Proceedings of the Jangjeon Mathematical Society
27 (2024), No. 1, pp. 17 – 28

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2024.27.1.17

AN ENCRYPTION METHOD FOR OPTIMIZING REPLICA'S IN CLOUD COMPUTING PLATFORM USING PACKING COLORING

Dafik[1], K. Rajalakshmi[2], M. Venkatachalam[3]

S. Lavanya[4] and Ika Hesti Agustin[5]

Department of Science and Humanities[2],

Sri Krishna College of Engineering and Technology,

Coimbatore - 641008, Tamil Nadu, India.

Department of Mathematics[3],

Kongunadu Arts and Science College,

Coimbatore - 641 029, Tamil Nadu, India.

Department of Artificial Intelligence and Data Science[4],

M. Kumarasamy College of Engineering, Karur - 639113, Tamil Nadu, India.

CGANT - Research Group[1,5], University of Jember, Indonesia.

Abstract : In recent technology many techniques lead to new innovations in real time business environment. This research aims to propose the use of packing coloring of Jump graph of Web graph on producing crypto keys which can be used in stream cipher encryption. This encryption takes place in cloud data centre to store files in the backend storage. The key generation using Jump graph of Web graph is implemented on data centre as API to generate keys. It is used to perform replication over number of servers and do optimization with the help of packing coloring.

Keywords : Packing Coloring, Jump Graph, Web Graph, Stream Cipher, Keystream, Encryption.

2010 Mathematics Subject Classification : 05C15, 05C70, 05C12, 05C76

1. Introduction

Cryptography is a technique for securing data and communication which can also be done using codes. In software engineering, cryptography alludes to make sure about the data and communication methods obtained from scientific ideas and

Manuscript Submission Date : 20.02.2023

Corresponding author : M. Venkatachalam : venkatmaths@kongunaducollege.ac.in

a rule-based figures to change the messages that are difficult to decrypt. These deterministic calculations are utilized for cryptographic key generation and it ensures secure information, web browsing, etc., For example, credit card exchanges and e-mail. Cryptography is a method of converting plain text to cipher text and vice versa, people who practice in this field are known as Cryptographers. A case of fundamental cryptography is an encoded message where letters are supplanted with different characters. To decrypt the encrypted data, one would require a framework or table that characterizes the transposition of letters. For instance, the below mentioned interpretation table could be utilized to decipher "1234195346" as "mangotreat".

1	m	9	t
2	a	5	r
3	n	3	e
4	g	4	a
1	o	6	t

The above value is called a cipher text. It can be simple interpretation code just like the above method or even be complex calculations. While straightforward codes got the job done for encoding manually written notes, the complex calculations are harder to break. PCs can process billions of counts for each second; they can even break complex calculations very quickly. Consequently, nowadays, cryptography involves creating encryption strategies that are hard for even supercomputers to break. Hence, the motivation to propose this research is to establish a strong key generation technique and perform encryption to create cipher codes with a stronger security. Also, it helps in creating optimized replica over servers in a distributed network. Consider a real time scenario in "Cloud", it is a distributed system consisting of many servers that hold different set of data. Cloud is a multitenant platform that allows multiple users to access the shared resource. The resources such as Computer, storage, network, application, DBMS, etc are placed in a centralized management and these resources are shared among multiple users as services through internet as shown in flow chart 1. There are two main participants in the cloud namely; 1) CSP (Cloud service provider who provides resources as services), 2) Cloud users

(those who use the cloud resources). When the user is requested to access a resource in the cloud, the CSP must ensure authentication, integrity of the data, right user accessing to right resources, security, etc., This research aims in providing security when users access to data in cloud. The second important issue focused in this research is when any cloud user is accessing a data, it should be present in any of the cloud server. When the number of users are increasing to access the same data then the process of placing replicas in different server is called replication. (For instance, IRCTC, a railway application is accessed by n number of users. Today, the number of users accessing to IRCTC website may be 10,000 in numbers, tomorrow it may be one billion users based on the demand), it should be placed in different number of server as replica's (copy of same set of files in different servers). The process of placing replica's in different server is called replication. Information Replication [4,6,12] is a way of storing data in more than one site or hub. It is helpful in improving the accessibility of information. The outcome is a dispersed database where clients can get continuous access to their data/assignments without disturbing other's job. Why replication is needed: When n users are accessing to the same resource, CSP has to place number of copies in different server. When users are increasing, replicas must be more, When users are limited in numbers, then it must be de -duplicated. This research aims in providing solution to security and replication in cloud. Here, Jump graph of web graph[10,11] is taken as the input graph to generate key streams. The constructed key streams are used by the stream cipher cryptographic algorithm to encrypt data in cloud when it is being stored in backend storage which ensures security. Packing Coloring process is applied on the web graph that ensures optimized placement of replica's over servers which leads to storage efficiency in cloud. Different block uses different key streams for encryption to achieve stronger protection. The other part of the research is sketched as follows. Section 2 explains the concept of Jump graph of web graph, section 3 explains about establishment of key streams for stream cipher and section 4 presents the experimental review of the stream cipher.

