International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

GLEncObfus-Encryption and Obfuscation Technique to Enhance Data Protection in Public Cloud Storage

D. I. George Amalarethinam, Lalu P. George, Anjana S. Chandran

Abstract— There is a rapid increase in data volume all over the world. In the computer network world also, imminent changes are happening. Under any circumstance, data can be vulnerable from one's own side or by a service provider or on data movement. In that case we need to secure our data. In this paper, the improved methods of protection against data leakage has been discussed. Public cloud data theft can happen through intruders or hackers or service providers. The data securing algorithm are used prior to storing the data in the server. Any data entering the cloud area is segregated into numerical and non-numerical parts, where non-numeric is operated by one algorithm and obfuscation method is applied on the numeric part. These two operations are done simultaneously with different threads. This both works come together and developed an entirely different algorithm. Hence the proposed algorithm maximizes the security and reduces the service cost. The proposed method is implemented as a cloud application and hosted on a cloud platform as a service and tested by subsisting present methods with respect to time and security levels. From the results, it is observed that the proposed method GLEncObfus is more efficient than present methods with reference to encryption-obfuscation time, decryption-de-obfuscation time and security level.

Keywords : Cloud computing, Cloud security, Secure outsourcing, Public cloud.

I. INTRODUCTION

In the cloud, data can be accessed virtually and stored in public, private or in hybrid. There are many advantages in cloud structure- anytime data accessibility, less investment and quick geographic coverage. [1][2]. But may reduce the data security. Presently data in the cloud are increasing very highly and it can be stored anywhere. Due to rapidly increasing data volume, data vulnerability is also increasing. Nowadays, data can be stored in any places in the world, so everywhere this is a need to check data security. This increase in data volume demands the security of data [3][4][5]. Mostly in the internet world data are stored in server or storage device, given by the service provider. The sensitive data may be lost or damaged without the administrator's knowledge or through mishandling, or by hackers [6][7]. Security may be implemented in hardware side, bulk data storing area, live server, movement of data from one place to another, encryption-decryption algorithm and key side algorithm [8]. In the cyber area, every day new developments are coming in cloud computing, fog computing, internet of things like physical developments. All these developments are nothing without a network connection and data storage [9]. In the network field, current network technologies are giving different types of capabilities against the network attack.

In this era of drastic development, cloud computing security is the most important. Different types of attack may happen in the cloud network field like malware injection attacks, cloud service abuse, service denial, service channel attacks, wrapping attack, a man in the middle attack, Spector and Meltdown persistent, etc. [10] [11] [12]. Threats are found out easily through different test-penetration test vulnerability test, network scanning and tools like Snort and nexus [13] [14] [15]. This issue can be addressed through encryption and decryption methods. If the algorithm is weak, anyone can easily identify the methods of algorithm or key [16] [17] [18] [19]. Cryptography is the method of writing secret codes. Through cryptanalysis one can break the code in different parts and find out the solution to open the original file or data. In cryptography there are differing modes like encryption, decryption, key management to ensure security in every aspect [20] [21] [22].

To develop a secured method for encryption and decryption. The proposed algorithm can be applied for both numeric and non-numeric formats. After determining the numeric and non-numeric value from normal text, encryption procedure is applied in non-numeric and obfuscation procedure is applied in a numeric value. Encryption is applied to GLEnc [23]. In this encryption procedure the real text is converted into ASCII decimal value, after splitting and dividing into different format, applying different types of key, rotating and application of XOR, final results are obtained in highly encrypted text. The obfuscation is done on GLObfus [24].

Manuscript published on November 30, 2019.
* Correspondence Author
Dr. D. I. George Amalarethinam*, Bursar & Director (MCA), Associate Professor of Computer Science, Jamal Mohamed College (Autonomous), Tiruchirappalli – 620 020, Affiliated to Bharathidasan University, Tamil Nadu, India.(Email: di_george@ymail.com)
Lalu P. George, Research Scholar, Department of Computer Science Jamal Mohamed College (Autonomous), Affiliated to Bharathidasan University, Tiruchirapalli-620 020, INDIA. (Email : icelalu@gmail.com)
Dr.Anjana S. Chandran, Assistant Professor, SCMS School of Technology and Management, Cochin-683501, India.(Email : anjooosureshnair@gmail.com)

To get an Obfuscated text in GLObfus different types of splitting, addition and application of key are performed. Both GLEnc and GLObfus are working in parallels at the same time. Finally, an encrypted and obfuscated data is obtained.

