IJCTA, 9(27), 2016, pp. 107-113 ISSN: 0974-5572

Confidentiality Technique for Enhancing Data Security in Public Cloud Storage using Data Obfuscation

D.I. George Amalarethinam* and B. Fathima Mary**

ABSTRACT

Cloud delivers storage as a service (STaaS) all over the internet. STaaS is a service where data is remotely maintained, managed, and backed up. Cloud storage provider (CSP) is only responsible for controlling, monitoring and maintaining the data. So, there is no need to invest any capital investments and also to maintain the storage server and data. Cloud offers enormous amount of space to their user data. This technology has proved itself as a new venture because of its ability for releasing massive computational storage with reducing cost from anywhere to any user at any time. Apart from the benefits, it has lot of security and vulnerability issues on the data stored in the cloud. When a user outsources the data to the cloud, there is possibility to attack the data at rest as well as data in transit. Now the concern is how to secure the data and rely on the services in cloud. In order to protect the data from unauthorized access, data should be in either encrypted format or masked format. This paper proposes a confidentiality technique named as WMRADO (Word Magical Rolling Alpha Digits Obfuscation) to enhance the security of data in cloud. This technique is applied in plaintext in both ways such as word by word and line by line obfuscation. WMRADO technique is based on word by word obfuscation whereas MRADO is line by line obfuscation technique which we have proposed earlier. By applying this MRADO technique, the obfuscated data size is reduced compared to the existing MONcrypt technique. So, it reduces the size of data being uploaded to the cloud storage. The cost of MONcrypt and MRADO obfuscated text are calculated by using Google cloud data storage cost. The proposed method enhances the data security and also reduces the cost of data storage while uploading the data to the cloud storage compared to the MONcrypt technique.

Keywords: STaaS, CSP, data security, confidentiality, cryptography, obfuscation, cost.

1. INTRODUCTION

Cloud computing is the use of computing resources that is delivered as a services over a network. The services may be a hardware or software. Cloud dominates it industry by its tremendous characteristics. NIST defines, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[1][2]. Cloud provides three kinds of services like Infrastructure as a service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). IaaS is a service model that delivers hardware, storage, servers and data center to the users. One of the main services provided by the cloud is StaaS[3]. Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network.

Once the data is outsourced to the cloud, CSP is only responsible for maintaining, monitoring and controlling the data. Nowadays many organizations and enterprises have started to outsource their data to cloud. Cloud is a public environment where there are lots of possibilities to attack the user data. Security is the highest concern

* Dean of Science & Director (MCA), Jamal Mohamed College, Trichy, Tamilnadu, India, *Email: di_george@ymail.com*

** Research Scholar, Bharathiar University, Coimbatore, Tamilnadu, India, *Email: fathimamary02@gmail.com*

in the cloud environment. Outsourced data to the cloud are kept by third party CSP[4]. In this situation, data may be attacked from inside as well as outside the cloud. Data security is ensured by security parameters such as confidentiality, integrity and availability. This paper uses the confidentiality parameter to enhance the security of data in cloud storage.

Confidentiality of data is to be ensured by cryptography and obfuscation technique. Cryptography is an effective tool that helps to protect the data from unauthorized access while data at rest in cloud server. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It is the process of encryption and decryption. Cryptographic techniques are classified into Conventional and Public key cryptography. Conventional cryptography is also referred as symmetric key cryptography. The same key is used for encryption and decryption in symmetric key cryptography. Public key cryptography is called as asymmetric key cryptography. Public key and private key are used for encryption and decryption respectively [5].

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 [8]. 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.

2. RELATED WORKS

Monikandan et al.[9] proposed data obfuscation technique named as Moncrypt SSA to protect the numerical 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.

Arul oli et al.[10] presented an approach named as ARO_Obfus to enhance the confidentiality of numerical data in public cloud storage. The plain text is multiplied with the key1 value and the square root is calculated for the multiplied value. Key2 is generated and the calculated square root values are rotated. Modulo operation is performed by 256 and the remainder value is converted to ASCII value.

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.