2. Result on Packing Coloring of Jump Graph of Web Graph

One of most thriving branches of mathematics with application to a wide variety of subject is "Graph theory". Coloring of the graph is an assignment of colors to the vertices of a graph so that no two adjacent vertices get the same color. The given graph can be colored in different ways. "Packing Coloring" is one such way. The packing chromatic number χ_ρ of a graph G is the smallest integer k for which there exists a mapping π from V(G) to $\{1, 2, ..., k\}$ such that any two vertices of color i are at distance at least i+1. Let $G(p, q)$ be a graph with $p = |V|$ and $q = |E|$ denote the number of vertices and edges of a graph G, respectively. All the graphs considered in this paper are simple graphs. We include $V(G)$ its set of vertices and $E(G)$ its set of edges. The distance $d_G(u, v)$, or simply $d(u, v)$, between vertices u and v in G is the length (number of edges) of a shortest path joining u and v. Computer science applications highly utilizes the graph theoretical ideas exclusively in areas of data mining, image segmentation, clustering, image capturing, networking etc., For example, using the graph concepts in a data structure can be designed in the form of a tree which in turn uses the vertices and edges. Likewise, graph concepts help in the modeling of network topologies. Similarly, the most essential concepts of graph coloring is made use in resource allocation, scheduling. Also the paths, walks and circuits in graph theory are used in remarkably in applications like travelling salesman problem, database design concepts, resource networking, which aids to the development of new algorithm and new theorems that can be used in remarkable applications. Goddard et al.[3] introduced the packing coloring of graphs under the name of broadcast chromatic number and the anthers showed that the deciding whether $\chi_\rho(G) \leq 4$ is NP-hard. Packing coloring problems is NP-complete for trees[2]. Using the name of packing chromatic number, Bresar et al.[1] studied the problem on Cartesian products graphs, hexagonal lattice and trees. A Web graph W_n is one obtained by joining the pendant points of a helm to form a cycle and then adding a single pendant edge to each vertex of this outer cycle. The Jump graph $J(G)$[5] of G is the graph whose vertices are edges of G and where two vertices of $J(G)$ are adjacent if and only if they are not adjacent in G. Equivalently, the Jump graph $J(G)$ of G is the complement of line graph of G.

Theorem 2.1

If $\chi_\rho[J(W_n)]$ is packing chromatic number of the Jump graph of web graph for $n \geq 3$, then $\chi_\rho[J(W_n)] = 4n - 2$.

Proof

Let $V(W_n) = \{a_p, f_p, g_p : 1 \leq p \leq n\}$ and

$V[J(W_n)] = \{a_p, f_p, g_p, e_p, b_p, d_p, h_p : 1 \leq p \leq n\}$

For $1 \leq p \leq n$

- Each edge $a_p f_p$ is partition of by b_p of W_n
- Each edge $f_p g_p$ is partition by h_p of W_n
- e_n is the vertex corresponding to the edge $a_n a_1$ of W_n
- d_n is the parallel to the edge $f_n f_1$ of W_n

For $1 \leq p \leq n-1$

- Each edge $a_p a_{p+1}$ is partition by e_p of W_n
- Each edge $f_p f_{p+1}$ is partition by d_p of W_n

Assign the packing coloring to $J(W_n)$ as follows:

