International Journal of Pure and Applied Mathematics
Volume 118 No. 6 2018, 1-9
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Security Enhancement for Public Cloud Storage with Minimum Cost

D.I. George Amalarathinam[1] and B. Fathima Mary[2]

[1]*Department of Computer Science,*
Jamal Mohamed College (Autonomous), Tiruchirappalli–620 012.
di_george@ymail.com
[2]*Department of Computer Science,*
Bharathiar University,
Coimbatore, Tamilnadu, India
fathimamary02@gmail.com

Abstract

Data security is the most important challenge in the public cloud environment. User outsources their data to the cloud for flexible, efficient and seamless services. Security is one of the major issues which reduces the growth of cloud computing. Once the data is sent to the cloud, the cloud service provider (CSP) alone is responsible for the data. Data security is one of the major issues which acts as an obstacle in the adoption of cloud computing. To protect the data from unauthorized access, this paper proposes a confidentiality enabled technique named as CBO (Cube Based Obfuscation) to secure the data in the cloud storage. The proposed confidentiality technique is based on the data obfuscation technique. The proposed confidentiality technique is based on the data obfuscation technique. Data obfuscation (DO) is a function that transforms data into new form and it must conceal the original data. Storage cost is based on the size of data and lifespan of the storage. By applying the proposed CBO technique, the obfuscated data size is reduced compare than the existing technique. Hence, it reduces the size of data being uploaded to the cloud storage. The costs of existing and proposed obfuscated text are calculated by using Google cloud data storage cost. Hence, the proposed method enhances the data security and also reduces the cost of data storage while uploading the data to the cloud storage compare than the existing technique.

Key Words and Phrases: Cloud Storage, CSP, security, data obfuscation, confidentiality, Cube, rotation.

1 Introduction

Cloud computing is a use of computing that is delivered as a services over a network, the services may be a hardware or software [1, 2]. It has more powerful computing infrastructure with a pool of thousands ofcomputers and servers. The cloud offers several benefits like fast deployment, pay-for-use, lower costs, scalability, rapid provisioning, rapid elasticity and ubiquitous network access. It helps to reduce the computational infrastructure investment and maintenance cost [3]. Cloud has multiple data centers placed in different geographical locations in the world to provide reliable services to the users. It provides unlimited service provisioning without any human intervention. The prominent issue focused in cloud computing is data security. CSP is responsible for maintaining and monitoring the outsourced data. Cloud is a public environment where there are many possibilities to attack the data [4]. Data outsourcing brings security issues in the cloud while move to storage. This paper uses confidentiality parameter to enhance the data security, while the data is stored in cloud. Confidentiality of data is enabled by using efficient cryptography and obfuscation technique [5].

In cryptography [4], original data is transformed into coded format by using encryption techniques. Hence that only authorized users can decode the encoded message is known as encryption. And the process of retrieving original data from encoded data using an encryption key/decryption key is known as decryption. Obfuscation is the process of hiding the original value of data [6] [7]. It is a process applied to information to intentionally make it difficult to reverse without knowing the algorithm that was applied. The main difference between them is that even if the algorithm is known, the encrypted data cannot be processed without the key required for decryption. Similarly, obfuscated data can be processed without any requirement of key.

Data obfuscation is used for security which makes it hard to reconstruct the plaintext. This technique has recently become popular for data storage security in cloud storage [8]. Researchers start using obfuscation technique to provide security to the data in the cloud rather than cryptography techniques. This paper discusses the data obfuscation technique named as CBO. This technique improves the classical obfuscation technique by introducing the Rubik's cube rotation technique. Rubik's cube was invented in 1974 by Hungarian sculptor and professor of architecture Ernő Rubik. Cube is solved by using 18 different rotations for classical Rubik's cube [14]. 3×3 cubical structure is shown in Fig. 1. The Number of rotation (NR) is represented in Eq. (1),

$$NR = 3_{\text{layer}} \times 6_{\text{faces}} = 18 \tag{1}$$

The proposed CBO technique increases the data security and reduces the size of data being uploaded to the cloud storage. The rest of the paper is organized as follows: Section 2 gives related work. Section 3 presents the proposed algorithm in detail. Section 4 evaluates the performance of our existing and proposed technique. Section 5 offers conclusion.

