Available online at: http://www.ijmtst.com/vol5issue10.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 05, Issue No: 10, October 2019

Data Transmission in Clouds using Heed and Energy Efficient Routing Algorithm

Abhinash Singla | Renu Nagpal | Yogesh kumar

Assistant Professor ,Computer Science and Engineering Department, BGIET Sangrur, Punjab, India

To Cite this Article

Abhinash Singla, Renu Nagpal and Yogesh kumar, "Data Transmission in Clouds using Heed and Energy Efficient Routing Algorithm", *International Journal for Modern Trends in Science and Technology*, Vol. 05, Issue 10, October 2019, pp.-44-48.

DOI: https://doi.org/10.46501/IJMTST051008

Article Info

Received on 25-September-2019, Revised on 18-October-2019, Accepted on 25-October-2019, Published on 31-October-2019.

ABSTRACT

Cloud Computing is a field of computer science in which user can access resources remotely through browser .Cloud Computing increases the speed of accessing the services in very much less cost without actually deploy them. It decreases the time from implementing the software to actually deploy it. Cloud Computing users can access resources on demand. Cloud provides the on demand services, virtualization and open source. The data owner can stored and access the data from the cloud with the help of cloud service provider. In the large organizations the data which is stored on the cloud is accessed by the many users of the same organization. In such a case the problem of inconstancy may arise, because the unauthorized user can delete or modify the data. If the two persons are accessing the same data at same time, then read-write, write-read conflicts may arise. In this, I even have designed wireless clump rule with the assistance node degree, Stability issue, and weight and CH choice. In this work, there is data duplication and data redundancy problem that I have faced and some other problem are the network life time problem due to the redundancy and transmission energy is lost, so there is energy consumption problem. Due to these problems some other problems like scheduling problem.

KEYWORDS: *WSN, Cluster head, Energy, HEED, Nodes, Cloud , WSN, CH, routing and Hops*

I. INTRODUCTION

Cloud is accessed through the internet and internet is available everywhere. So anyone can access their information on cloud at any time and from anywhere. In traditional approach all the data of user would be stored at user's end but in cloud whole scenario is different. Data on cloud is stored on virtual servers and user does not know where the virtual servers exist. So the user don't need to be at the location where the data is stored. Cloud provider uses the in-house or external resources for providing services to users.[1]

Data security is important because it also have impact on service quality. Every day there is new challenge to the data security arises in cloud computing.[1]

As we know user's loss their control over the data once it is stored on cloud, so the traditional cryptographic methods for

encrypting the data could not be adopted. Each user stores the various kinds of data on cloud and

they expect that their data will be stored securely for the longer period of time, and to verify the correctness of data for such a long time is very tough
task. Cloud is not like that once the user stored the data and user will only need to access the data. In cloud users perform many operations on the data such as updating, deletion, append etc. [2] The data on cloud is updated after a certain time as the user needs to update it. So cloud needs to ensure the security of that dynamically updated data, this is the most important thing. Due to this feature traditional technique fails and need to find out new solutions.[1]

II.CRITICAL AREAS FOR CLOUD COMPUTING

This guide finds that there are many areas that need to be look after. As the Cloud Computing is the new model so that is cannot be fully secured with the traditional cryptography techniques. In Cloud Computing infrastructure there are six specific areas where substantial security is implemented by TCG specifications implemented software.

- **Securing data at rest**

The best way to secure the data at cloud provider is cryptography encryption. There is the law to secure data and to protect data at cloud provider in many countries such as U.S states and other countries. Hard drive companies now making the devices which can automatically encrypt the data stored on them by using the TCG's standards. These kind of devices has the encryption hardware build in them which automatically encrypt the dart and takes the minimal cost and performance impact. [2]

- **Securing Data in transit**

Encryption scheme can also be used when the data is transferred. It confirms that the data is going only there where the user wants it to go and the data is not modified in-between the transition. This provides the additional security check for the integrity of data. [2]

- **Authentication**

User authentication is major goal to be achieved at the first. Users can access the data on the basis of access control list maintained by cloud so that the unauthorized cannot access system. The main motive is to achieve it in very less cost. All the information of cloud can be accessed by any one at any time so the authentication and access control are major important terms.[2]

