISP.

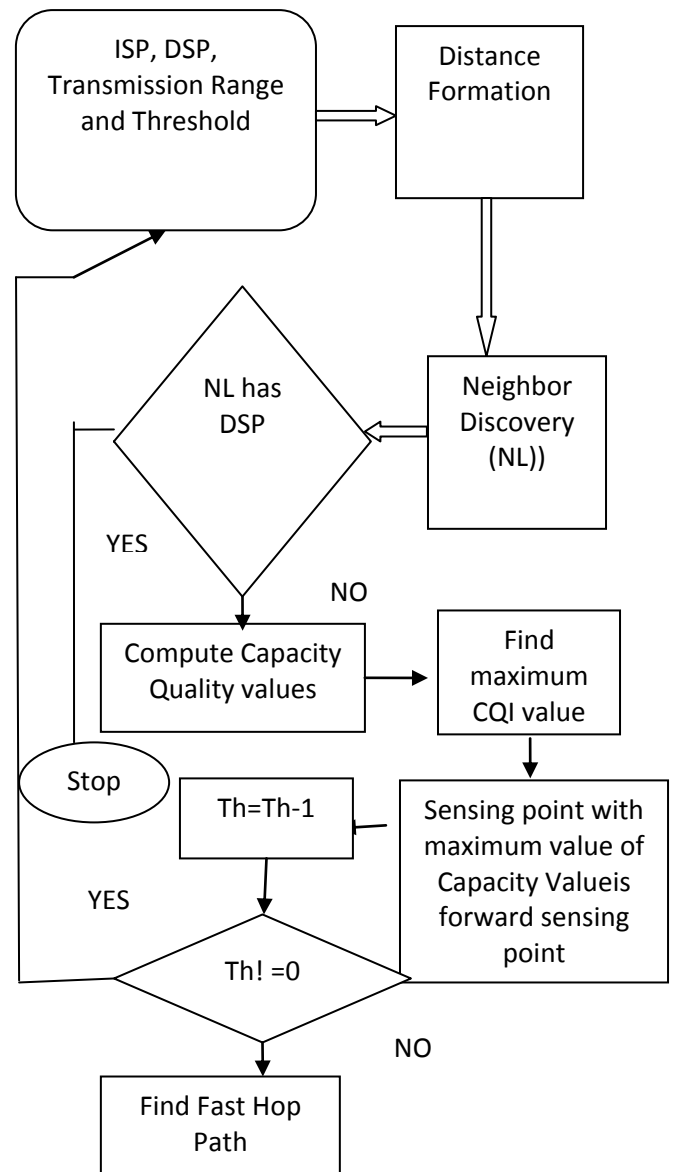


**Fig3: Multiple Path Formation using Optimized**

Fig 3 shows the multiple path formation using Optimized method. As shown in the fig initiator Sensing Point (ISP), Destination Sensing Point(DSP), Transmission Range and Threshold will act as input, Find the Neighbor Sensing points, Find the length of neighbor sensing points, start from the first sensing point till all the neighbor sensing points, Perform Individual Path Discovery using Optimized Method between ISP and DSP, Cache the path in the ISP and then repeat process until all paths are found.

### 3.3 Individual Path Formation using Optimized

The individual path formation is responsible for finding the end to end path between the ISP and DSP by making use of Channel Quality or a fast path once the threshold expires. Fig 4 shows the individual path formation using optimized Individual OPTIMIZED route discovery algorithm can be described in the fig4. The fig shows ISP, DSP, transmission range and Threshold acts as an input. The routing table is generated for all the sensing points in the network. The first step is to find the set of neighbor sensing points. If the neighbor sensing points have the DSP then the process is stopped. The second step is to compute the CAPACITY QUALITY values for all the neighbor sensing points. The third step is to find the maximum CAPACITY QUALITY value and the corresponding sensing point The fourth step is to compute value threshold period. if threshold value is non zero then process is repeated. If threshold is zero then find fast path hop algorithm is triggered.



**Fig4: Individual Path Formation using Optimized**

### 3.4 Fast Path using Optimized

The Fast Path Optimized is triggered in the middle of the path formation once the threshold expires so that DSP can be reached at a faster pace. Fig 5 shows the path optimized method. Initiator Sensing Point (ISP), Destination Sensing Point (DSP)& Transmission Range acts as an input. The neighbor sensing points are computed w.r.t ISP. If the neighbor sensing points have the DSP then stop the process. If the DSP is not present, then Compute the distance of each of the neighbor w.r.t destination. Find the sensing point which corresponds to minimum distance and then Repeat the process until destination is reached.