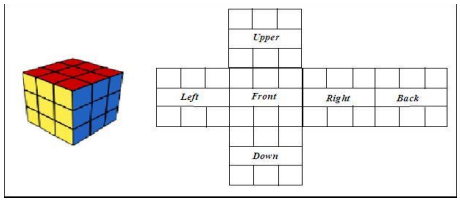

Figure 1: 3×3 Cubical Structure.

2 Related Works

Himani et al. [9] proposed a model which contains encryption and obfuscation techniques are used to protect the data while transits as well as at rest. The author proposed a model based on data classification such as numerical and non numerical data. Monikandan et al. [10] proposed data obfuscation technique named as Moncrypt SSA to protect the data from unauthorized access. Plain Text values are arranged as an array and square root is calculated for the value. Calculated square root values are rotated based on the key and the key is incremented by one for each value. Finally, the rotated values are divided by 256 and the remainder values are taken. Finally, the obfuscated text is attained by converting the remainder value into ASCII character code. saha et al. [11] proposed multiple key cryptography technique to enhance the data security and minimize the cost for cloud storage. In this technique, data is directly converted to RGB image which is a steganography concept and then apply multiple keys cryptography to this image for security. Multiple keys are generated randomly and the whole process is data-to-image-to-data conversion. File size is totally reduced when the file is converted to image.

Asif et al. [12] proposed encryption algorithm for data security in the cloud. The proposed hybrid approach uses a data compression method to reduce the size of original data and then encrypt the data using ASIF Encryption Algorithm. It reduces the size of data and requires less storage space because of data compression method. Balamurugan et al. [13] proposed obfuscation technique for numerical data. This technique uses different mathematical methods to convert the original data into unintelligible data and minimizes the data size. Rajavel et al. [14] proposed cubical scrambling method to represent the text in a cube format. Cube's rotation type is defined randomly by generating random sequence.

The proposed CBO technique is an obfuscation technique and it obfuscates both the numerical as well as non numerical data. In this proposed technique, Frequently used words are eliminated from plain text and the cubical rotation is applied for remaining text. Cubical representation of the shuffling gives the novelty of the research and it affords the new approach to the obfuscation technique. Cubical form of text is more reliable, because single rotation of a cube scrambles the text in five out of six faces of a cube. Hence, the attacker cannot easily deobfuscate the data without knowing the position of FUW and the cubical rotation.

Input: Plain Text
Output: Obfuscated Text
Method:

1. Start
2. Read W from PT
3. Generate WL
4. Compare WL with FUWD
5. Generate Tokens
   Tokens → eliminate FUW from WL
6. N ← Count of Tokens
7. for i← 1 to N
8. RC→ generate cube matrix with 3×3 size
9. populate the tokens inside the RC
10. RT1 → Rotate the RC i.e. Clockwise
11. RT2 → Rotate the RC i.e. anti clock wise
12. Generate OT
13. end for
14. end

where

W—Words, WL-Word List

PT—Plain text

FUWD—Frequently used words Dictionary

RC-Rubiks Cube

RT—Rotation

OT—Obfuscated Text

Figure 2: Obfuscation Technique.

Input: Plain Text
Output: Obfuscated Text
Method:

1. Start
2. Read OT
3. RC→generate cube matrix with 3×3 size
4. populate the OT inside the RC
5. RT1→Rotate the RC i.e. anti clock wise
6. RT2→ Rotate the RC i.e. Clockwise
7. for i←1 to N
8. Re-Generate Tokens
9. Compare Tokens with FUWL
10. Generate WL
11. Generate PL
12. End for
13. End

Figure 3: De-Obfuscation Technique.

3 Proposed Methodology

CBO technique improves classical obfuscation techniques by integrating substitution, transposition and values. This technique is used to shuffle the original value of data and it should not be reversible. Initially the Word (W) lists are generated from the plain text(PT). The CBO technique maintain the frequently used words dictionary (FUWD) and it contains the words like as is, of, the, to, this etc. The PT words are filtered by FUWD. If any words occurred in FUWD, that words are eliminated from PT is named as tokens. Frequently used words (FUW) and its position are maintained in frequently used words location (FUWL). The tokens are horizontally populated inside the Cube. CBO technique takes cube size as 3×3. The obfuscated text will be attained by rotating the cube. Pseudo code for CBO is given in Figs. 2 and 3.

