International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

Implementing Secure Transmission of Data in Cloud Using Safe Coloring

S. Kharthikeyan[1], S. Muthukumaraswamy[2], J. Nagasurya[3], G. Vijayabalaji[4], S. Vijayasuriya[5]

[1]Assistant Professor, Dept. of CSE, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India

[2,3,4,5]UG Student, Dept. of CSE, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India

ABSTRACT: Secure transmission of data in between sender and receiver is done through cloud using encryption techniques. Encryption requires a password to encrypt and decrypt the file. Therefore, we intend to securely transfer the data between nodes in cloud using safe coloring techniques. Safe coloring is simple way of labeling graph components such as vertices under some constraints. In a graph, no two adjacent vertices are colored with minimum number of colors. In safe coloring no key values are needed, it sends files through safe colored nodes. It is more efficient and secure than existing system. Secret sharing is a way of securing a secret from a number of attackers by dividing it into parts and then distributing those parts to some persons, represented here by graph vertices. The user uploads the folder in the cloud. The nodes are initialized when the folder in uploaded in the cloud and a network is created. The receiver downloads the folder and split the data and distributed files over series of safe nodes and collectively receive files from the colored nodes. From this project, we hope to securely transfer the data using nodes in cloud from hackers.

KEYWORDS: Graph Theory, Safe coloring,Secret sharing, Data Security.

I. INTRODUCTION

Graph colorings are a well-known subject in graph theory.A graph coloring is a function which assigns a color to every vertex or edge of the graph, hence vertex colorings and edge colorings. Mostly the goal is to determine a minimal number of colors to color the graph properly or respecting some special conditions, but other goals have also been explored, like analyzing families of graphs that are colorable in a specific way or developing efficient algorithms for specific coloring.

The idea is that some secret code or message is not safe enough if kept in one place, so it is divided into pieces and those pieces are distributed to the nodes of network. This is a well-known method of secret sharing in cryptography. Usually the assumption is that some of the actors are corrupted, they are “the attackers”, which behave in a certain way to steal the secret of prevent the rest of the group from reading it. In our considerations, a group is represented by a graph, and each piece of the secret corresponds to one color which is then distributed to the vertices. The motivation of securing a secret against a number of corrupted vertices (the attackers) yields conditions on the coloring which prompt us to define a safe vertex coloring.

The conditions for safe coloring follow from the assumption that the secret is safe if the group of attackers didn’t manage to read the whole secret, i.e. collect all the pieces, and further, that they didn’t disable the rest of the group from reading the secret. We assume that the attackers leave the group at some point (the attacker vertices are removed from graph), and the group can still read the secret if there is a component of the remaining graph that has all the pieces.

II. METHODOLOGY

Safe coloring is simple way of labeling graph components such as vertices under some constraints. The transfer of data between source and destination are done by encryption and decryption techniques involving key values which involves lots of head counts and steps. When we use data transfer using safe coloring methods the use of key values is eliminated resulting in decrease of processes. Safe coloring is the process of sending data through nodes present in a graph structured network. This provide a efficient way of encryption and decryption techniques which is more secure and easy way of secure data transfer.

The AntColony algorithm is a probabilistic technique for solving computational problems which can be reduced to finding good paths through graphs.Each ant stochastically constructs a solution on each iteration i.e. the order in which the vertex in the graph should be followed. The paths found by the different ants are compared and updating the pheromone levels on each vertex.

The following steps are:

1. The sender selects the folder that is to be transferred.
2. The selected folder is uploaded in the cloud.
3. The receiver now is ready to download the folder and instigates the process.
4. The nodes will be initialized.
5. While deployment of the nodes the position and distance between 2 nodes is defined and connectivity between nodes will be established thus forming a network.
6. The nodes will be colored using safe coloring techniques by that the safe nodes are identified amongst the n number of nodes and transfer the file in a secured way.
7. Now the files in the Folder will be transferred using the safe colored nodes one by one.
8. Thus the transferred files are received at the other end of the receiver.
9. After the transfer of all the files in the Folder the transfer process ends.
10. Now the receiver has received the Folder in a secure and can now access the Folder.
11. When hacker or eavesdropper try to access any other nodes other than safe nodes, the process gets terminated.