Himani et al. [12] proposed a model which contains encryption and obfuscation techniques 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. Hussain et al.[14] proposed architecture to store the data in the cloud database. The author proposed cryptography technique for non numerical and obfuscation technique for numerical data.

Asif et al. [13] 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. MRADO obfuscation technique is proposed [14] to enhance the security of data. This technique is used to obfuscate both the numerical and non numerical data. Word to numerical conversion is done using this technique and obfuscated text is the combination of Alpha-Digits only. Security is improved and cost is minimized by applying this technique.

3. PROPOSED WMRADO TECHNIQUE

The existing obfuscation technique uses substitution, redaction or nulling, shuffling and blurring. WMRADO Technique improves classical obfuscation techniques by integrating substitution, transposition and ASCII values. This technique is used to hide the original value of data and should not be reversible. Initially the Word (W) lists are generated from the plain text. In the corresponding lines, characters(C) are converted to ASCII value and that ASCII(ASC) value is multiplied with that character position where it appeared in the word. After that, the multiplied value of individual character is added with another character value and it produces a Numerical Code(NC) to the corresponding word. The look-up table (LT) is generated. It maintains the line and the corresponding NC value which is derived from the lines. The Modulo Operation (MO) is performed on NC by 64 to get the remainder and quotient value. The MRADO Square is generated based on the Seed(S) and it contains alphabets like as small a-z, capital A-Z, digits 0-9,@and #. S is a single value and it must be an either alphabets or digits. Based on the S value, alphabets and digits are sequentially placed inside the MRADO square and the traversal is shown in figure 2. Finally, Alpha-Digits values are taken, according to the remainder of NC value. Finally, the obfuscated text (OT) is attained by the combination of Alpha-Digits. In WMRADO, obfuscation is done word by word whereas is MRADO, obfuscation is based on line by line. Pseudo code for WMRADO and MRADO is given below.

Pseudo Code for WMRADO Obfuscation Technique	**Pseudo Code for MRADO Obfuscation Technique**
1. Start	1. Start
2. Read W from file	2. Read L from file
3. Read C from W	3. Read C from L
4. NC←Convert W into Numeric Code by corresponding C position is multiplied with ASC	4. NC←Convert W into Numeric Code by corresponding C position is multiplied with ASC
5. LT←NC,W	5. LT←NC, L
6. N Count of NC	6. N ← Count of NC
7. for i←1 to N	7. for i←1 to N
8. MO(i)←NC%64 i = 0, 1, 2, ….. N	8. MO(i)←NC%64 i = 0, 1, 2, ….. N
9. S←Seed	9. S←Seed
10. Generate MRADO Square based on S	10. Generate MRADO Square based on S
11. OT(i)← Convert MO(i) based on its position in MRADO	11. OT(i)← Convert MO(i) based on its position in MRADO
12. end for	12. end for
13. end	13. end

4. ILLUSTRATION OF WORKING OF THE WMRADO TECHNIQUE

The MRADO technique is tested with sample text. The experiment procedure is done below.

Step 1: Consider the following plain text

"Jamal Mohamed College"

Step 2: converting the word to the Numeric Code(NC) by multiplying the ASCII value of Individual characters to its position.