III.PROBLEM DEFINITION

The data owner can stored and access the data from the cloud with the help of cloud service provider. In the large organizations the data which is stored on the cloud is accessed by the many users of the same organization. In such a case the problem of inconstancy may arise, because the unauthorized user can delete or modify the data. If the two persons are accessing the same data at same time, then read-write, write-read conflicts may arise. The second problem is that, if the cloud service provider is the malicious then it can also modify or delete the user's data.. In the existing schemes such as "Third party is used to store the encrypted data using AES encryption algorithm ", "In this Third party is used to store the encrypted data using private and public key in RSA algorithm". AES has longer key. In such algorithms lot of data computations and time is required for setting up a secure data connection. It requires more computation keys and more round for communication as compare to DES. In this work, we will propose new algorithm with will require less computations and time for setting up a secure connection.

IV.METHODOLOGY

The major challenge of cloud data storage is the security. There are many security algorithms are present in the cloud. To provide security in cloud DES, AES these types of algorithms are required. AES is the algorithm which is used for security purposes. It has great hardware software speed. It has 128 bit size which is more than DES. But there are some issues in AES which are responsible for the security threat in cloud. AES has 128 bit key size so computation resources and time required for this process is also more as compare to other. If computations power are more than it consume more energy as compared to other security algorithm. So to overcome this problem a new security algorithm is required which provide more security than AES and consume less energy.

Proposed Algorithm

Cluster head Selection Input: No of Sensor nodes, Initial node energy, probability (p), No of rounds.
Output: Cluster heads, Clusters.

Start:

Step 1. The base station broadcasts Beacon packets.

Step 2. All Sensor node replies with residual energy and location.

Step 3. If network life time is not over then,

i. For first round, Cluster heads are randomly

selected.

ii. For rest of the rounds, Base station chooses p% of the nodes as Cluster heads having more residual energy.

Step 4. If a node is Cluster head then,

i. It broadcasts its Cluster head advertisement packet.

ii. All non-Cluster head nodes sends joining request packet to those cluster head, who's received signal strength is more.

Step 5. Assumption:

i. All nodes are fairly distributed for tier one and tier two.

ii. Nodes are static and not mobile.

iii. The initial energy for all nodes is same.

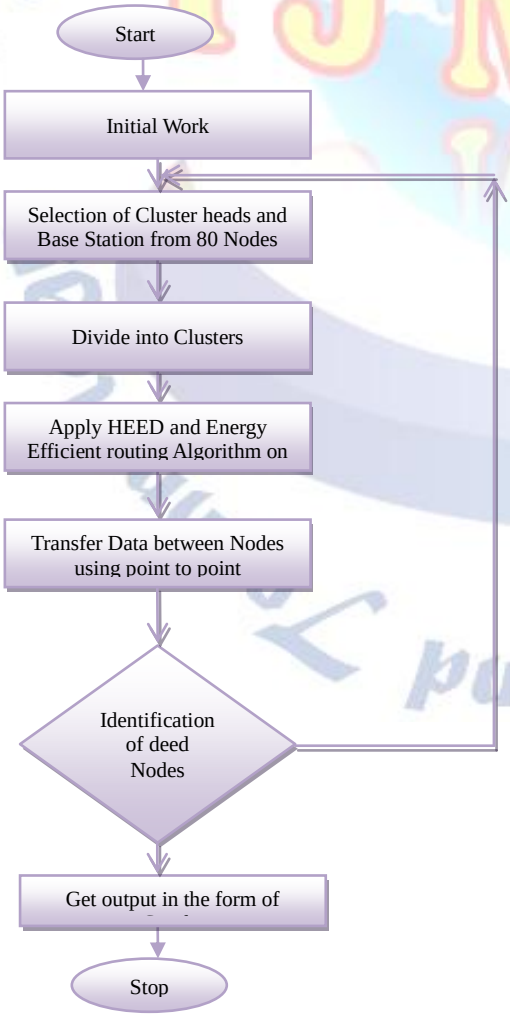
iv. The base station of this network is located at the Centre of the field.

Step 6. Node Distribution**:** The sensor nodes are distributed into tier one and tier two based on the area of circle formula as follows;

Area of big rectangle, ® = (2(l*b))

The base station is located in the center of the sensor network which the coordinate is (1000, 1000).

