ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 1, January 2016

Confidentiality Technique using Data Obfuscation to Enhance Security of Stored Data in Public Cloud Storage

S. Arul Oli[1], Dr.L. Arockiam[2]

Research Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, India.[1]
Dr. L. Arockiam, Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, India[2]

Abstract:Cloud computing is an upcoming paradigm that offers tremendous advantages. Data is processed, transferred and stored by non-internal service providers to use full potential of cloud computing. It provides users a large space to store data. However, data users are very cautious to store their data outside their own control limits and securing data in remote places have become important issues. Hence, Security is needed both in private and public cloud sphere. Security issues are considered more important for protection of sensitive data, since security is not guaranteed much in public cloud. Relying on standard encryption process is not enough since stored data has the possibility with threatening elements. The available techniques also do not serve the purpose of protecting the data. This paper proposes an obfuscation technique to strengthen a numerical data in public cloud storage. The obfuscation method is used to encrypt the numerical data before uploading into cloud storage. The cryptographic systems are used to strengthen the data confidentiality in protecting sensitive data before storing into cloud storage. The sample experiments are done and the results are obtained.

Keywords: Cloud Storage; Obfuscation; Confidentiality; Cryptography; Symmetric Encryption;

I. INTRODUCTION

Security in cloud computing nowadays is becoming more and more challenging due to its popularization. While the users enjoy the conveniences and advantages that cloud computing has brought, it has also brought the risks and challenges with it. So it is necessary to analyse the main risks thoroughly to guarantee the protection to the user's information. In recent times, massive security issues happened frequently with cloud computing providers. On February 15th, 2008, Amazon experienced network server downtime that affected thousands of websites which applied Amazon EC2 cloud computing and S3 cloud storage, including Twitter, SmugMug, 37Sigals and Adaptive Blue. In 2009, Google Gmail had a global malfunction and services were suspended longer than four hours because one of the data centres in Europe was under maintenance while the other one was overloaded and this caused chain effect to other data centres. In the same year, a large number of user files leaked in Google. On 15 March 2009, Microsoft Azure was suspended about 22 hours, however the detail of cause has not been given by Microsoft. On 11 June 2009, Amazon EC2 service was interrupted for several hours due to the broken electrical equipment that supplied data centre damaged by lightning stroke [1]

While security in general has become important, the security of data of each user in cloud has been considered more important for protection. Cryptography is a technique applied for encryption and decryption of data. The several techniques are classified into two major groups namely conventional and public key Cryptography [2]. Conventional cryptography is also referred as symmetric encryption or single key encryption. Same key is used for encryption and decryption. Public keycryptography is referred as asymmetric encryption or public key encryption and separate keys are used for encryption and decryption in public key encryption technique.

Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g., the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Encrypting data in transit also helps to secure it as it is often difficult to physically secure all access to networks. When a message is decrypted, it is returned to its original readable form. Encryption can provide strong security for data to give sensitive data the highest level of security. The goal of encryption is to make data unintelligible to unauthorized readers and extremely difficult to decipher when attacked. The security of encrypted data depends on several factors like what algorithm is used, what is the key size and how was the algorithm implemented in the product.

Brian Hay et. al[3] focused on data authentication, data integrity, querying and outsourcing the encrypted data. Data encryption refers to the technique that uses cryptography theory to encrypt data on storage devices. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [4]. Cryptographic algorithm is a technique used for concealing the content of message from all users except the sender and the receiver and to authenticate the correctness of message to the recipient [5]. In [6] the authors evaluated the performances of

cryptographic algorithms (symmetric and asymmetric algorithms) in a cloud platform. Based on key size, the performance and the size of the output file, different encryption techniques in a cloud environment have been studied.

Many techniques are available to protect sensitive data of users from attackers and service providers. Our approach is to protect data confidentiality from service providers, and to ensure that service providers cannot tamper the data stored in cloud environments. CC fascinates the users with many advantages. However several important problems in encryption process are resolved through data obfuscation method. Obfuscation is another technique used for encrypting the data. It is hot topic now in the field of digital management, protecting against reverse engineering and tampering as discussed in [7]. Digital management is a question of making money by illegal copying and resale of software. At the same time, reverse engineering is on the increase by utilizing the prevalence of tools to assist this task. Tampering deals with the modification of software that contains encryption of keys. Obfuscation is a means for protecting the cloud. It is a technique to transform a source code into a functionality equivalent program that makes reverse engineering more complex [8] [9]. Code obfuscation could be classified according to the transformation subject into various classes.