The proposed and existing technique is tested with the plain text. Fig. 4 shows the overall process of existing technique. The plain text is "Internet is run on computers & connects many computers ". Initially, words are generated from the plain text shows in Fig. 4(a). The words are populated inside a matrix cube shown in Fig. 4(b). After rotation, the characters are scrambled as shown in Fig. 4(c). Finally, cube face values are taken one by one horizontally which it is considered as a cipher text is shown in Fig. 4(d). Fig. 5 shows the overall process of proposed technique. Initially, WL are generated from the plain text is shown in Fig. 5(a).

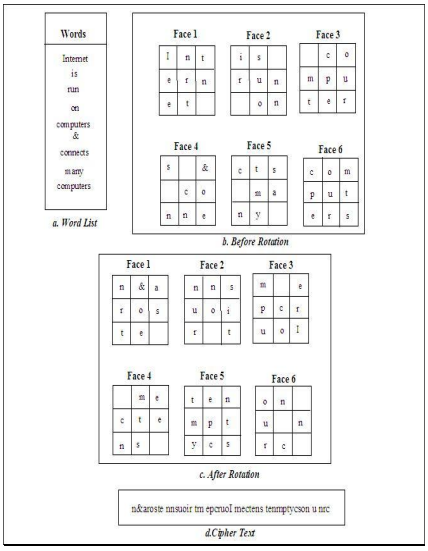

Figure 4: SCA Technique.

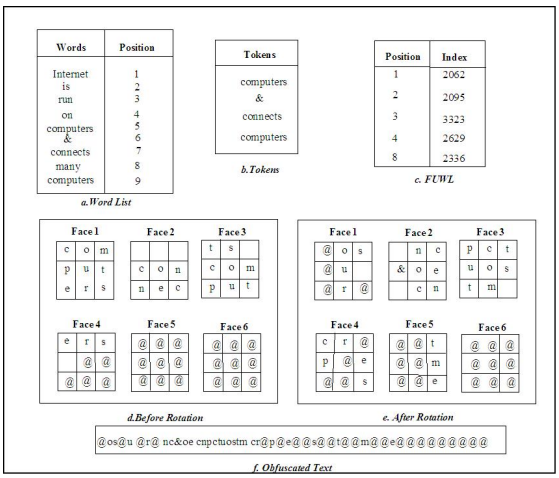

Figure 5: Proposed CBO Technique.

WL are compared with FUWD. If there is any words occurred in FUWD, words are eliminated from the plain text and it is stored in FUWL with appropriate word position and index is shown in Fig. 5(c). The filtered words in the plain text are considered as a token is shown in Fig. 5(b). The tokens are populated horizontally inside the cube matrix horizontally shown in Fig. 5(d). After rotation, the tokens are scrambled inside the cube matrix is shown in Fig. 5(e). Finally, the cube face values are taken horizontally is shown in Fig. 5(f). In the existing technique, cipher text contains the same size as equal to the size of plain text. Hence, the attacker may try to hack the cipher text with the possible type of rotation. In the proposed technique, the cipher text contains the combination of scrambled tokens and '@' sign. Even if the intruder tries to attack the cipher text without knowing FUWL, it is not possible to predict the scrambling pattern. The security of cipher text is to be increased in the proposed technique compare than the existing technique.

4 Results and Discussion

The proposed methodology CBO is implemented in Java. Whenever increase the security, execution time will be increased. It takes additional time to filter the plaintext by removing the FUW. In the existing technique [14], original message is scrambled with the possible rotation types. At the end of the rotation, scrambled message is considered as an obfuscated text. It is possible to reproduce the original text with the possible type of rotation. In CBO technique, the plain text is filtered and performed the matrix cube rotation. Prediction is not possible without the knowledge of location file in CBO. The proposed technique improves the security by using obfuscated technique. Table 1 includes the size of the existing and proposed obfuscated text. When the file size is 100 kb, SCA technique produces the obfuscated text as 100 kb whereas the proposed CBO technique produces in

Table 1: Estimated Data Storage Cost.

