International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Hybrid Text and Value Based Ncryption and Obfuscation (Tvbencobfus) To Safeguard Data in Cloud Storage Server

B.Rex Cyril, S.Britto Ramesh Kumar

***Abstract:** The proposed hybrid encryption and obfuscation technique are more efficient than previously proposed two algorithms. Because this technique considers all types of data which are ready to be uploaded to the cloud. It integrates the independent two procedures into a single procedure and executes both procedures in a parallel manner. For Example, if we consider data with a mixer of text and value-based, then, the proposed algorithm is called the tbenc() and vbobfus() procedure for text and value-based data respectively.*

***Keywords:** Cloud Computing, Security, value based, text-based,Encryption*

I. INTRODUCTION

Cloud computing provides more sophisticated data storage. Data in the cloud are replicated in multiple data centers located in different geographical locations. Each data center is controlled and monitored by several administrators of the CSPs. Users are not able to locate the particular place of the data stored in cloud servers. Users' data are hacked from any cloud data center situated in different geographical locations. CSP should ensure the protection of unwanted entry of cloud users into the places where they are not permitted to access. The security issue is addressed by the proposed algorithms and techniques [Sat, 12]. Users may choose either TBEnc or VBObfus based on their necessity. The CTs in EOaaS individually perform well and protect the data in the cloud storage. TBEnc technique gives better security for the text-based data, and VBObfus gives better security for the value-based data. If users want to secure all the data such as text and value-based, they should choose TBEnc and VBObfus Confidentiality Techniques one by one. Users should pay for the service cost of TBEnc and VBObfus separately. Instead, users could choose TVBEncObfus which is proposed in this chapter. TVBEncObfus is a single CT to secure all types of data like text and value-based in the cloud. If the users wish to protect all types of data then they should choose this CT in the EOaaS. Cost of TVBEncObfus is lower than the total cost of TBEnc and VBObfus used together.

Manuscript published on 30 August 2019.

***Correspondence Author(s)**
B.Rex Cyril, Research Scholar and Asst. Professor, Department of Computer Science, St.Joseph's College(Autonomous), Trichy, Tamilnadu, India
S.Britto Ramesh Kumar, Asst. Professor, Department of Computer Science, St.Joseph's College(Autonomous), Trichy, TamilNadu, India.

1.2. Objectives

This section describes the objective of the chapter.

- To propose a hybrid security algorithm to ensure the security of text and value-based data using encryption and obfuscation.
- To maximize the security and reduce the cost of confidentiality echnique used from EOaaS.

1.3. Methodology

The SECON framework has three confidentiality techniques in EOaaS. The CT, TVBEncObfus is proposed for data security. It is one of the CTs in EOaaS. Among the three CTs in EOaaS, users could choose a CT for the data protection according to their requirement. If the users need to protect all the data such as text and value-based, then they should choose TVBEncObfus. The methodological diagram of TVBEncObfus is represented in Figure 5.1.

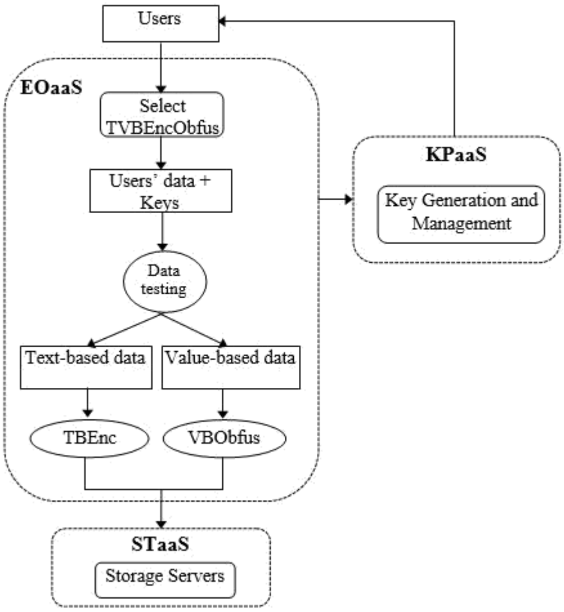

Figure 1.1. Methodological Diagram of TVBEncObfus

According to the framework SECON, the data are secured using the proposed encryption and obfuscation technique before the data are sent to the storage server. Initially, the TVBEncObfus analyses users' data to determine the type of data. Value-based data are obfuscated by the obfuscation technique, and text-based data are encrypted by encryption technique. The execution of the two techniques is begun simultaneously.