II. RELATED WORK

Xiaoyu Li et al proposed one system for two factor public data encryption protection for cloud systems. Each user needs to satiate two requisites, one is user need to satiate the access policy and the other is user has a sanction key. This method supports the AND access policy enjoying the properties of cipher text with low consumption cost, at the same time data owner executes the user level revocation. This model is proven secure against chosen plain text attack. From this information it is experimentally proven that computational cost of encryption, decryption and attribute revocation is efficient when compared with some other technique [22].

Lalu P. George et al proposed an encryption algorithm named GLEnc, developed for non-numerical plain text. The original plain text is converted to ASCII decimal value. This value is again converted to binary values. Here it is split into Odd and Even blocks. After eight-bit block division two keys - k1, k2 are applied. Rotate the odd block into k1 times. Similarly rotate the even block in to k2 times. Then one's complement is applied again. Another k3 is generated from the key service area. Apply XOR application with each Odd and Even Blocks. k3 is then incremented to one of the each eight-bit values. After merging and division, highly encrypted cipher text is received [23].

Lalu P. George et al developed an obfuscation method Globfus for numerical plain text. Which interchanges the odd to even and vice versa. Corresponding positions are subtracted from the original value to calculate the squares and there after applying the key. After division with 256 the coefficient value is kept as a secret key. The mod values are converted into ASCII character. That ASCII again converted to cipher text. This is a powerful mechanism for numerical value using obfuscation method [24].

III. PROPOSED GLENCOBFUS

The proposed method is mainly going through encryption and obfuscation. Both are running in the same thread and finally getting an entirely different cypher text with minimum time.

1. The user's records submitted for encryption and obfuscation.
2. Information may also comprise both numerical and non-numerical.
3. Determine the non-numerical and numerical values from the plain text.
4. Encryption procedure is applied to non-numerical values.
5. Obfuscation technique is carried out to numerical values.
6. Encryption invokes GLEnc procedure.
7. Obfuscation invokes GLObfus method.
8. GLEnc and GLObfus approaches are accomplished in parallel.
9. Customer's information is encrypted and obfuscated using each GLEnc and GLObfus.

A. Procedure for GLEnc.

1. The given unique text is transformed into ASCII decimal value.
2. ASCII decimal values are converted into binary values is divided 0s' and 1s'
3. Binary values into 2 blocks based on odd or even position.
4. Dividing further to eight-bit blocks and applying two keys- k1 and k2
5. Rotate the bits in the block at k1 number of times from left to right, and other block- k2 times and apply 1's complement in each block.
6. Generate a key - k3 from any key service area and apply XOR
7. Finally producing a cipher text [23].

B. Procedure for GLObfus

1. Interchange the values in odd role to even and vice versa.
2. Get the location of every value
3. Subtract positional price from corresponding original values.
4. Calculate square for subtracted values in actual textual content.
5. Generate a key and apply it on squared values
6. Divide the values via 256 to locate the mod.
7. Convert the mod values into ASCII code.
8. ASCII to cipher text [24].

C. The Pseudo code GLEncObfus(PT)

1. Start
2. PT←Plaintext
3. Ki←Keys from KYaaS
4. N←Sizeof(PT)
5. Num(i)←isdigits(T(i))
6. Nonnum(i)←(!isdigit(T(i)))
7. Thread.globfus(num(i),K)- Call numerical values procedure
8. Thread.glenc(nonnum(i),Ki) Call non-numerical values procedure
9. Ciphertext(CT) is produced by the parallel execution of glenc() and globfus()
10. End

Thread.globfus(num(i), k) invokes the GLObfus manner. It ensures confidentiality of records by means of obfuscating the numerical values inside the plaintext. It also minimizes the dimensions of the facts to be sent to the cloud storage. For example, the size of the plaintext is four bytes, and after the obfuscation by using globfus, the size of obfuscated textual is reduced to one byte. Thread.glenc(nonnum(i), ki) invokes GLEnc procedure. It executes non-numerical information and produces ciphertext. Thus, GLEnc is a symmetric encryption method, which uses exceptional keys received from the key generation cloud service area. Keys are carried out at the statistics based totally on process derived in the GLEncObfus. As symmetric encryption algorithm, makes use of equal keys for both encryption and decryption the keys have to be kept safe. These two algorithms are executed simultaneously by running the threads.

GLEnc algorithms is applied for encrypting non-numerical values. So, the time taken for executing GLEncOBfus algorithm is very less.