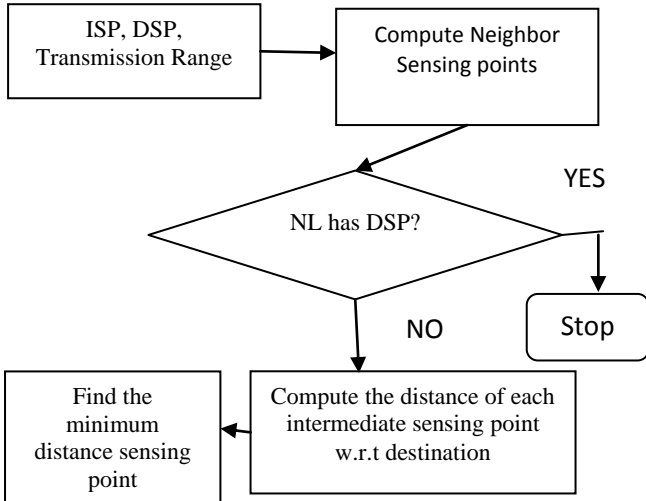


Fig4: Individual Path Formation using Optimized

### 3.5 Chunk Distribution Across Sensing points

The Chunk Distribution is responsible for distributing the file across multiple sensing points in the network. The Chunk Distribution can be described as follows - Divide the File into Pages, Find the Number of Pages in the document ,For each of the pages ,Execute the Split Method and then form statements and Each statement is a chunk of data .Note – Each chunks are distributed on different sensing points in a cyclic fashion

### 3.6 DES Encryption for the File Chunks

The DES Encryption is used for the file chunks before placing them on the sensing points in the cloud network. The file chunk is encrypted in a simultaneously fashion. The entire chunk is divided into blocks with each block size as 64 bit. The encryption is performed by making use of secret key and cipher text with the help of permutation and substitution combination. The process is repeated for about 16 rounds; the cipher block of next chunk is also dependent on previous block chunk.

### 3.7 Best Path Selection Optimized

The best path selection for the optimized method will be done based on the channel quality of the path which depends upon the residual energy of the sensing points, path loss and Signal to Noise Ratio (SNR).

## 4. EXISTING METHODS

This section describes the existing methods which are used for comparison with the proposed optimized method.

### 4.1 Between Centrality Method

The network containing set of sensing points and the data can be distributed between ISP and DSP. The between centrality will find multiple paths based on rules and then picks the best path which has the lowest between centrality distance. The number of rules will depend upon the number of sensing points which are present within the transmission range. After finding the multiple paths the best path is chosen as the path which has the lowest value of between centrality distance. The between centrality distance can be defined as below

$$BC_{distance} = \frac{path\ size}{nodes\ distance\ within\ path} \quad (1)$$

### 4.2 Closeness Centrality Method

The closeness centrality method will find the multiple paths by using the same process as that of between centrality. The selection of the best path will be done based on a different distance measure described as below

$$CC_{distance} = \frac{totalNetworkNodes - 1}{nodes\ distance\ within\ path} \quad (2)$$

### 4.3 E- Centrality Method

The E-Centrality Method will find the paths in a similar fashion as that of Closeness Centrality but is optimized in nature because the number of paths found are less due to selection of only one hop sensing points. The E-Centrality will find the best path based on distance between sensing points within the path

$$EC(d) = \sum_{i=1}^{Nnodes} d(i) \quad (3)$$

## 5. RESULTS

This section will describe the results of the proposed optimized method and also compares with several existing methods like between centrality, closeness centrality and E-centrality.

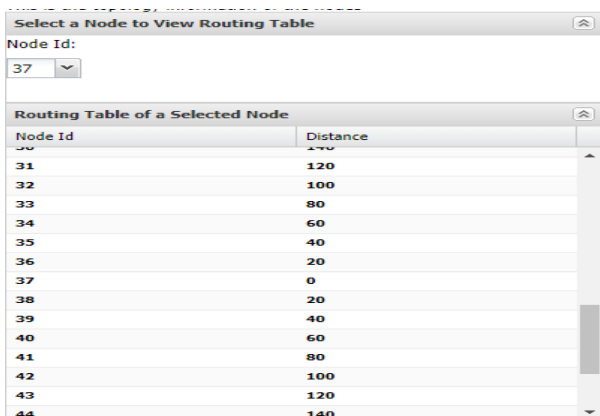
Table1: Experimental Input

Parameter Name	Parameter Value
Number of Sensing points`	50
Minimum X end point	1
Maximum X end point	99
Minimum Y end point	1
Maximum Y end point	99
Distance between sensing points	20
Energy for Sensing points	9999 mJ
Energy Required for Transmission	20 mJ
Energy Required for Generation	10 mJ
Attenuation Factor	10
File Uploaded	2MB
Initiator Sensing Point	2
Destination Sensing Point	50