The organisation of this paper is as follows. Section II deals with the related works of obfuscation. Section III explains the Proposed Obfuscation Technique of Aro_Obfus CT. Section IV gives the experiments of ARO_Obfus CT with sample data. Section V explains the results and findings. Section VI ends the conclusion.

II. Related Works

The authors [10] introduced Third Party Auditor between the service provider and the user, where the provider acts as external auditor for auditing the outsourced data of the user. This scheme provided secure and efficient dynamic operations on data blocks stored in cloud. The authors [11] proposed that asymmetric cryptography algorithms and digital signature techniques are reliable and efficient to provide more security of user's data in Cloud. Dai Yuefa et al. [12] analyzed data security as the requirements of cloud computing and have given an addition of mathematical model on the basis of these requirements.

Sheryl Duggins et al. [13] proposed an approach to protect software intellectual property by increasing its complexity to prevent reverse engineering. They also introduced four conjectures for software protection through obfuscation and provided rationale for why these four conjectures make logical sense. They discussed the obfuscation for security, and explored the types of obfuscation used for defences against malicious attacks. They also discussed three types of attacks namely software piracy, malicious reverse engineering, and tampering [14]

Varun Maheshwari et al. [15] introduced a scheme which allowed the user to store data in cloud and perform database style query on the stored data without using standard cryptography to maintain data confidentiality. They introduced the glyph image method for obfuscation, added noise and split glyph image into small portions. The authors [16] proposed two effective and flexible distributed features for an explicit dynamic data support to ensure data confidentiality which achieved the integration of storage correctness insurance and data error localization, and supported secure, effective and efficient dynamic operations on data blocks.

AtiqurRehman et al. [17] proposed a framework to store sensitive data with a combination of encryption and obfuscation. The cloud users maintained data storage to store keys that are used for encryption. This paper further proposed mechanism to query over encrypted and obfuscated data on server side. Once the required data is filtered on server side, then data is transferred on client side where de-obfuscation and decryption is performed. The authors [18] presented three approaches such as separating software and infrastructure service providers, hiding data owner's information in cloud and, data obfuscation technique for security. The authors [19] presented a framework with two-step encryption process which is used to completely protect the encrypted sensitive data from users to cloud and cloud to users.

Arockiam et al. [20] proposed the importance of security of data in Small and Medium scale Enterprises (SMEs). They proposed a new cryptographic algorithm for security named AROcrypt to ensure the security of data stored in cloud storage. This AROcrypt technique was based on a symmetric encryption provided through SEaaS model. In this model, encrypted data are stored on storage while secret keys are kept by data owner and access to the user is granted by issuing the corresponding keys for encryption and decryption. The data are encrypted before uploading into the cloud storage.

The authors in [21] proposed a framework called AROMO, which consists of three cloud services, namely, SEcurity as a Service (SEaaS), Key Generation and Management as a Service (KGMaaS) and STorage as a Service (STaaS). Three Security Service Algorithms (SSAs), namely, AROcrypt, MONcrypt and AROMONcrypt are provided for enhancing the security of data in cloud storage. SEaaS provides these security service algorithms as a service to the users of cloud storage where users have the liberty to choose any one SSA to secure their data. This AROMO is developed to secure data in cloud storage and to protect data from different threats. The researchers [22] proposed numerous unresolved security issues which threaten the storage in public cloud environment. They also pointed out various security concerns in relation with three basic services provided in cloud computing environment.

Anitha et al. proposed a method to provide protection to the data stored through metadata at the data server [23]. This process provided to protect with cipher key which is created from features of metadata. The time required in this model for generating the cipher key is proportional to the number of attributes in the metadata as well the algorithms used for cipher key generation. Their proposal envisioned safety through two novel features: On the one hand, security is provided by their proposed design, where the encryption and decryption keys will never be compromised without the involvement of data user and Metadata Data Server (MDS). On the other hand, the cipher key generated using the modified feistel network holds good for an avalanche effect as each round of feistel

function depends on the previous round value. This approach is time consuming for generation of cipher key.

Siani Pearson et al. [24] described a privacy manager, which reduces risk to cloud computing users of their private data being misused, stolen or tampered. The privacy manager uses a feature called obfuscation as a first line of defence. The idea is that instead of unencrypted form being present in cloud, the user's private data is sent to cloud in an obfuscated form. The obfuscation method uses a key chosen by user and known by privacy manager, and not communicated to service provider. Thus the service provider is unable to de-obfuscate user's data. This data is not present with service provider, reducing the risks of theft of data from cloud and unauthorized uses. Moreover, service provider is not subject to legal restrictions applying to processing of the un-obfuscated data.