IV. GLENCOBFUS EXECUTION PROCEDURE & RESULTS.

The precise execution of **GLEncObfus** is defined below.The following student information are considered: Name, Reg Number, Class, Marks and Result.

The Plaintext is,

Table- 1: The Plain text value

S.Name	S.Class	Sub1	Sub2	Sub3	Sub4	Sub5	Result
Kumar	MSc	77	51	60	94	80	Pass

Here it contains combination of numerical and non-numerical values. To secure the full text, users should use GLEncObfus. The GlEncObfus procedure invokes GLEnc and GLObfus to produce ciphertext. The result of ciphertext produced by GLEncObfus is,

wX■Vô☺~Vû┘@└aQ╜Zμ╥i

Decryption is the reverse process of the same procedure. Here, One log file is used for the file that is produced after the encryption and obfuscation processes.For retrieval same procedure is carried out on the log file. So, the reverse process is easily done.

A. Simulation Result.

Table 2 shows the performance comparison of GLEnc and GLObfus together with GLEncObfus based on encryption and obfuscation time. The results show that GLEncObfus has taken minimum time duration than GLEnc and GLObfus together for encryption and obfuscation, decryption and de-obfuscation.

Users should pay a service cost for the services which are used from the cloud. The cost is based on the service. The proposed techniques in GLCaaS are also provisioned for the users at nominal cost. The cost is lower when the users choose GLEncObfus algorithm instead of GLEnc and GLObfus sequentially for securing the whole data in numerical and non-numerical types.

Table 2: Performance Comparison of GLEnc+GLObfus together and GLEncObfus Based on Encryption and Obfuscation Time

Size	GLEnc	GLEncObfus
	(Milliseconds)	
1 MB	226	207
2 MB	437	409
3 MB	669	613
4 MB	934	812
5 MB	1152	1089
10 MB	2492	2162
15 MB	3817	3365

Table 3 shows the performance comparison of GLEnc and GLObfus together with GLEncObfus based on decryption and de-obfuscation time. Here to also take different size of data. In each time thread execution is taking minimum time compared with one after another like GLEnc executing first and GLObfus executing second.

Table3 : Performance Comparison of GLEnc+GLObfus together and GLEncObfus Based on Decryption and De-obfuscation Time

Size	GLEnc	GLEncObfus
	(Milliseconds)	
1 MB	231	216
2 MB	449	428
3 MB	647	619
4 MB	867	833
5 MB	1108	1052
10 MB	2309	2201
15 MB	3446	3324

Let X be the cost for GLEnc in GLCaaS, for example X = Rs.100/-

Let Y be the cost for GLObfus in GLCaaS, for example Y = Rs.100/-

Let P be the cost for GLEncObfus in GLCaaS, for example P = Rs.150/-

Calculate cost when the users choose the GLEnc and GLObfus,

Cost_GLEnc_GLObfus = X + Y = 100 + 100 = Rs.200/-

Calculate cost when the users choose the GLEncObfus,

Cost_GLEncObfus = P = Rs.150/-

Let's take a simple example of real-life situation for a better understanding. In the first scenario, consider a shopping mall, where different products are displayed in the rack. Among them single pears soap costs Rs.45/-. In the same rack, displayed in a pack of three pears soap at the cost of Rs.110/-. People who adequately use pears soap will definitely buy three soaps in the pack for Rs.110/-.

In the second scenario, in the same shopping mall, where a bread pack costs Rs.15/- and butter costs Rs.15/-. Users could buy these two products individually for Rs.30/-. At the same time, a pack of bread and butter together costs Rs.25/-. People who want these two products will definitely prefer to buy the pack of bread and butter at the cost of Rs.25/-. In the same way users who want to hide all data with minimum cost and maximum security would choose GLEncObfus.

GLEncObfus is developed as a web service and hosted in the cloud server. The data are submitted to proposed encryption algorithm, and then they are encrypted and obfuscated before being uploaded to the cloud storage. Security level is analysed by using ABC Hackman tool. This tool analyses the security level of three security service algorithms.

Performance and security level of proposed GLEncObfus are compared with GLEnc and GLObfus individually. Simulation study is conducted for different sizes of data. For each size of data, time taken for encryption and obfuscation, decryption and de-obfuscation, and security level are measured and evaluated.

Performance of proposed technique is measured by the time taken to complete encryption and obfuscation, decryption and de-obfuscation process.

Table 4 represents the performance comparison of GLEnc, GLObfus and GLEncObfus. The time taken is calculated for different sizes of data.