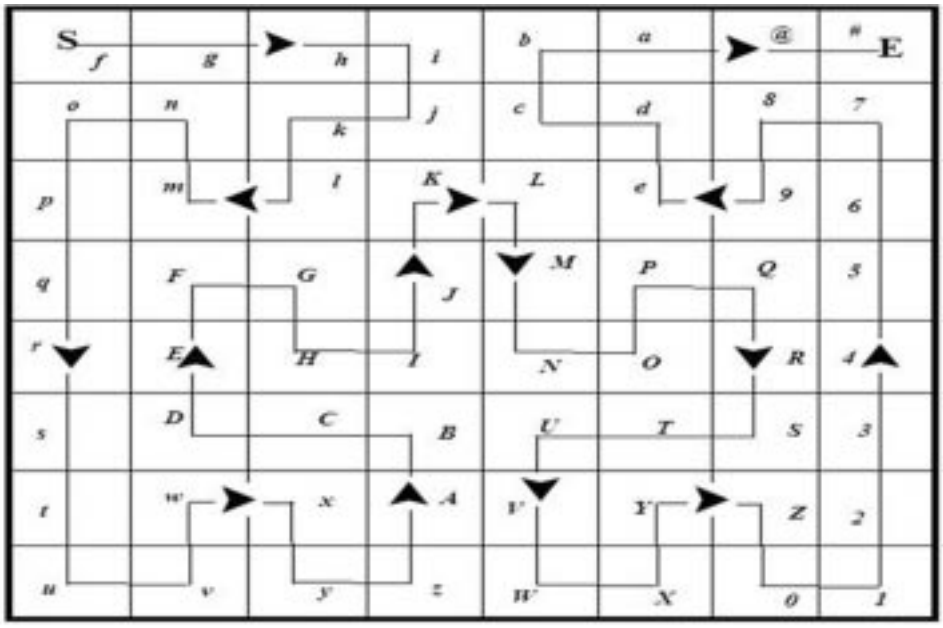
Word	*ASCII*	*Position*	*NC*
Jamal	J a m a l	1 2 3 4 5	74×1+97×2+109×3+97×4+108×5=1523
	74 97 109 97 108		
Mohamed	M o h a m e d		
	77 111 104 97 109 101 100	1 2 3 4 5 6 7	77×1+111×2+104×3+97×4+109×5+101×6+100×7=2850
College	C o l l e g e		
	67 111 108 108 101 103 101	1 2 3 4 5 6 7	67×1+111×2+108×3+108×4+101×5+103×6+101×7=2875

Step 3: The modulus operation is performed by 64 to the corresponding numeric codes and the quotient, remainder values are taken.

NC	*NC%64*	
	Quotient	*Remainder*
51	1523	23
34	2850	44
59	2875	44

Step 4: based on the seed value, MRADO is constructed.

Seed is *f*



Step 5: Finally, Alpha-Digits values are taken from the MRADO according to the quotient and remainder value.

Step 6: The obfuscated text is 6A UH Uz

5. EXPERIMENTS AND RESULTS

The proposed methodology is implemented in JAVA. The methodology is used to obfuscate the plain text both word by word and line by line. The implementation screen shot of the WMRADO and MRADO technique is shown in figure 4 and figure 5. The same obfuscation technique is applied in line by line obfuscation and the produced obfuscated text is cGK which is shown in figure 5. It takes additional time to generate magical rolling alpha-digits square. but It takes less time for obfuscation and de- obfuscation process. The randomness of the value of MRADO square enhances the security of the obfuscated text. In the aspect of security enhancement, one more input value called seed value is included. Based on the seed value, the MRADO square is constructed. The seed value must be in between 1 to 64. That indicates the position of the Alphabets and digits. This technique obfuscates the data in both ways like word by word and line by line.

There are lot of CSP's which offers Storage as a Service (StaaS) for users. 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

Table 1
Estimated cost for Google cloud data storage

Plain Text File size (MB)	*Total cost per Month for Plain Text($)*	*Obfuscated File Size using MONcrypt (KB)*	*Obfuscated File Size (KB)*		*Total Cost per Month of using MONcrypt($)*	*Total Cost per Month of using MRADO ($)*	
			WMRADO	*MRADO*		*WMRADO*	*MRADO*
1	11	160	546	86	1.76	5.86	0.88
2	22	321	1094	171	3.41	11.75	1.87
3	33	481	1640	256	5.06	17.62	2.75
4	44	642	2186	341	6.93	23.48	3.63
5	55	802	2732	426	8.69	29.35	4.62