*Retrieval Number: J97150881019/19©BEIESP
DOI: 10.35940/ijitee.J9715.0881019
Journal Website: www.ijitee.org*

*Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.*

Keys used for the CT are created in KPaaS, and they are dispatched to the users. Users apply the keys with TVB Enc Obfus. Keys used by TVB Enc Obfus are not communicated to the CSPs.

1.4. Proposed Hybrid TVBEncObfus

TVBEncObfus is a hybrid algorithm; it integrates both text and value-based procedure into one algorithm. It helps the users to protect the data in all types. It produces better performance compared with other proposed algorithms. Steps involved in the TVBEncObfus are as follows:

1. Users have to submit their data.
2. Both text and value-based data are processed by this algorithm.
3. Split the text-based and value-based data from the users' input.
4. Text-based Encryption is invoked for text data
5. Value-based obfuscation is applied for value-based data.
6. TBEnc and VBObfus are called Text and Value-based data respectively.
7. Both procedures are executed in parallel.
8. Users' data are encrypted as well as obfuscated.

1.4.1. Pseudo Code of Proposed TVBEncObfus

The pseudo code of TVBEncObfus is given below.

```
sub tvbencobfus(PT)
1.  PT←plaintext
2.  N← sizeof(PT)
3.  for i=1 to N then
        if ( isdigits(PT(i))) then
        value←value+PT(i)
        else
        text←text+PT(i)
        end if
4.  end for
//  call to TBEnc
5.  Thread.tbenc(text)
//  call to VBObfus
6.  Thread.vbobfus(value)
7.  end
```

1.4.2. Sample Experiment of TVBEncObfus Procedure

The proposed hybrid encryption and obfuscation technique are more efficient than previously proposed two algorithms. Because this technique considers all types of data which are ready to be uploaded to the cloud. It integrates the independent two procedures into a single procedure and executes both procedures in a parallel manner. For Example, if we consider data with a mixer of text and value-based, then, the proposed algorithm is called the tbenc() and vbobfus() procedure for text and value-based data respectively.Sample plaintext considered for TVBEncObfus() procedure,: is the data taken from students mark statement.

Name	Class	Mark1	Mark2	Mark3	Mark4	Total	Result
Arabindu	II M.Sc	80	84	79	93	336	Pass

The proposed technique encrypts and obfuscates the text and value-based data. The tvbencobfus() identifies the text and value-based data in the plaintext considered for security. It splits the text and value-based data and invokes the text-based and value-based procedures simultaneously. Now both the procedures are executed in a parallel manner and produce a result as shown below.

Name	Class	Mark1	Mark2	Mark3	Mark4	Total	Result
ç dx»ïf	⌡ →²º=ç	·	P	ⁿ	Γ		û àÿ

The result shown above clearly describes that no one can retrieve the data without knowing the key of the encryption and obfuscation. This proposed TVBEncObfus hides all types of data. Hence the cryptanalyst could not get any pattern and ideas to get the original data.

1.5. Simulation Results

The proposed algorithm is implemented in the same way as used in the previously proposed two confidentiality techniques. This proposed technique is compared with TBEnc and VBObfus techniques with respect to time, size and Security level. Table 5.1 and Figure 5.2 demonstrate the comparison of TVBEncObfus with TBEnc and VBObfus based on performance encryption and obfuscation time taken for all the three algorithms.

Table 1.1 Comparison of TVBEncObfus with TBEnc+VBOfbus based on Encryption and Obfuscation Time

Size	TBEnc +VBObfus	TVBEnc Obfus
	(Milliseconds)	
1 MB	306	245
2 MB	545	472
3 MB	735	672
4 MB	1088	892
5 MB	1227	1113
10 MB	2352	2258
15 MB	3486	3392

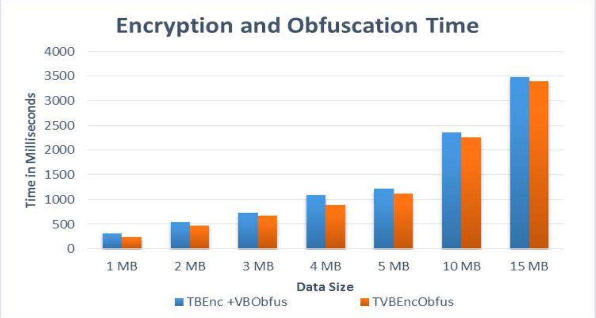

Figure 1.2. Comparison of TVBEncObfus with TBEnc+VBOfbus based on Encryption and Obfuscation Time

Table 5.2 and Figure 5.3 demonstrate the comparison of TVBEncObfus with TBEnc and VBObfus based on performance Decryption and Deobfuscation time taken for all the three algorithms.