END



V.RESULT

In this paper different problems are resolved with the help of different snap shorts . These Snap shorts are given below along with grphs and Tables:

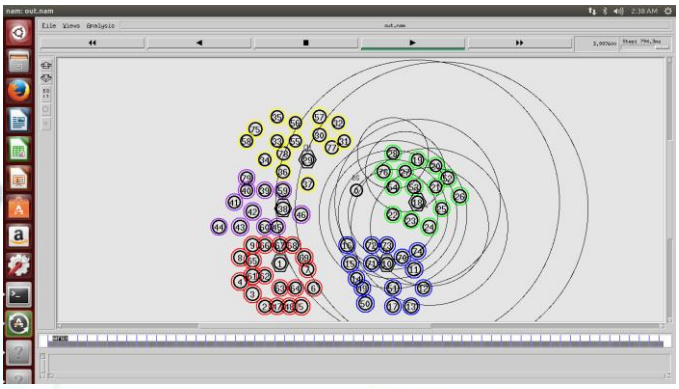


Figure 2: Node Signal Broadcasting on Network

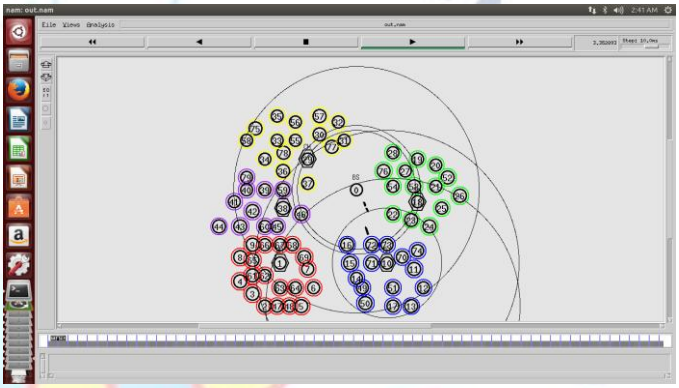


Figure 3: Data transfer between nodes

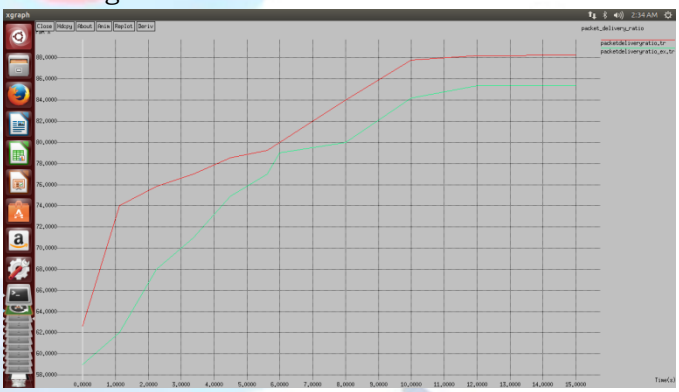


Figure 4: Packet Delivery ratio of existing and proposed work

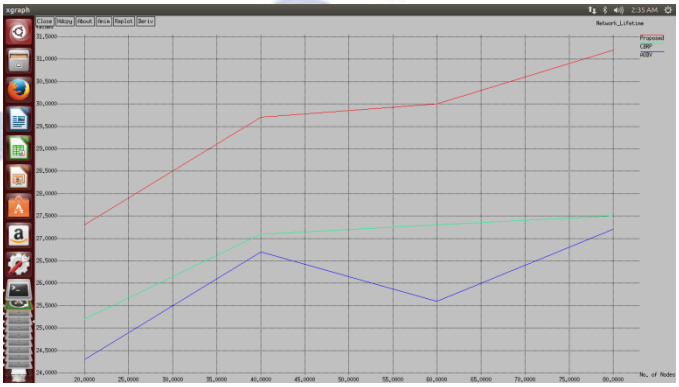


Figure 5: Network life time of existing and proposed work

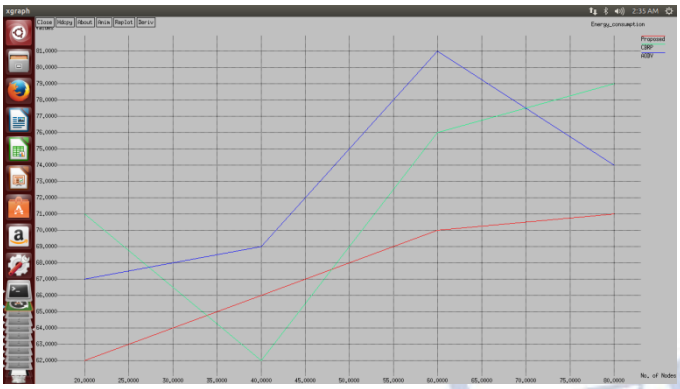


Figure 6: Energy Consumption of existing and proposed work

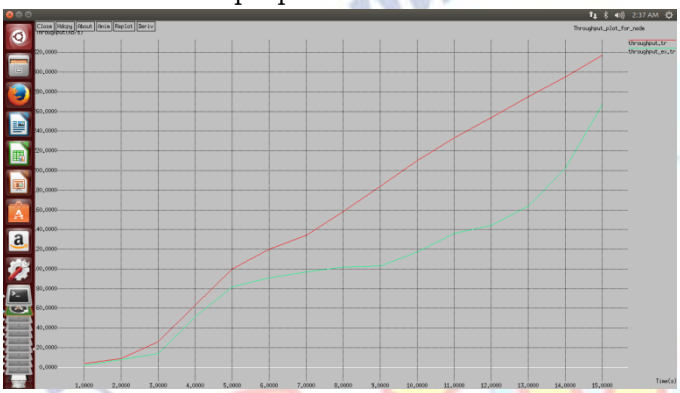


Figure 7: Throughput for Node of existing and proposed work

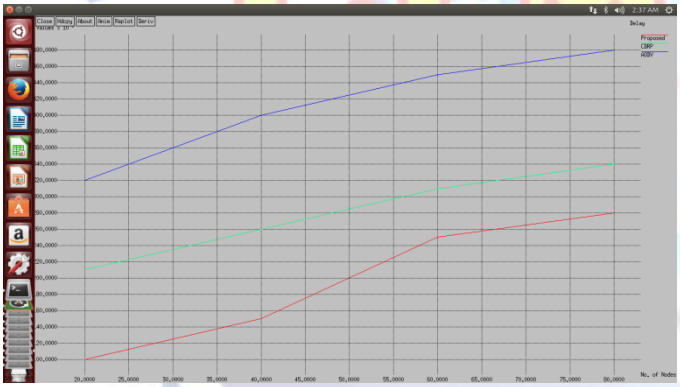


Figure 7: Delay of existing and proposed work

Table 1: Packet Delivery Ratio

Packet Delivery Ratio		
Time	**Existing**	**Proposed**
0	59	62.649
1	125.62	125.74
2	25.68	75.823
3	375.71	375.77
4	574.9	578.53
5	625.77	625.79
6	79	80
8	80	84
10	84.18	87.78
12	85.34	88.23
15	85.37	88.24

Table 2: End to End Delay

End to End Delay			
Time	**Existing**		**Proposed**
	CBRP	**AODV**	
20	0.21	0.32	0.10
40	0.26	0.40	0.15
60	0.31	0.45	0.25
80	0.34	0.48	0.28

Table 3: Network Life Time

End to End Delay			
Time	**Existing**		**Proposed**
	CBRP	**AODV**	
20	25.2	24.3	27.3
40	27.1	26.7	29.7
60	27.3	25.6	30.0
80	27.5	27.2	31.2

Table 4: Residual Energy

Residual Energy			
Time	**Existing**		**Proposed**
	CBRP	**AODV**	
20	71	67	72
40	62	69	66
60	76	81	80
80	79	74	85

VI.CONCLUSION

Clustering WSN have been research intensively in the previous decade because this technique can significantly decrease communication expenditure of the network nodes since the sensors only need to send data to the adjacent cluster-head. In HEED the associate nodes do not communicate directly with the base station. The CH collects data from the member nodes and ahead it to the base station thus restrictive the number of transmissions. The base station is the collection node for the entire WSN. The CH is selected according to following reasons: - 1) Residual Energy –The cluster heads are selected depending on the remaining energy levels. 2) The cost of intra cluster Communication –A node can come in the variety of multiple clusters, so the inclusion of node in the cluster will depend on the low intra cluster communication. Clustering is one of the significant methods to be applied in order to extend the network lifetime of

WSN. The existing protocols are not appropriate to those WSNs that are deployed in large regions because it uses single hop routing where each sensor node can communicate directly to the CH and the BS. So, it causes problems of energy imbalance. The problem of disturbed energy dissipation in the cluster based WSNs is investigated. In this, I even have designed wireless clump rule with the assistance node degree, Stability issue, and weight and CH choice. In this work, there is data duplication and data redundancy problem that I have faced and some other problem are the network life time problem due to the redundancy and transmission energy is lost, so there is energy consumption problem. Due to these problems some other problems like scheduling problem.