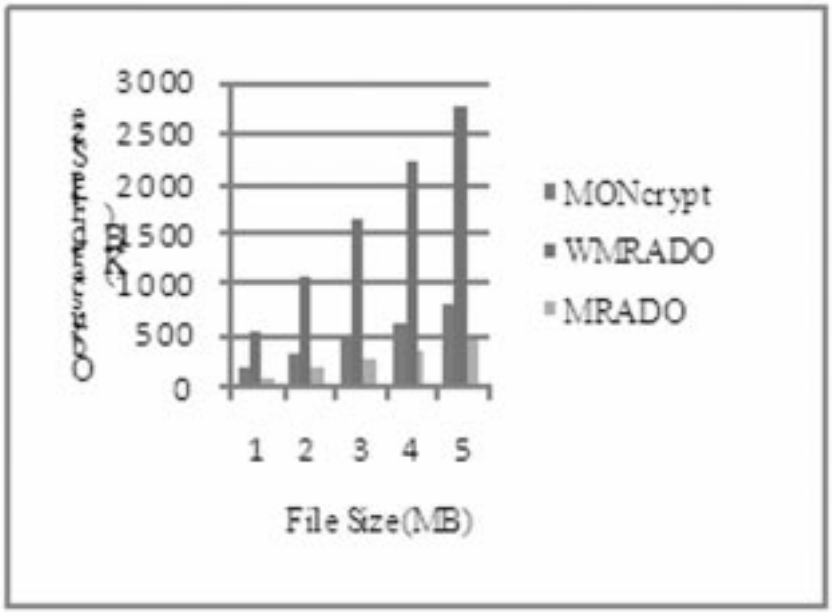


Figure 2: Comparison of Obfuscated File Size

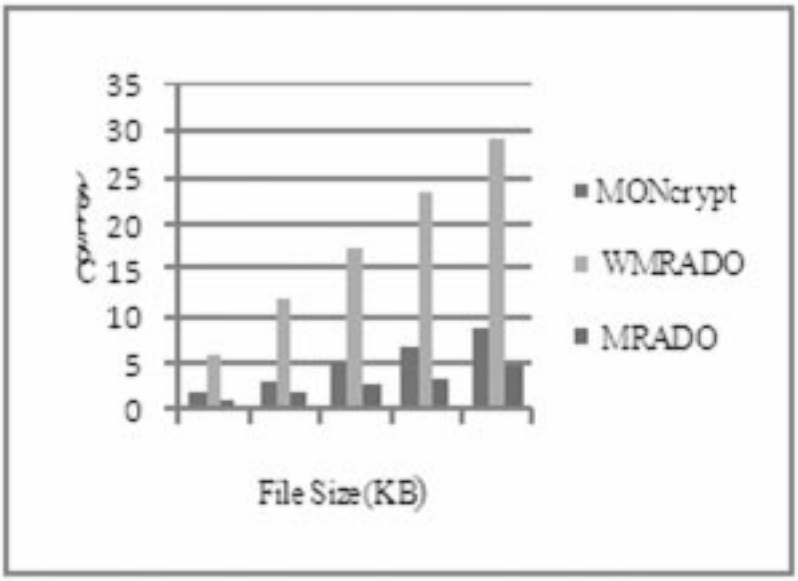


Figure 3: Comparison of Total Cost

Figure 4: Obfuscation using WMRADO Technique

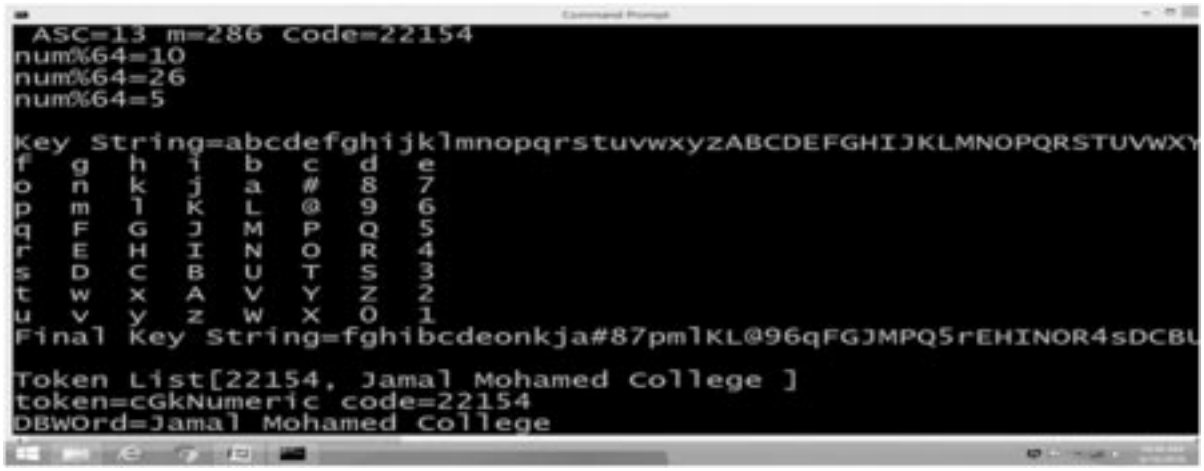


Figure 5: Obfuscation using MRADO Technique

calculated by using Google cloud storage cost. It is observed that the obfuscated file size is highly reduced in line by line obfuscation method than word by word obfuscation method. But, the security is high in the both techniques than the existing MONcrypt technique. This WMRADO and MRADO technique obfuscates both the numerical as well as non numerical data. In word by word obfuscation, the data size for the above plain text is 21 bytes and the obfuscated file size is 8 bytes. Whereas in line by line obfuscation, the obfuscated file size is 3 bytes only. It is decreased by one seventh. It enhances the security of the obfuscated text. Table 1 denotes the size of the existing and proposed obfuscated text. Graphical representation of obfuscated file size and total cost is shown in figure 2 and figure 3. It is observed that whenever the plain text file sizes increases from kb to mb, the obfuscated file size will also decrease from mb to kb.

7. 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 as well as transit. This paper discusses confidentiality enabled obfuscation technique named as MRADO. According to this technique, data are obfuscated before they are uploaded to the cloud storage. It performs the obfuscation line by line as well as word by word instead of performing the character by character obfuscation. So the size of obfuscated text is reduced. An experimental result shows that MRADO technique enhances the data security and also reduces the cost of data storage compare to the existing MONcrypt technique.

REFERENCES