Table 4: Performance Comparison of GLEnc, GLObfus and GLEncObfus separately Based on Encryption and Obfuscation Time

Size	Algorithms in GLCaaS		
	GLEnc	GLObfus	GLEncOb
	(Milliseconds)		
1 MB	195	19	207
2 MB	389	48	309
3 MB	592	77	613
4 MB	799	112	812
5 MB	1005	143	1089
10 MB	2137	313	2162
15 MB	3291	472	3365

\

The results show that compared to the GLEnc and GLncObfus, the GLObfus has taken minimum time duration for obfuscation.

Table 5 represents the performance comparison of decryption and de-obfuscation of GLEnc, GLObfus and GLEncObfus. The time taken by the GLEnc, GLObfus and GLEncObfus is calculated for different sizes of data.

Table 5: Performance Comparison of GLEnc, GLObfus and GLEncObfus separately Based on Decryption and De-Obfuscation Time

Size	Algorithms in GLCaaS		
	GLEnc	GLObf	GLEncObfus
	(Milliseconds)		
1 MB	208	19	216
2 MB	416	31	428
3 MB	599	45	619
4 MB	812	49	833
5 MB	1043	59	1052
10 MB	2198	111	2201
15 MB	3318	124	3324

The results show that the GLObfus obfuscation method has taken minimum time duration for de-obfuscation than GLEnc and GLEncObfus

B. Comparison of Encryption Algorithms with respect to Security.

Table 6 represents the comparison of security level. Security level is analysed through a security analysis tool called ABC hackman. This tool analyses the safety level of proposed and current strategies. This device is hooked up in cloud server for reading the safety stage of proposed algorithm. It uses exceptional assaults like dictionary and brute force attack to retrieve the authentic textual content. At the end of retrieval, hackman compares the plain text with retrieved textual content to find the share of original text retrieval. Based on percentage of comparison, safety stage of the proposed set of rules is measured. In this manner, safety stage of current cryptographic techniques is calculated and compared with the proposed GLEncObfus. The result shows that the proposed GLEncObfus possesses a maximum level of security than GLEnc and GLObfus.

Table 6: Comparison of Security Levels of GLEnc, GLObfus and GLEncObfus

S. No.	Security	Security Level
1.	GLEnc	91
2.	GLObfus	93
3.	GLEncObfus	94

The results show that the GLObfus has taken minimum time duration compared with GLEnc and GLEncObfus. GLEncObfus produces 94% of security level, compared with GLEnc and GLObfus.

GLEncObfus in entire environment gives maximum security level and ensures the confidentiality of the non-numerical and numerical data stored in the public cloud environment.

V. CONCLUSION

With the exploited growth of the internet and easy accessibility of data, data safety is a major concern. Everybody needs to think about the safety of data. So many solutions exist in the real scenario. But still theft can happen through any of the loopholes. GLEncObfus method, hosted in the cloud server is one fine solution where the data are submitted to newly generated encryption algorithm and then they are encrypted and obfuscated before being uploaded to the cloud storage. So, there is no need to have more concern towards the security of the data. Because of the simultaneous process of encryption of non-numerical data and obfuscation of numerical data, security have been enhanced. Since both threads are running at the same time, there is a quick delivery of results and consumption of time is also minimized. Hence, this is an efficient method.

REFERENCES

1. P. Ravi Kumar, P. Herbert Rajb, P. Jelcianac ,"Exploring Data Security Issues and Solutions in Cloud Computing", PP.691–697, Procedia Computer Science 125 (2018).
2. Rongzhi Wang, "Research on data security technology based on cloud storage", PP.1340 – 1355, Procedia Engineering 174 -2017.
3. Huaqing Lin, Zheng Yan , Yulong Fu, "Adaptive security-related data collection with context awareness",ELSEVIER, PP-88-103, Journal of Network and Computer Applications 126 (2019)
4. B. Wang, B. Li, and Hui. Li, ''Oruta: Privacy-preserving public auditing for shared data in the cloud,'' IEEE Trans. Cloud Computing., Vol. 2, No. 1, PP. 43–56, Jan./Mar. 2014.
5. Ibrahim Elgendi, Md. Farhad Hossain,Abbas Jamalipour , and Kumudu S. Munasinghe ," Protecting Cyber Physical Systems Using A Learned Mape-K Model",IEEE Access PP.90954-90963 , Vol 7, 2019 .
6. David H Deans "How public cloud continues to drive demand for cybersecurity solutions",www.cloudcomputing-news.net/news/2019/jul/12/public-cloud-drives-demand-for-cybersecurity-solutions,12 July 2019.
7. Chris Woodford "Cloud computing",https://www.explainthatstuff.com/cloud-computing-introduction.html, May 11, 2019.