Miranda et al. [25] described a privacy manager to control policy-based obfuscation and de-obfuscation of personal, sensitive, or confidential data within cloud system. Hence, cloud users foresee minimum risk of their sensitive data being stolen or tampered. In addition, the assistance is provided to cloud providers with the help of conforming to privacy law. They described different architectures for such privacy management in cloud computing, and have given an algebraic explanation of obfuscation features provided by privacy manager, and have described how policies may be defined to control such obfuscation.

Prasad Reddy et al. [26] provided maximum security and privacy to data stored on cloud by using Double Authentication and Hybrid Obfuscation Technique with the use of a plug-in for an internet browser. They proposed a plug-in keeps temporary log of obfuscation keys and it performs different functions. If the respective key of the file is present in log of plug-in then the data is de-obfuscated else data is not displayed or remains obfuscated. The data and keys are separately kept on different clouds with no direct communication between them by 'Divide and Rule' policy for safe and secured cloud environment.

Muhammad et al. [27] presented an approach to protect users' confidential data in cloud computing from cloud service providers. Their proposed approach has three features namely, separation of software and infrastructure service providers, hiding information about the owner of data and data obfuscation. Our cloud system architecture ensures that cloud service providers cannot know location of the users' data, access the user's data, or understand the meaning of the user's data simultaneously. The experimental results on the performance of data obfuscation and de-obfuscation show that the overhead for data obfuscation and de-obfuscation appear to increase linear with the size of input data. Their approach is scalable with size of input data.

Zeljko et al. [28] presented a program obfuscation method. It is based on the combination of strong encryption of code and data and a CPU simulator implementing the MIPS I instruction set. This method has the possibility of supplying decryption key to the simulator. They introduced different layers to make the hackers more complicated and confused. There are CPU simulator layer, the encryption layer, finding the encryption key, and deducing the encryption mode. The CPU simulator layer and the simulated program can additionally be obfuscated by existing obfuscation methods.

Bertrand et al. [29] presented the need for evaluation of quick and quality of practical obfuscating transformations. They presented first step for comprehensive evaluation suite consisting of a number of de-obfuscating transformations and complexity metrics. These could be readily applied on existing and future transformations in the domain of binary obfuscation. Their framework is based on software complexity metrics which measures four program properties namely code, control flow, data and data flow, which enables the users to quantitatively evaluate the existing obfuscation techniques and existing attacks and to evaluate and compare resulting complexity form obfuscation techniques.

Kovinda et al. [30] proposed an agent based model to ensure the security instead of leaving them entirely on server's side for implementation. The architecture provided a user-centric trust model which helps users to control their sensitive data and it also ensures that the client has fewer burdens at his side. These features clearly assisted in communicating his security related preferences to the service provider. The key feature of the agent is obfuscation, used by users to protect security of data even if there is no cooperation from service provider. The agent automatically obfuscates some or all of the fields in data structures before it is uploaded onto cloud for processing and translated the output from the cloud back into the de-obfuscated form. The obfuscation and data retrieval is done using the key which is chosen by the agent and not revealed to the service provider. This means that the applications in cloud cannot de-obfuscate the data. An attacker who uses the same applications will not be able to retrieve user' data by observing results, when he obfuscates his own data, since his obfuscation key will never be the same with agent's key. This method is more attractive to secure sensitive data since the obfuscation is controlled by the agent.

III. PROPOSED OBFUSCATION TECHNIQUE: ARO_OBFUS CT

The proposed obfuscation technique is used to protect the numerical data in the cloud storage. When the user wants to encrypt the sensitive numerical data by obfuscation, then this proposed technique is suitable and convenient. This technique is a symmetric crypto system. There are two keys used in this proposed algorithm for encryption and decryption. And both the keys are of integer values. With these two keys, the obfuscation of numerical data is possible by the proposed ARO_Obfus CT for protecting the data in public cloud.