Table 1.2. Comparison of TVBEncObfus with TBEnc+VBOfbus based on Decryption and Deobfuscation Time

Size	TBEnc +VBObfus	TVBEncObfus
	(Milliseconds)	
1 MB	288	238
2 MB	491	442
3 MB	699	632
4 MB	903	846
5 MB	1143	1063
10 MB	2297	2221
15 MB	3408	3347

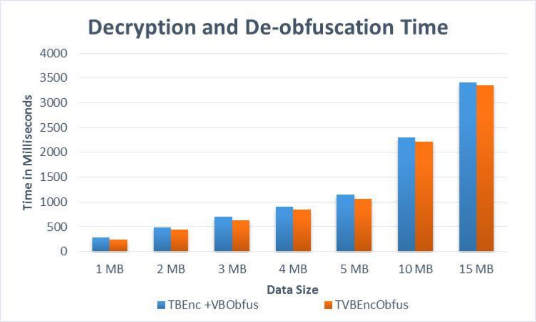

Figure 1.3. Comparison of TVBEncObfus with TBEnc+VBOfbus based on Decryption and Deobfuscation Time

The results show that TVBEncObfus takes minimum time duration than TBEnc+ VBObfus 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 EOaaS are also provisioned for the users at a nominal cost. The cost is lower when the users choose TVBEncObfus instead of TBEnc and VBObfus sequentially for securing the whole data in text and value-based types.

Let A be the cost for TBEnc in EOaaS, for example, A = Rs.1000/-

Let B be the cost for VBObfus in EOaaS, for example, B = Rs.1000/-

Let X be the cost for TVBEncObfus in EOaaS, for example X = Rs.1300/-

Calculate cost when the users choose the TBEnc and VBObfus, Cost_TBEnc_VBObfus =

A + B = 1000 + 1000 = Rs.2000/-

Calculate cost when the users choose the TVBEncObfus,
Cost_TVBEncObfus = X = Rs.1300/-

Let’s take a simple example of a real life situation for a better understanding. In the first scenario, consider a shopping mall, where different products are displayed on the rack. Among them single Biscuit packet costs Rs.30/-. In the same rack, displayed in a pack of three biscuit packet at the cost of Rs.70/-is displayed. People who adequately consume biscuits will definitely buy three in the pack for Rs.70/-.

In the second scenario, in the same shopping mall, where a bread pack costs Rs.25/- and butter costs Rs.30/-. Users could buy these two products individually for Rs.55/-. At the same time, a pack of bread and butter together cost Rs.40/-. People who want these two products will definitely prefer to buy the pack of bread and butter at the cost of Rs.40/-. In the same way, users who want to hide all data with minimum cost and maximum security would choose TVBEncObfus. TVBEncObfus is developed as a web service and hosted in the cloud server. The data are submitted to the proposed encryption algorithm, and then they are encrypted and obfuscated before the data is sent to the storage server. Security level is analyzed by using ABC Hackman tool. This tool analyses the security level of three confidentiality technique algorithms. Performance and security level of proposed TVBEncObfus are compared with TBEnc and VBObfus individually. A simulation study is conducted for different sizes of data. For each size of data, the time taken for encryption and obfuscation, decryption and de-obfuscation, and security level is measured and evaluated. Performance of proposed technique is measured by the time taken to complete encryption and obfuscation, decryption and de-obfuscation process.

Table 1.3 and Figure 1.4 represent the performance comparison of TBEnc, VBObfus, and TVBEncObfus. The time taken is calculated for different sizes of data. .

Table 1.3. Performance Comparison of TBEnc, VBObfus, and TVBEncObfus Based on Encryption and Obfuscation Time

Algorithms in EOaaS			
Size	**TBEnc**	**VBObfus**	**TVBEncObfus**
	(Milliseconds)		
1MB	230	36	245
2MB	458	67	472
3MB	656	98	672
4MB	879	130	892
5MB	1092	161	1113
10MB	2243	333	2258
15MB	3378	489	3392