Topology					
Node Id	X Coordinate	Optimized Algo Energy	E Centrality Algo Energy	Between Centrality Algo Energy	Closeness Centrality Algo Energy
1	0	9999	9999	9999	9999
2	20	9999	9999	9999	9999
3	40	9999	9999	9999	9999
4	60	9999	9999	9999	9999
5	80	9999	9999	9999	9999
6	100	9999	9999	9999	9999
7	120	9999	9999	9999	9999
8	140	9999	9999	9999	9999
9	160	9999	9999	9999	9999
10	180	9999	9999	9999	9999

**Fig5: T-Color Sensing point Placement**

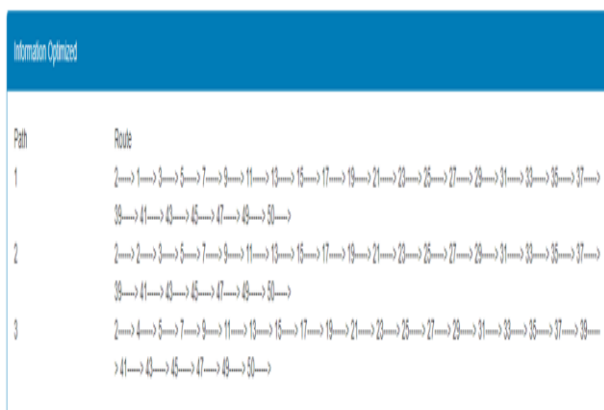
Fig 5 shows the sensing point placement for a linear topology based T-Color method. As shown in the fig the first column is the sensing point id, the second column is the distance of the sensing point with respect to reference point, from third column till the sixth column all values are 9999 mJ which is the battery initial assigned to the sensing points across all the four algorithms. This is a partial snap of the results showing 10 sensing points but the actual experimental result has 50 sensing points information.



Node Id	Distance
31	120
32	100
33	80
34	60
35	40
36	20
37	0
38	20
39	40
40	60
41	80
42	100
43	120
44	140

**Fig 6: Distance Sensing points Computation**

Fig 6 shows the distance between the sensing point 37 to every other sensing point in the network. As shown in the Fig the 37 SP is having a distance of zero with respect to itself and has a distance of 20m with respect to 36 SP and 38 SP



**Fig7: Possible Paths between ISP and DSP**

Fig 7 shows the possible paths between ISP and DSP. As shown in the fig there are three possible paths from the Sensing point2 to destination Sensing point 50 found out by making use of optimized method.

Best Information - Optimized

Best Route

2->4->5->7->9->11->13->15->17->19->21->23->25->27->29->31->33->35->37->39->41->43->45->47->49->50->

Best CQI

**160.2645021983676**

**Fig8: Best Route Optimized**

Fig8 shows the best route for the optimized method and the respective Channel Quality indicator value of 160.264. Among the three paths present in Fig7 the one best path is chosen which is having high CQI value.

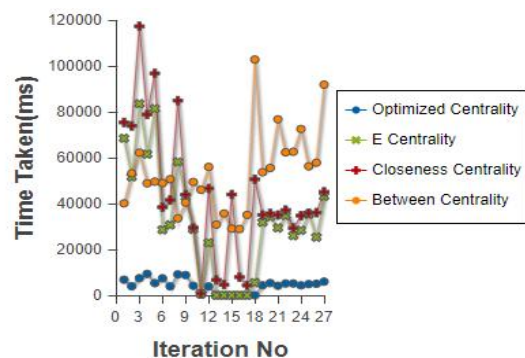
Time Taken (ms)	Total Hops	Energy Consumed	No Of Alive Nodes
21934.0	80	1803.3244855574749	35

Remaining Energy	Routing Overhead	Throughput
207668.97395527447	0.16	0.045591319412783805

**Fig 9: Measure of Parameters**

The various parameters after the execution of optimized method are described as above. The first parameter is the delay in ms with a value of 21934, the total hops across all paths found is 80, the total energy consumed is around 1803.324 mJ, The number of alive sensing points will be 35, the total remaining energy of the entire network is 207668, routing overhead value is around 0.16 and then has a throughput of 45 percent.



**Fig 10: Time Taken Comparison**

Fig 10 shows the time taken comparison between the various methods. As shown in the fig 10 Optimized Centrality has the lowest time taken as compared to E-Centrality, Closeness Centrality and Closeness Centrality. The comparison is made by repeating the experiment for the period of 27 iterations. The time taken is the time it takes for the path formation between the ISP to DSP and storage of packets in the sensing points along the path.