III. SYSTEM ARCHITECTURE

The below block diagrams explains the architecture of the proposed system (Fig 3.1 Architecture Diagram and Fig 3.2 Flow Diagram):

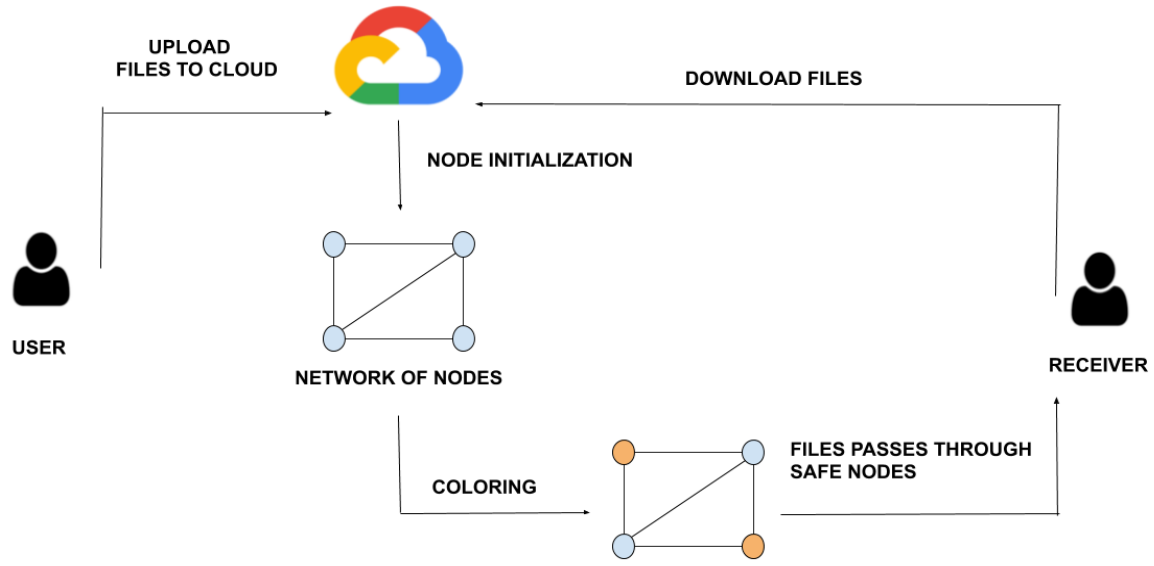

Fig 3.1 Architecture Diagram

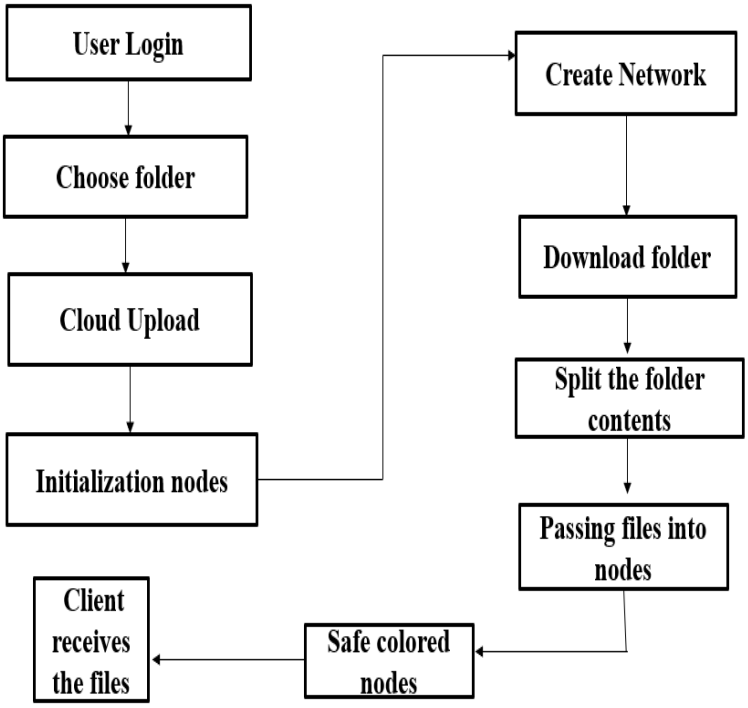

Fig 3.2 Flow Diagram

IV.RESULT

Thus, the safe coloring algorithms is proven to be easy to use and more effective in many aspects than normal cryptography techniques that are being used. Safe coloring is proven to help in secure transfer of data in cloud which uses fast optimization algorithm (Ant Colony).