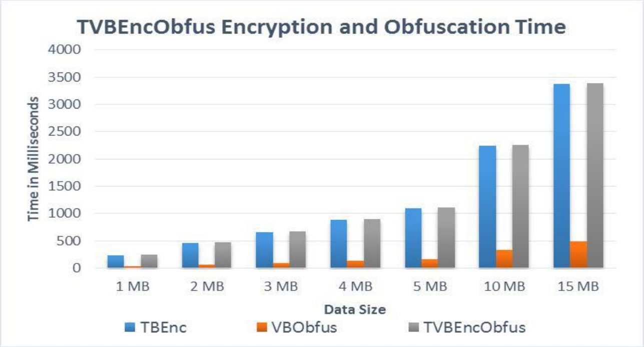

Figure 1.5. Performance Comparison of TBEnc, VBObfus, andTVBEncObfus Based on Encryption and Obfuscation Time

The results show that compared to the TBEnc and TVEncObfus, the VBObfus has taken minimum time duration for obfuscation.Table 1.4 and Figure 1.5 represent the performance comparison of decryption and de-obfuscation of TBEnc, VBObfus, and TVBEncObfus. The time taken by the TBEnc, VBObfus, and TVBEncObfus is calculated for different sizes of data.

Table 1.4. Performance Comparison of TBEnc, VBObfus and TVBEncObfus Based on Decryption and De-Obfuscation Time

		Algorithms in EOaaS	
Size	TBEnc	VBObfus	TVBEncObfus
		(Milliseconds)	
1 MB	225	24	238
2 MB	428	39	442
3 MB	617	55	632
4 MB	833	59	846
5 MB	1059	71	1063
10 MB	2206	117	2221
15 MB	3331	132	3347

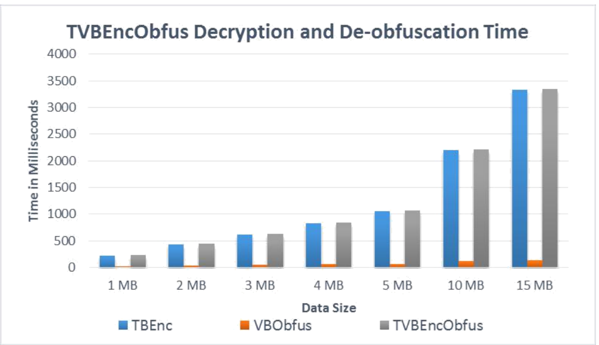

Table 1.4. Performance Comparison of TBEnc, VBObfus and TVBEncObfus Based on Decryption and De-Obfuscation Time

The results show that compared with TBEnc and TVBEncObfus, the VBObfus algorithm has taken a minimum time duration for de-obfuscation.Table 5.5 and Figure 5.6 represent the comparison of the security level. The result shows that the proposed TVBEncObfus possesses a maximum level of security than TBEnc and VBObfus.

Table 1.5. Comparison of Security Levels of TBEnc, VBObfus and TVBEncObfus

S. No.	Security Algorithms	Security Level (%)
1	TBEnc	91
2	VBObfus	92
3	TVBEncObfus	93.5

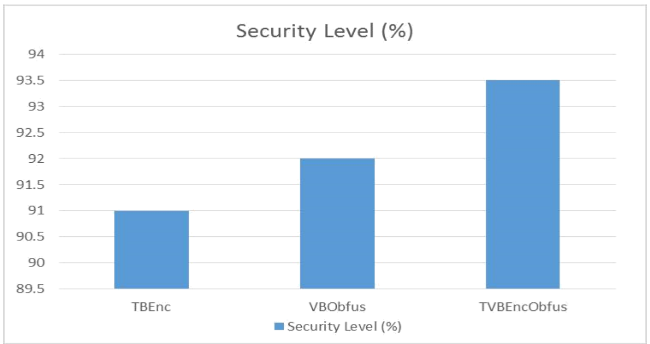

Figure 1.6. Comparison of Security Levels of TBEnc, VBObfus, and TVBEncObfus

The results show that the TVBEncObfus has produced maximum security when compared with TBEnc and VBObfus. TVBEncObfus produces 93.5% of security level, compared with TBEnc and VBObfus.

TVBEncObfus in EOaaS gives maximum security level and ensures the confidentiality of the text and value-based data stored in the public cloud environment.

1.6 Research Finding and Interpretation

TVBEncObfus is one of the CTs in the EOaaS. Users should choose the proposed CTs to secure all the data. Cost of choosing TVBEncObfus is low when users choose TBEnc and VBObfus together. The time taken for execution of TVBEncObfus is also minimum than the execution time taken for TBEnc and VBObfus sequentially. The keys used for TVBEncObfus are created in KPaaS and sent to the users. Users encrypt and obfuscate the plaintext in TVBEncObfus using keys. The keys are not communicated to CSPs.