The proposed ARO_Obfus Cryptographic Techniques (CT) uses five different mathematical operations such as mul(), pow(), rotate(), mod(), ascii() on numerical data. The two secret keys are generated in cloud side and forwarded to the users. These keys are maintained in the service provider called Key Management as a Service. (KMaaS). The entire work and result is compared with the existing techniques like Base32, Base64 and Hexadecimal Encoding. The size of the given plain text is calculated for obfuscation technique. The plain text is multiplied with the sample value of K_1 and deposited in the array. The square value is calculated for the multiplied value. The sample

generated $_{K2}$ is incremented by one and put into the square values. These values are rotated from left to right for $_{K2}$ times each time. In the next step, the mod value is found out by dividing 256. The ascii character is derived for each mod value. These ASCII values are the equivalent cipher text for the plaint text. The pseudo code for the proposed ARO_Obfus CT is given below.

Pseudocode for ARO_Obfus CT for Numerical Data:

ARO_Obfus(PT)

1. *start*
2. *PT← plaintext*
3. *N←sizeof(PT)*
4. Get a key K_1 from cloud for ARO_Obfus CT

//Multiple the K_1 into PT(i)

5. *MT(i)<-- PT(i)*K_1 *i=0,1,2…<N*

//find square SQ value for MT(i)

6. *SQ(i)← pow(MT(i),2) i=0,1,2…<N*

//Rotate the SQ at K number of times

7. *Get a key K_2*from cloud for ARO_Obfus CT

//Rotate the RTN at K_2 number of times

8. *RTN(i)← rotate(SQ(i),K_2+j) j=1,2…<=N*

//Find the module MOD for RTN by 256

9. *MOD(i)← RTN(i)%256*

//Convert the MOD into ASCII code to produce Ciphertext CT

10. *CT(i)←ascii(MOD(i))*
11. *CT← cipher Text*
12. *End*

IV. Experiments of ARO_Obfus CS with Sample Data

Theexperiment procedure of proposed obfuscation technique is done below with the sample data and sample automatic generated keys.

Step 1: Consider the following plaintext which is the age of employees

*PT<-- **35 56 47 56 51 48***

Step 2: Find the total size of values in the PT and put as N.

N<--6

Step 3: The generated K_1 value is multiplied with the plain text (PT) and put as MT. Here the value of K_1 is 12.

Multiple the K_1 into PT, Sample K_1 = 12.

PT(i)	***MT(i)=PT(i)*K_1***
35	*420*
56	*672*
47	*564*
56	*672*
51	*612*
48	*576*

Step 4: The square value for MT values are calculated: Find the square SQ(i) for MT(i)

MT(i)	***SQ(i)= Pow(MT(i),2)***
420	*176400*
672	*451584*
564	*318096*
672	*451584*
612	*374544*
576	*331776*

Step 5: The key K_2 is generated and here the sample K_2 is 4. The square value is rotated from right to left with number of K_2 times. And K_2 is incremented by one.

Rotate the SQ(i) by K_2 numbers of time from right to left (back to front)

Sample K_2 = 4, k_2 is incremented by 1 for consecutive values in SQ(i),

K_2+i ,i=1,2,3,…N

SQ(i)	***K_2=4***
176400	*K_2=4*
451584	*K_2=5*
318096	*K_2=6*
451584	*K_2=7*
374544	*K_2=8*
331776	*K_2=9*

Step 6 : Rotated RTN(i) is ,

SQ(i)	***RTN(i)***
176400	*640017*
451584	*515844*
318096	*318096*
451584	*445158*
374544	*443745*
331776	*776331*

Step 7: find the Modulus of RTN(i) by 256. The Mod values are calculated by dividing the rotated values by 256. And the ascii character is produced for each mod values. These asci characters are the ciphertext of the original numeric plaintext.

MOD(i) = RTN(i)%256

RTN(i)	***MOD(i)***
640017	*17*
515844	*4*
318096	*144*
445158	*230*
443745	*97*
776331	*139*

Step 8 : Convert MOD(i) into ASCII Code to produce the ciphertext CT

CT =1$1ga,

V. Result and Findings

The proposed obfuscation technique executes properly and produces the ciphertext with the mixture of all types of ASCII character codes. The following findings are drawn from the above results and sample data inputs.

Plaintext to Ciphertext:

The Plain text is : 35 56 47 56 51 48
The CipherText : 1$1ga,

The Findings: The numerical data '56' appears two times in the plain text and the position of these data are 2 and 4. The ciphertext character in the equivalent position of these plaintext is '$g'. It leads conclusion that the same data in the plaintext has different ascii character in the ciphertext.

Ciphertext to Plaint text:

The CipherTextis :1$1ga,
The Plain text is : 36 56 47 56 51 48

The Findings: The ascii character in the plaintext '1' appears two times in the position of 1 and 3. The plaintext equivalent to these positions are 36 and 47. It is derived that the same character in the ciphertext does not have the same data or value in the plaintext. Rather it is different.