Plain Text File size (kB)	Obfuscated File Size (kB)		No of Cube Required		Total cost per Month for Plain Text ($)	Total Cost per Month for SCA Technique ($)	Total Cost per Month for CBO Technique ($)
	SCA Technique	Proposed CBO Technique	SCA Technique	Proposed CBO Technique			
100	100	66	1897	1251	11	1.07	0.71
200	200	133	3793	2522	22	2.15	1.43
300	300	199	5689	3773	33	3.22	2.14
400	400	265	7586	5025	44	4.29	2.85
500	500	331	9482	6276	55	5.37	3.55

66 kb. Similarly when the file size is 500 kb, SCA technique gives the obfuscated text as 500 kb whereas the proposed CBO technique gives 331 kb. Whenever the plain text file sizes increases, the obfuscated file size will also decreases. In Table 1, the number of cube is lower than the SCA technique. One of the CSP is Google cloud storage, which is massively scalable, it can store and process hundreds of terabytes of data [15]. Total cost is calculated by using Google cloud storage cost. The proposed CBO technique reduces the storage cost compare than SCA technique. Consistently the proposed CBO technique gives the better result. Hence, the proposed CBO obfuscation technique is more efficient and suitable for cloud environment.

5 Conclusion

Cloud Storage provides cost-effective services to individual users as well as organization. It provides huge amount of space to outsource the data to the cloud. Organization and enterprises do not possess full infrastructure to maintain their data with their premises. Data outsourcing helps to effectively maintain their data in cloud storage. Whenever user moves their data to the cloud, there are many possibilities to attack the data at rest. This paper discusses confidentiality enabled obfuscation technique named as CBO. According to this technique, data are obfuscated before they are uploaded to the cloud storage. The plain text file is filtered with the help of dictionary. Hence the size of plain text file is reduced. After that, rubik's cube rotation is performed for the purpose of shuffling the data. Whenever the file size increases, the obfuscated file size will be reduced depends on the FUW. An experimental result shows that CBO technique enhances the data security and also reduces the cost of data storage.

References

[1] Buyya R, Vecchiola C, S. ThamaraiSelvi,*Mastering Cloud Computing Foundations and Applications Programming,* Elsevier, (2013).

[2] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I,*Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility* , Elsevier Science, (2009).

[3] Furht B. Cloud computing fundamentals,*Handbook of Cloud Computing. Springer Science* , Business Media, LLC,(2010).

[4] Diogo A. B. Fernandes, Liliana F. B. Soares, Joao V. Gomes, Mario M. Freire and Pedro R. M. Inacia, Security Issues in Cloud Environments: A Survey,*International Journal of Information Security*, Springer, (2013) 113-170.

[5] L. Arockiam, S. Monikandan, P. D. Sheba K Malarchelvi, Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage,*International Journal of Computer Applications*, (2014), 17–21.

[6] `http://www.techopedia.com/definition/25015/dataobfuscation-do`

[7] S.Arul Oli, L. Arockiam, Enhanced Obfuscation Technique for Data Confidentiality in Public Cloud Storage, *MATEC Web of Conferences*, (2016), 1–5.

[8] `http://www.sans.org/reading-room/whitepapers/engineering/pdf-obfuscation-primer34005`

[9] Maninder Singh Bajwa, Himani, An Intensify approach of Data owner Dominant Model for Safeguard Data security in Cloud,*International Journal of Computer Engineering In Research Trends*, (2015), 260–263.

[10] S. Monikandan, L. Arockiam, Confidentiality Technique to Enhance Security of Data in Public Cloud Storage using Data Obfuscation, *Indian Journal of Science and Technology*,(2015), 1–10.

[11] Tushar Kanti Saha, A B M Shawkat Ali, Storage Cost Minimizing in Cloud–A Proposed Novel Approach Based on Multiple Key Cryptography, *Proceedings of the IEEE Asia-Pacific World Congress on Computer Science and Engineering*,(2014), 1–9.

[12] Md Asif Mushtaque, Harsh Dhiman, Shahnawaz Hussain, A Hybrid Approach and Implementation of a New Encryption Algorithm for Data Security in Cloud Computing, *International Research Publication House* **7**,(2014) ,669–675.

[13] S. Balamurugan, S. Sathyanarayana and S. S. Manikandasaran," ESSAO: Enhanced Security Service Algorithm using Data Obfuscation Technique to Protect Data in Public Cloud Storage",*Indian Journal of Science and Technology*, **9**, (2016) 1–6.

[14] Rajavel D, Shantharajah SP, "Scrambling algorithm for encryption of text using cube rotation artificial intelligence technique",*Biomedical Research*,(2016), 251–256.

[15] `https://cloud.google.com/products/calculator/{#}id=d969f758--720a-4003--9ac2a85668e672cb`