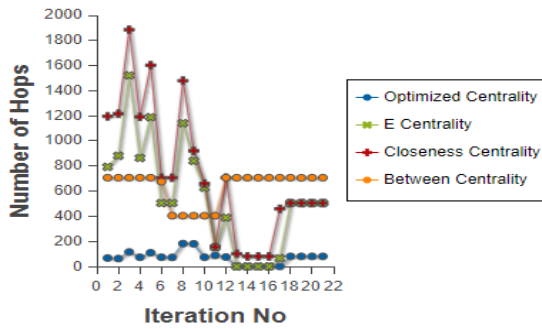


Fig 11: Number of Hops Comparison

Fig 11 shows the comparison of number of hops. The Optimized Centrality method has the lowest number of hops across all the paths found out under each iteration. As shown in the fig Optimized Centrality has the lowest hops compared to other methods.

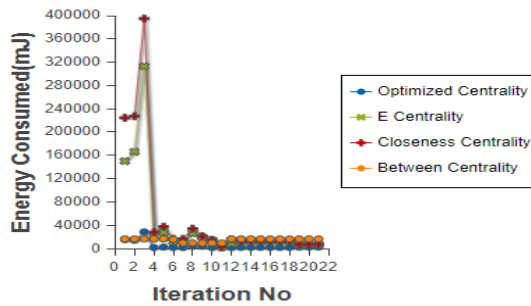


Fig 12: Energy Consumed Comparison

Fig 12 shows the energy consumed for the various algorithms. As shown in the fig the Optimized Centrality method has the lowest energy consumption as compared to other methods. The highest is for closeness centrality, then for between centrality followed by E-centrality with the least being Optimized Centrality.

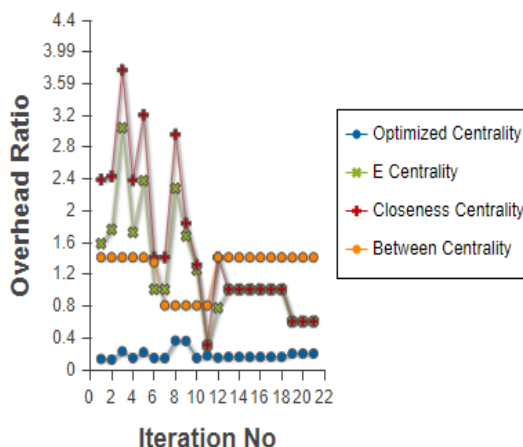


Fig 13: Overhead Ratio Comparison

Fig 13 shows the overhead ratio comparison. The overhead is

defined as the ratio of number of control packets to the number of data packets the lower the overhead ratio the better is the algorithm. As shown in the fig 13 the optimized method is having the lowest overhead as compared to other methods.

## 6. CONCLUSION

In this work the sensing points spread on an area using cloud sim, the distances between sensing points are computed. T-Color paths algorithms namely Closeness Centrality, E-Centrality, Between Centrality and optimized method. Once the paths are found the entire data file is divided into chunks and then spread across the best path among multiple paths of T-Color Algorithms. Also the data chunks are provided to other sensing points in the network map for replica purpose. The algorithms are also compared with respect to delay, hops, energy consumption, routing overhead and throughput.

## 7. REFERENCES

- [1] 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, 2013, pp. 1771-1783.
- [2] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," *IEEE Transactions on Cloud Computing*, Vol. 1, No. 1, 2013, pp. 64-77.
- [3] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," In *IEEE Globecom Workshops*, 2013, pp. 446-451.
- [4] Y. Deswarte, L. Blain, and J-C. Fabre, "Intrusion tolerance in distributed computing systems," In *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland CA, pp. 110-121, 1991.
- [5] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," *IEEE Security and Privacy*, Vol.9, No. 2, 2011, pp. 50-57.
- [6] W. K. Hale, "Frequency assignment: Theory and applications," *Proceedings of the IEEE*, Vol. 68, No. 12, 1980, pp. 1497-1514.
- [7] K. Hashizume, D. G. Rosado, E. Fernandez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, Vol. 4, No. 1, 2013, pp. 1-13.
- [8] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," In *44th Hawaii IEEE International Conference on System Sciences (HICSS)*, 2011, pp. 1-10.
- [9] A. Juels and A. Opera, "New approaches to security and availability for cloud data," *Communications of the ACM*, Vol.56, No. 2, 2013, pp. 64-73.
- [10] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, "Dike: Virtualization-aware Access Control for Multitenant Filesystems," University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.