Contradictory method is used to prove the lower bound. For that, we assume that $\chi_\rho[J(W_n)] < 4n - 2$. Now, select the colors for each valid vertex in $\chi_\rho[J(W_n)]$ as $4n - 3$. From jump graph of web graph, $c(e_1) = c(e_2) = c(b_1) = 1$, $d(e_p, d_p) = d(e_p, h_p) = 1$ and $d(b_p, d_p) = d(d_p, h_p) = 2$ are true. Here, the maximum distance is 2 then the diameter of $J(W_n)$ is also 2. This shows that we can repeat only the color 1 as much as possible in $J(W_n)$. Since, we assumed $4n - 3$ colors for $J(W_n)$, now, we are left with a remaining colors as $4n - 4$. According to the definition of packing coloring, if two vertices of color i are at distance of at least $i + 1$ apart and $d(d_p, h_p) = 2$ then $c(d_p) \neq c(h_p)$ and $4n - 4$ colors are required for each d_p and h_p. While this proves a contradictory value compared to the desired output, the

statement $\chi_\rho[J(W_n)] < 4n-2$ is wrong. Also, an easy check shows that, the total number of vertices of $J(W_n) = 4n$ and

$$\rho G(i) = \begin{cases} 3 & for \quad i = 1 \\ 1 & for \quad i \geq 2. \end{cases}$$

Therefore, $\chi_\rho[J(W_n)] \geq 4n-3+1 \geq 4n-2$.

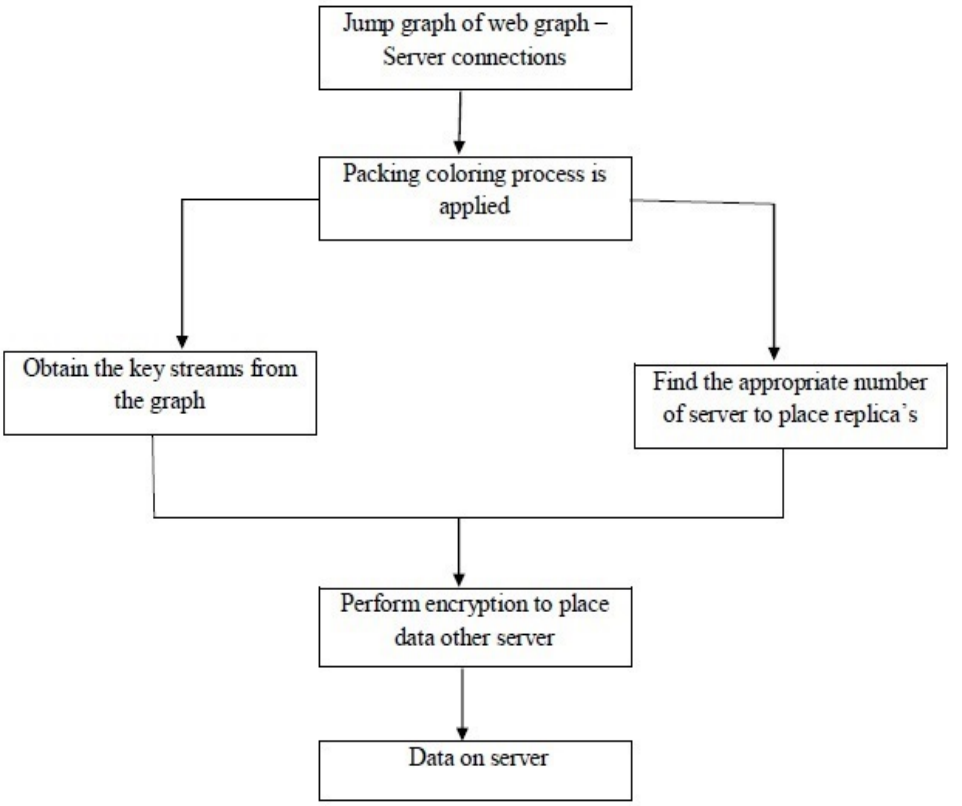
Hence, we conclude that the lower bound $\chi_\rho[J(W_n)] \geq 4n-2$. Next, we need to calculate the upper bound $\chi_\rho[J(W_n)] \leq 4n-2$.

Consider the color function $c : V[J(W_n)] \to \{1, 2, ..., 4n-2\}$ is defined by,

$$\begin{array}{lll} c(e_1) = c(e_2) = c(b_1) = 1 & \text{for} & 1 \leq p \leq n \\ c(e_p) = p-1 & \text{for} & 3 \leq p \leq n \\ c(b_p) = n-2+p & \text{for} & 2 \leq p \leq n \\ c(d_p) = 2n-2+p & \text{for} & 1 \leq p \leq n \\ c(h_p) = 3n-2+p & \text{for} & 1 \leq p \leq n \end{array}$$

Therefore, the upper bound $\chi_\rho[J(W_n)] \leq 4n-2$. Hence, $\chi_\rho[J(W_n)] = 4n-2$.