II. CONCLUSION

This chapter has proposed a hybrid confidentiality technique for securing both text and value-based data. The proposed framework consists of this technique with the EOaaS. The framework enables users to choose this TVBEncObfus for their data protection. Users could receive the keys for executing this technique in their system setup. Users submit data and keys are processed based on the procedure described for the TVBEncObfus. It uses two techniques to protect the data, namely, encryption and obfuscation. Both types of data are considered separately and they executed encryption for text-based data and obfuscation for value-based data.A simulation experiment is conducted with real-time in a cloud environment. The output of the TVBEncObfus shows that it has consumed lesser time for obfuscation and encryption, decryption and de-obfuscation than TBEnc and VBObfus together. The cost of service consumed by the users is also minimum for the TVBEncObfus. TVBEncObfus produce maximum high-level security than other two proposed techniques. The following chapter demonstrates the design of a proposed secured framework named, SECON, with different confidentiality techniques to enable the safe infrastructure in the public cloud environment.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

REFERENCES

1. Sascha Fahl and Marian Harbach, “Confidentiality as a Service – Usable Security for the Cloud”, *Proceedings of IEEE International Conferenceon Trust, Security and Privacy inComputing and Communications*, 2012, pp. 153-162.
2. Satyendra Singh Rawat and Niresh Sharma, “A Survey of Various Techniques to Secure Cloud Storage”, *International Journal of ComputerScience and Network Security*, Volume 12 Issue 3, 2012, pp. 116-121.
3. Pardeep Sharma, Sandeep K. Sood, and Sumeet Kaur, “Security Issues in Cloud Computing”, *High Performance Architecture and GridComputing Communications in Computer and Information Science,* Volume 169, 2011, pp 36-45.
4. Shirole Bajirao Subhash and Dr Sanjay Thakur, “Data Confidentiality in Cloud Computing with Blowfish Algorithm”, *International journal of Emerging Trends in Science and Technology*, Volume 1, Issue 1, 2014, pp. 01-06.
5. Shucheng Yu, Wenjing Lou, and Kui Ren, “Data Security in Cloud Computing”, *Handbook on Securing Cyber-Physical Critical Infrastructure*, Chapter 15, Elsevier, Morgan Kaufmann Publisher, 2012, pp. 389-410.
6. Shweta Kaushik, Charu Gandhi. "Cloud data security with hybrid symmetric encryption", 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016.
7. Siani Pearson, Yun Shen and Miranda Mowbray, “A Privacy Manager for Cloud Computing”, *Proceedings of International Conference on Cloud Computing*, Springer-Verlag Berlin, Heidelberg, LNCS Volume 5931, 2009, pp. 90-106.
8. Subashini S and Kavitha V., “A Survey on Security Issues in Service Delivery Models of Cloud Computing”, *Elsevier Journal of Network and Computer Applications*, Volume 34, Issue 1, 2011, pp. 1-11.
9. Subhasri P. and Padmapriya A., “Multilevel Encryption for Ensuring Public Cloud”, *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 7, 2013, pp. 527-532.
10. Sudha M and Monica M, “Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography”, *Advances inComputer Science and its Applications*, Volume 1, Issue 1, 2012, pp. 32-37.
11. Atiq, U.R. and M. Hussain, “Efficient cloud data confidentiality for DaaS”, International Journal of Advanced Science and Technology, volume 35, 2011, pp.1-10.
12. Mather T., Kumaraswamy S. andShahed, L., “Cloud security and privacy”, Chapter 4, O’Reilly Media, Inc, 2009, pp.61-71.
13. William, S., “Cryptography and network security: principles & practices”, Fifth edition, Prentice Hall, 2005, pp. 6-56.
14. Sascha, F., Marian, H., Thomas, M and Matthew, S., “Confidentiality as a service – usable security for the cloud”, IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 153-162.

AUTHORS PROFILE

Prof. B. Rex Cyril is working as Assistant Professor and pursuing doctor of philosophy in Department of Computer Science, St. Joseph’s College,(Autonomous),Tiruchirappalli, Tamil Nadu, India. He received his M.Phil degree from Prist University. He received his MSc degree from St. Joseph’s College, Tiruchirappalli. His area of interest is Cloud Security Services. He has published research papers in the National/ International Conferences and Journals

Dr. S.Britto Ramesh Kumar is working as Assistant Professor in the Department of Computer Science, St. Joseph’s College (Autonomous), Tiruchirappalli, Tamil Nadu, India He has published many research articles in the National/International conferences and journals. His research interests include Cloud Computing, Data Mining, Web Web Mining, and Mobile Networks.