[1] Buyya R, Vecchiola C, S. ThamaraiSelvi.," Mastering Cloud Computing Foundations and Applications Programming" *Elsevier*, 1-469,2013.

[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 Publishers*, **25**, 599–616, 2009.

[3] Furht B., "Cloud computing fundamentals. Handbook of Cloud Computing" *Springer Science*, 1–17, 2010.

[4] Sandeep K.Sood.," A combined approach to ensure data security in cloud computing" *Journal of Network and Computer Applications*, **35**,1831-1832, 2012.

[5] L. Arockiam, S. Monikandan, P. D. Sheba K Malarchelvi., "Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage" *International Journal of Computer Applications*,**88**,17-21,2014.

[6] Data Obfuscation 2013.Available from: *http://www.techopedia.com/definition/25015/ data obfuscation-do.*

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

[8] Robertson C. PDF obfuscation - A primer. 2012. Available from: *https://www.sans.org/reading-room/whitepapers/ engineering/pdf-obfuscation-primer-34005*.

[9] S. Monikandan , L. Arockiam.," Confidentiality Technique to Enhance Security of Data in Public Cloud Storage using Data Obfuscation" *Indian Journal of Science and Technology*,**8**,1-10,2015.

[10] S. Arul Oli, L.Arockiam.," Enhanced Obfuscation Technique for Data Confidentiality in Public Cloud Storage" *MATEC Web of Conferences*, 1-5, 2016.

[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, IEEE*,1–9,2014.

[12] 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*, **2**,260-263,2015.

[13] 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**,669-675,2014.

[14] Dr.D.I.George Amalarethinam, B.FathimaMary., "Data Security Enhancement in Public Cloud Storage using Data Obfuscation" *Perspective in Science, Elsevier*,2016.(communicated).

[15] https://cloud.google.com/products/calculator/#id=d969f758-720a-4003-9ac2-a85668e672cb.