3. Architecture flow of this research in cloud computing



4. Establishment of key streams

Stream cipher[7,8,9] is the most popular and secure technique in cryptography to transfer data from one place to another and it uses different key streams for each block where as block cipher uses the same key to perform encryption and decryption. Initially, random key is used to encrypt the first block and the subsequent key streams are generated by our crypto systems based on the below function.
The crypto system consists of 5 tuples: $[G = gjump(H, P_2, n)$,$l, b, g(k)$,$CBC]$, which can also be described as follows.

- The source of the key stream is chosen from the Jump graph of web graph $G = gjump(H, P_2, n)$

- The introductory block key has a length of b and starts with the l^{th} element of the sequence produced by the packing coloring.
- The key stream is created by the function $g(k)$
- Stream cipher is executed using the Cipher Block Chaining mode.

The key streams are generated using packing coloring process that yields a sequence of labeled numbers from the graph $G = \text{gjump}(H, P_2, n)$. The advantage of this process is to provide strong security and ensure storage efficiency with the help of minimal replication. For the sake of security, take alphabets A to Z numbered 0 to 25 respectively. The key stream construction is as follows

Algorithm 1

- Take v as vertex
- Draw the jump graph of web graph by considering the vertices
- Let s be sequence and let t = length of s
- The sequence are used as key streams
- Determine b = length of the block
- Let l, such that $1 \leq l \leq t - b$
- Assume $k = s_l, s_{l+1}, s_{l+2}, ..., s_{l+b-1}$ as introductory block key.
- Determine stream function $k_{j+b} = g(k_j, k_{j+1}, ..., k_{j+b-1})$

The output of the above algorithm produces the key streams from the jump graph of web graph starting from 1, 1, 2, 3, 4, 5, 6, 1, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26 by doing equivalence modulo 26. We have initial block key k= 1, 1, 2, 3, 4 and thus the key stream is 1, 1, 2, 3, 4 – 5, 6, 1, 7, 8 – 9, 10, 11, 121, 3 – 14, 15, 16, 17, 18 – 19, 20, 21, 22, 23 - 24, 25, 26. Assume k is the preferred size of the user.

5. Encryption Algorithm

The key stream created by the algorithm 1 is used to establish stream cipher.

Algorithm 2

Step 1: Let plain text $P = (p_l)$ $1 \leq l \leq h$

Step 2: Divide P into blocks of the length b

Step 3: $P = 1$ to $\lceil h/b \rceil$ calculate the cipher text blocks by employing equation 1.

$C_n = C_{n-1} + P_n + K_n \ mod\ 26$

The n^{th} block of plain text, key sequence and cipher text are P_n, K_n, C_n.

Initially $n = 1$, C_{n-1} is a null vector, the key stream becomes all zero's.

The below table explains the obtainment of key stream from algorithm 1 which is used to encrypt the plain text "APPLICATION OF PACKING COLORING" and yields the cipher text "BQROMHGWSAPERIVZJJQLJXWBGZGB". The reverse process can be done to perform decryption.

plaintext	A	p	p	l	i	c	a	t	i	o	n	o	f	p	a
P_i	0	15	15	11	8	2	0	19	8	14	13	14	5	15	0
C_{i-1}	0	0	0	0	0	1	1	2	3	4	5	6	1	7	8
P_i'	0	15	15	11	8	3	1	21	11	18	18	20	6	22	8
K_i	1	1	2	3	4	5	6	1	7	8	9	10	11	12	13
C_i	1	16	17	14	12	7	6	22	18	0	1	4	17	8	21
ciphertext	B	Q	R	O	M	H	G	W	S	A	B	E	R	I	V
plaintext	C	k	i	n	g	c	o	l	o	r	i	n	g		
P_i	2	10	8	13	6	2	14	11	14	17	8	13	6		
C_{i-1}	9	10	11	12	13	14	15	16	17	18	19	20	21		
P_i'	11	20	19	25	19	16	3	1	5	9	1	7	1		
K_i	14	15	16	17	18	19	20	21	22	23	24	25	26		
C_i	25	9	9	16	11	9	23	22	1	6	25	6	1		
ciphertext	Z	J	J	Q	L	J	X	W	B	G	Z	G	B		

5.1. Experimental Analysis

This research yields advantages in two ways.