Parameters analysed	Encryption and DecryptionTechnique	SafeColoring Technique
Algorithm	RSA	Ant Colony
Structure	Factorization	Network of nodes in cloud
Key Size	1024 to 4096	NA
Block Size	Variable	Nil(No blocks are used as files are transferred as a whole)
Complexity	CdmodN	NP-Complete
Running time	O(log(N)3)	$O(2^n)$
Known Attacks	Factoring public key	No known attacks

Structure of safe colouring algorithms is more reliable and easy to understand than RSA.Elimination of usage of key values is a major advantage of safe colouring over RSA.No blocks are required in safe colouring as files in a folder are transferred one at a time.Complexity of safe colouring is more reliable than RSARunning time is less in safe

colouring.There are no known attacks for hacking or eavesdropping safe colouring. Thus, the safe coloring algorithms is proven to be easy to use and more effective in many aspects than normal cryptography techniques that are being used. The algorithm itself is proven for quickly classifying the safe and unsafe nodes from the network which helps to transfer data through the safe node to mislead from hackers.

IV. FUTURE WORK

In future it is proven that we can implement this by the real time cloud like firebase in android. This will result to yield a better performance and results for the convenient of the user. We can also transfer the huge amount of files at a time. Our application can be further developed as an android and iOS application so that the user can use the application easily wherever they are, using their mobile phones or any of their handhelds and it will be more than a user-friendly application. Building as a mobile app has a lot of benefits like faster download speed, Instant Online, and Offline access and Push Notifications and instant updates. It can be build using Edge Computing technology so we can bring computation and data storage closer to the location where it is needed, to improve response times and save bandwidth.

REFERENCES

[1] Tanja Vojkovic, Damir Vuckicevic, " Safe 3-Coloring of graphs", Department of Mathematics, Croatia, August 29,2018.
[2] Zemin Jin and Xue liang Li Center for Combinatorics and LPMC , **"**Dynamically Exchanging Nodes of the Critical Node Problem", 2018.
[3] Franciso J.Aragon Artacho, Ruben Campoy (2016), "Solving graph coloring problems with Douglas-Rachford", Department of Mathematics, University of Alicante.
[4] Sanjay KumarPal,Samar SenSarma, "Graph Coloring Approach for Hiding of Information", (2014).
[5] Josephine Yik Chong Leung, Wai Shan Lui(2014), "The Application of Graph Theory To Sudoku", journal of Hang Lung Mathematics Awards Vol.6(2014), pp. 321-349.
[6] Mohammed A.Khasawneh, Mohammad I. Malkawi, Thaier S. Hayajneh, "A graph-coloring-based navigational algorithm for personnel safety in nuclear applications", March 26,2012.
[7] Hao Lu, Mahantesh Halappanavar, Daniel Chavarría-Miranda, Assefaw H. Gebremedhin, Ajay Panyala, "Algorithms for Balanced Graph Colorings with Applications in Parallel Computing", October 21,2016.
[8] Umma Habiba, Md. Saidur Rahman, Shah Hasnat Lamia, Tahmima Chowdhury, "Safe labeling of graphs with minimum span", May 25, 2015.
[9] Avanthay, C., Hertz, A., Zufferey, N.: "A variable neighborhood search for graph coloring". Eur. J. of Oper. Res. 151(2), 379–388 (2008).
[10] Philippe Galinier, Jean-Philippe Hamiez, Jin-Kao Hao, Daniel Porumbel, "Recent Advances in Graph Vertex Coloring", pp 505-528, (2017).
[11] Blöechliger, I., Zufferey, N.: "A graph coloring heuristic using partial solutions and a reactive tabu scheme. Comput. & Oper". Res. 35(3), 960–975 (2008).
[12] Bui, T.N., Nguyen, T.V.H., Patel, C.M., Phan, K.-A.T.: An ant-based algorithm for coloring graphs. Discrete Appl. Math. 156(2), 190–200 (2008).
[13] Chalupa, D.: "Population-based and learning-based metaheuristic algorithms for the graph coloring problem". In: Krasnogor, N., Lanzi, P. (eds.) Proc. of the 13th annual Genet. and Evol. Comput. Conf. (GECCO), Dublin, Ireland, July 12-16, pp. 465–472. ACM Press, N.Y. (2011).
[14] Chiarandini, M.Stützle, T.: "An Analysis of Heuristics for Vertex Coloring". In: Festa, P. (ed.) SEA 2010. LNCS, vol. 6049, pp. 326–337. Springer, Heidelberg (2010).