FUTURE WORK

The research work includes a new energy-efficient routing algorithm for the software-defined wireless sensor networks. In our routing algorithm, the control nodes are assigned different tasks dynamically. It is further implemented with the help of other intelligent types like Honey Bee and ACO with PSO to get the real time work.

REFERENCES

[1] Abhishek Parakh, Subhash Kak, (2009)"Online data storage using implicit security" Information Sciences 179 (2009) 3323–3331.

[2] Asad Amir Pirzada and Chris McDonald, "Kerberos Assisted Authentication in Mobile Ad-hoc Networks" School of Computer Science & Software Engineering, The University of Western Australia 35 Stirling Highway, Crawley, W.A. 6009, Australia.

[3] Andreas Hafslund and Jon Andersson, Thales Norway AS (2006), "2-Level Authentication Mechanism in an Internet", 6th Scandinavian Workshop on Wireless Ad-hoc Networks.

[4] Cong Wang ,(2011)" Ensuring Data Storage Security in Cloud Computing "Journal of RecentTechnology and Engineering (IJRTE).

[5] Cong Wang ,(2012)" Towards Secure and Dependable StorageServices in Cloud Computing" IEEE.

[6] Deyan Chen, (2012)"Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering.

[7] Dr Nashaat el-Khameesy (2012) "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems" Journal of Emerging Trends in Computing and Information Sciences.

[8] Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. International Journal of Information Security and Privacy (IJISP), 4(2), 36-48.

[9] John Harauz ,Lori M. Kaufman,Bruce Potter," Data Security in the World of Cloud Computing " IEEE Security and Privacy July 2009. pp. 61-64.

[10] Jinguang Han, (2013) "Identity-based data storage in cloud computing "University of Wollongong.

[11] K.Shirisha Reddy, Dr.M.Balaraju ,(2012)"An Integrated Approach of Data storage and Security in Cloud Computing "International Journal of Application or Innovation in Engineering & Management (IJAIEM).

[12] K.ValliMadhavi R.Tamilkodi Data Storage Security in Cloud Computing for Ensuring Effective and Flexible Distributed System - 2012 National Conference on Research Trends in Computer Science and Technology .

[13] Mehmet Kuzu (2012) "Efficient Similarity Search over Encrypted Data".

[14] Men Longand ,Chwan-Hwa, "Energy-efficient and intrusion-resilient authentication for ubiquitous access to factory floor information", Industrial Informatics, IEEE Transactions on Volume: 2 , Issue: 1 Page(s): 40 - 47 .

[15] NEELA, K. "A Survey on Security Issues and Vulnerabilities on Cloud Computing".

[16] N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam," An Implementation of RSA Algorithm in Google Cloud using Cloud SQL" , Research Journal of Applied Sciences, Engineering and Technology,4(19), October 01, 2012, ISSN: 2040-7467.

[17] N. Gohring, (2008) "Amazon's S3 down for several hours," Online a http://www.pcworld.com/businesscenter/ article/142549/amazons s3 down for several hours.html, .National Institute of Standards and Technology -Computer Security Division.

[18] Punyada M. Deshmukh1, Achyut S. Gughane2 (2012)"Maintaining File Storage Security in Cloud Computing" International Journal of Emerging Technology and Advanced Engineering.

[19] Qian Wang (2009) "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing".

[20] Rampal Singh, Sawan Kumar, Shani Kumar Agrahari(2012)"Ensuring Data Storage Security in Cloud Computing" IOSR Journal of Engineering.

[21] Rohit Maheshwari, (2012) Department of Computer Science, Kautilya Inst. Of Technology, International Journal of Recent Technology and Engineering (IJRTE)

[22] Simarjeet Kaur, (2012) "Cryptography and Encryption In Cloud Computing "VSRD-IJCSIT, Vol. 2 (3)242-249.

[23] Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks" Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL 61801.

[24] Steven M. Bellovin, "Limitations of the Kerberos, Authentication System", AT&T Bell Laboratories Michael Merritt – AT&T Bell Laboratories.

[25] Syam Kumar P,2011" An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6.