- It reduces space consumption and avoids multiple copies of data when no longer required

- Enhances security in terms of encryption while placing data on the particular server.

5.2. Cipher text and plain text analysis

The attacker is aware only of the cipher text. The attacker may try it with the brute force method to find the key streams in all possible ways to find the original plain text. The different blocks of length h is divided into blocks of length b, and the same is encrypted using different keys. (i.e., 26^b possible keys for each block or $(26)^{b^{\lceil \frac{h}{b} \rceil}}$ possible keys). Hence, it is difficult for the attacker to work on brute force technique if the length of the block is more. Knowing several pairs of cipher text - plain text will not be sufficient to find the whole blocks, different blocks are encrypted by different sequence of keys. If an attacker tries to find the key streams using chosen cipher text - plain text or keys, then it is also difficult to encrypt or decrypt. The reason behind it, is that the cloud which is a dynamic configuration of servers, so often change of key streams are encountered. Hence, chosen plain text and cipher text is also not possible.

6. Conclusion

This research solved the problem of placing replica's on the server in cloud platform and also provides strong security to the cloud data. The stream cipher has been established from a jump graph of web graph using packing coloring process. This attempt proves to guarantee the reliability of crypto system. The method generates the invariable length of the key streams to the size of the graph that guarantees strong security because different blocks are encrypted using different keys. This strong crypto systems requires less storage capacity. This strongly tells the count of the replica's needed to be placed on the servers. Hence, wastage of storage capacity in server can be reduced. If the access to a particular file is limited, minimum number if replica's needs to be placed. Hence, this crypto system is strong, secure and it cannot be diluted by an attacker.

Bibliography

[1] B. Brešar, S. Klavžar, D. F. Rall, On the packing chromatic number of cartesian products, hexagonal lattice, and trees, Discrete Applied Mathematics, 155 (17), (2007), 2303–2311.

[2] J. Fiala, P. A. Golovach, Complexity of the packing coloring problem for trees, Discrete Applied Mathematics, Third Workshop on Graph Classes, Optimization, and Width Parameters, Euge ne, Oregon, USA, 158 (7), (2010), 771–778.

[3] W. Goddard, S. M. Hedetniemi, S. T. Hedetniemi, J. M. Harris, D. F. Rall, Broadcast chromatic numbers of graphs, ARS Combinatoria, 86 (2008), 33–49.

[4] Jon Grov and Ragnar Normann, Technical note: Replication graphs revisited, Journal of Computer and System Sciences, 72 (2006), 1251—1261.

[5] Y. B. Maralabhavi, S. B. Anupama, Domination number of jump graph, International Mathematical Forum, 8, (2013), 753—758.

[6] Netanel Raviv, Itzhak Tamo, Eitan Yaakobi, Private information retrieval in graph based replication systems, arXiv:1812.01566v2 [cs.IT] 4 Mar 2019.

[7] A. C. Prihandoko, Dafik and I. H. Agustin, Implementation of super H-antimagic total graph on establishimg stream cipher, Indonesian Journal of Combinatorics, 3 (1), (2019), 14–23.

[8] A. C. Prihandoko, Dafik , A. I. Kristiana, Salmin, The construction of encryption key by using a super H-antimagic total graph, Program and abstract the asian mathematical conference, 408, (2016).

[9] A. C. Prihandoko, H. Ghodosi, B. Litow, Deterring traitor using double encryption scheme, Proceedings of the IEEE International Conference on Communication, Network and Satellite, (2013), 100–104.

[10] K. Rajalakshmi, M. Venkatachalam, On packing coloring of double wheel graph families, International Journal of Pure and Applied Mathematics, 119 (12), (2018), 2389–2396.

[11] K. Rajalakshmi and M. Venkatachalam, On packing coloring of helm related graphs, Journal of Discrete Mathematics Sciences and Cryptography, 22 (6), (2019), 989–1005.

[12] L. Yohananov, E. Yaakobi, Codes for graph erasures, arXiv:1705.02639 [cs.IT], 2017.