The Data size reduced:

The data size for the above same plaintext is 17 bytes. (The plaintext is: *35 56 47 56 51 48*). But the data size of the ciphertext (The Ciphertext is: *1$1ga,*) for same plaintext is 6 bytes. It is decreased by one third (1/3).

From both the findings it is evident that the confidentiality is maintained and hence the security is enhanced.

VI. Conclusion

Data security in cloud storage is of prime importance ever since it started facing challenges and threats. Confidentiality of sensitive data stored in the public cloud has more serious concerns in order to win the confidence of the users. Many traditional cryptographic techniques are on the row for users. The symmetric algorithms are in easy access to the users in order to secure the data of users from the service providers. Symmetric encryption algorithms are very much handy since these algorithms have got speed and computational efficiency.

A new obfuscation technique, ARO_Obfus CT, is proposed and implemented in this paper to secure data confidentiality in public cloud storage. This proposed technique has produced minimum data size while storing the obfuscated data in the provider. This obfuscation technique also produced high percentage in security level and has taken minimum time for obfuscation and de-obfuscation process when compared with the existing techniques while encrypting and uploading data into public cloud storage. In this way the data confidentiality is protected in cloud storage. Thus the security is enhanced through this proposed obfuscation method.

References

1. Wu, J., Shen, Q., Zhang, J., Shen Z. and Ping, L. (2011) Cloud Computing: Cloud Security to Trusted Cloud. PhD thesis. Hangzhou Normal University and Zhejiang University.
2. Dr. L. Arockiam, S. Monikandan," Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Volume 2, Issue 8,ISSN : 2278-1021, August 2013, pp. 3064-3070.
3. Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii International Conference on System Sciences, pp.1-7, 2011.
4. A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, "Handbook of Applied Cryptography", Boca Raton, FL, USA:CRC Press, Inc., 1996.
5. NarenderTyagi, Anita Ganpati "Comparative Analysis of Symmetric Key Encryption Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 8, August 2014 ISSN: 2277 128X.
6. J. Mohammad, K. Omer, S. Abbas, E. S. M. El-Horbaty, and A. B. M Salem, "A comparative study between modern encryption algorithms based on cloud computing environment". 8th International Conference for Internet Technology and Secured Transactions (ICITST'13), IEEE, 2013, pp. 531-535.
7. C. Colberg and C. Thomborson, Watermarking, TamperProofing, and Obfuscation – Tools for Software Protection, IEEE Transactions on Software Engineering, vol. 28, No. 8, 2002, pp.737.
8. G. Wroblewski, "General Method of Program Code Obfuscation", PhD thesis, Wroclaw University of Technology, Institute of Engineering Cybernetics, 2002.
9. C. Collberg, C. Thomborson and D. Low, "A Taxonomy of Obfuscating Transformations," Technical Report 148, Dept. of Computer Science, Univ. of Auckland, July 1997.
10. Balakarishnan.S, Saranya.G, Shobana.S, Karthikeyan.S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", IJCST, Vol. 2, Issue 2, June 2011.
11. Joshi Ashay Mukundrao, Galande Prakash Vikram, "Enhancing Security in Cloud Computing", ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol. 1, 2011.
12. Dai Yuefa, Wu Bo, GuYaqiang, Zhang Quan, Tang Chaojing, "Data Security Model for Cloud Computing", ISBN 978-9525726-06-0, Qingdao, China, November 2009.
13. Sheryl Duggins, Frank Tsui, Orlando Karam, and Zoltan Kubanyi, "Semantic Obfuscation and Software Intention", International Conf. Sotware Eng. Research and Practice, September, 2013.
14. C. Colberg and C. Thomborson, Watermarking, TamperProofing, and Obfuscation – Tools for Software Protection, IEEE Transactions on Software Engineering, vol. 28, No. 8, 2002, pp.737.
15. Varun Maheshwari, Nourian, A., Maheswaran, M, "Character-based Search with Data Confidentiality in the Clouds", IEEE 4th International Conference on Cloud Computing Technology and Science, 2012.
16. Cong Wang, Qian Wang, Kui Ren and Wenjing Lou, "Ensuring Data Storage Security in the Cloud Computing", Department of ECE Illinois Institute of Technology, IEEE, Chicago 2009.
17. AtiqurRehman, and M. Hussain, "Efficient cloud data confidentiality for DaaS", International Journal of Advanced Science and Technology, Vol. 35, 2011, pp. 1-10.