8. O.Mirzaei,J.M.deFuentes,J.Tapiador,L.Gonzalez-Manzano, "Anadaptive Android obfuscation detector",PP.240–261,Elsevier,Future Generation Computer Systems90(2019).
9. ShiviGarg n, NiyatiBaliyan,"Data on Vulnerability Detectionin Android",PP.1081–1087,Elsevier-DatainBrief22(2019).
10. Mate Horvath, Levente Buttyan,"The Birth of Cryptographic Obfuscation∗ – A Survey ",The research presented in this paper was supported by the National Research, Development and Innovation Office – NKFIH of Hungary under grant,PP.1-59,January 7, 2018.
11. Rishab Goyal,Venkata Koppula,Brent Waters,"Lockable Obfuscation",PP.612-621 , IEEE Computer Society,0272-5428,2017.
12. Hanlin Zhang,Jia Yu , Chengliang Tian, Pu Zhao,Guobin Xu, Jie Lin,"Cloud Storage for Electronic Health Records Based on Secret Sharing With Verifiable Reconstruction Outsourcing",PP.40713-40721, IEEE Access Volume 6, 2018.
13. Hong Zhao , Zhaobin Chang , Weijie Wang, Xiangyan Zeng, "Malicious Domain Names Detection Algorithm Based on Lexical Analysis and Feature Quantification ", PP. 128990-128999,IEEE Access Vol 7, 2019.
14. Abhishek Kumar, Aditya Kaushik, Akanksha, Automated Man-power Data Analysis for Corporates, International Journal of Electronics Engineering (ISSN: 0973-7383) Volume 11, Issue 2 pp. 1-10 June 2019-Dec 2019.
15. Babatunde O. Lawal, Okesola, J. Olatunji," Managing Network Security with Snort Open Source Intrusion Detection Tools". International Conference on Science, Technology, Education, Arts, Management and Social Sciences iSTEAMS Research Nexus Conference, Nigeria, PP.471-482 May, 2014.
16. Shyam Nandan Kumar, "Review on Network Security and Cryptography ", International Transaction of Electrical and Computer Engineers System, PP-1-11, Vol. 3, No. 1,2015.
17. Jiale Zhang , Bing Chen, Yanchao Zhao , Xiang Cheng ,Feng Hu,"Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues", PP.18209-18237 , IEEE Access Vol 6, 2018.
18. Samarjeet Yadav, Vijay Tiwari, "Encryption And Obfuscation :Confidentiality Technique For Enhancing Data Security In Public Cloud Storage", PP.33-39 , JCIT Vol. 9(3), (2018).
19. D.I. George Amalarethinam, H.M. Leena,"A new key generation technique using GA for enhancing data security in cloud environment", Int. J. Cloud Computing, Vol. 7, No. 1, 2018.
20. Takayasu Fushimi,Kazumi Saito,TetsuoIkeda,Kazuhiro Kazama , "Estimating node connectedness in spatial network under stochastic link disconnection based on efficient sampling", Springer Open PP.1-24 Applied Network Science4:66 (2019)
21. Lifeng Zhou, Chunguang Li, "Outsourcing Large-Scale Quadratic Programming to a Public Cloud", IEEE Access, PP.2581-2589, Vol 3 ,2015.
22. Xiaoyu Li, Shaohua Tang, Lingling Xu, Huaqun Wang, Jie Chen, "Two-Factor Data Access Control With Efficient Revocation for Multi-Authority Cloud Storage Systems",IEEE Access PP.393-405, Vol 5, 2017.
23. Lalu P. George , Dr.D.I. George Amalarethinam ,Dr.Anjana S. Chandran, "GLEnc Algorithm to Secure Data in Public Cloud Environment", IEEE Xplore, DOI: 10.1109/ICACCI.2018.8554451, PP.2018-2021 ,Dec 2018.
24. Dr. D. I. George Amalarethinam, Lalu P. George, Dr. Anjana S. Chandran," GLObfus Mechanism to Protect Public Cloud Storage",American International Journal of Research in Science, Technology, Engineering & Mathematics, Special Issue of 5thInternational Conference on Mathematical Methods and Computation (ICOMAC – 2019), pp. 313-316, February 2019