18. Yau SS, An HG, "Confidentiality protection in cloud computing systems", International Journal Software Informatics, Vol. 4, Issue 4, 2010, pp. 351-365.
19. ManpreetKaur and Rajbir Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications, Vol. 70, Issue 18, 2013, pp. 16-21.
20. Dr. L. Arockiam, and S. Monikandan, "Arocrypt, "A Confidentiality Technique for Securing Enterprise's Data in Cloud", International Journal of Engineering and Technology (IJET) Vol.7 No. 1. 2015, Feb-Mar pp. 245-253.
21. Dr. L. Arockiam, S. Monikandan, "AROMO Security Framework to Enhance Security of Data in Public Cloud", International Journal of Applied Engineering Research ISSN 0973-4562 Vol. 10, Number 9, Research India Publications. 2015, pp. 6740-6746.
22. RohitBhadauria, SugataSanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques", School of Electronics and Communications Engineering, Vellore Institute of Technology, Vellore, India, 2012.
23. R. Anitha, P. Pradeepan, P. Yogesh, and Saswati Mukherjee, "Data Storage Security in Cloud using Metadata", 2nd International Conference on Machine Learning and Computer Science (IMLCS'2013), Kuala Lumpur (Malaysia), August 2013, pp.26-30.
24. Siani Pearson, Yun Shen and Miranda Mowbray, "A Privacy Manager for Cloud Computing", CloudCom '09 Proceedings of the 1st International Conference on Cloud Computing, Springer-Verlag Berlin, Heidelberg, 2009, pp.90 – 106.
25. Miranda Mowbray, Siani Pearson, Yun Shen, "Enhancing privacy in cloud computing via policy-based obfuscation", J Supercomput (2012) 61:267–291, DOI 10.1007/s11227-010-0425-z, Published online: 31 March 2010, © Springer Science+Business Media, LLC 2010.
26. Prasadreddy P.V. G.D., T. Srinivasa Rao, S. PhaniVenkat, "A Threat Free Architecture for Privacy Assurance in Cloud Computing", IEEE World Congress on Services, 2011.
27. Muhammad Hataba, Ahmed El-Mahdy, Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, "Cloud Protection by Obfuscation: Techniques and Metrics", IEEE, The Computer Society, 2012.
28. Zeljko Vrba, Pal Halvorsen, Carsten Griwodz, "Program obfuscation by strong cryptography", Simula Research Laboratory, Oslo, Norway Department of Informatics, University of Oslo, Norway.
29. Bertrand Anckaert, Matias Madou,Bjorn De Sutter, Bruno De Bus, Koen De Bosschere, Bart Preneel, "Program Obfuscation: A Quantitative Approach", Ghent University. QoP'07, Alexandria, Virginia, USA. Copyright 2007 ACM 978-1-59593-885-5/07/0010, 29 October 2007.
30. K. Govinda, E. Sathiyamoorthy, "Agent Based Security for Cloud Computing using Obfuscation", Elsevier, Procedia Engineering 38, ICMOC, 2012, pp.125-129.

AUTHORS' BIOGRAPHY

S. Arul Oli received his Master's in Computer Science from Bharathidasasn University, Tiruchirappalli, India. Currently, he is a Ph.D. research scholar in the Department of Computer Science at St. Joseph's College (Autonomous), Tiruchirappalli affiliated to Bharathidasan University, India. He has published Research Papers in International Journals with Impact Factor. His main area of research is Cloud Computing. He has attended several National and International Conferences and workshops.

Dr. L. Arockiam is working as Associate Professor in the Department of Computer Science, St. Joseph's College, Tiruchirappalli, Tamil Nadu, India. He has 26 years of experience in teaching and 18 years of experience in research. He has published more than 235 research articles in the International & National Conferences and Journals. He has also presented 3 research articles in the Software Measurement European Forum in Rome, Bali and Malaysia. He is also the Member of IEEE, Madras Section. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has Co-authored 5 books. His research interests are: Cloud Computing, Big Data, Cognitive Aspects in Programming, Data Mining and Mobile Networks. He has been awarded "Best Research Publications in Science" for 2009, 2010, 2011 & 2015 and ASDF Global "Best Academic Researcher" Award from ASDF, Pondicherry for the academic year 2012-13 and also the "Best Teacher in College" award for the year 2013 & 2014.