IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 3, March 2016

ARARO Framework for Confidentiality Techniques to Enhance Security of Numerical and Non-Numerical 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]

Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, India [2]

Abstract: Cloud computing is a new venture that offers tremendous advantages in Information Technology. Data may be transferred, processed & stored in the cloud storage provided by service providers in order to leverage the full use of its capacity. However, data users are very sceptical to store their data in cloud storage. The data in cloud storage are out of direct control from their own users. The data stored in private cloud are secured to some extent whereas security of data stored in public cloud are not guaranteed. There are many techniques to protect the confidentiality of data before stored into cloud storage. This paper proposes a novel framework to protect data confidentiality of numeric and non-numeric and to enhance the security of data using cryptographic techniques in public cloud storage before being uploaded into cloud storage.

Keywords: Cloud Storage, Confidentiality, Encryption, Obfuscation, Framework, Security.

I. INTRODUCTION

Cloud computing (CC) is a great and powerful invention in Information Technology (IT). The cloud computing resources are provided as 'everything as a service'. The rapid deployment in cloud gives tremendous advantages to cloud users. CC is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or serviceprovider interaction" [1]. In a nutshell, CC could be termed as '3 4 5', for simple understanding: The Three basic service models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The Four deployment models are Private, Public, Community and Hybrid clouds. The Five essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

The essential characteristics promote a lot of benefits in cloud computing environment. To add flavour to these characteristics, Gartner defines cloud computing as "a style of computing where scalable and elastic IT-related capabilities are provided as a service to external customers using internet technologies" [2]. Every day, the data are growing at a rapid rate in enterprises. One of the most profitable, essential services provided by cloud computing is cloud storage. While discussing the benefits of cloud storage, Toby Velte et al [3] define as follows: "cloud storage has become a boon to Information Technologies (IT), to have an infinite space for their data storage". To store data, a large number of processing units, hard drives, network infrastructure and other resources are required. Clusters and grids distributed systems are used to store huge amount of data by enterprises. The enterprises at times develop a tendency to tamper the data without the authorisation of users [4].

Data storage in cloud computing faces various security issues [5] such as malicious data access, imperfect data segregation, unauthorized authentication and authorization, false identity management, wrong policy integration, proxy recovery, fake accountability, malicious insiders, unprotected management console security and unauthorised account control [6]. Considering the importance of data security in cloud storage, it is essential to identify and analyse the countermeasures against threats and vulnerabilities [7] [8].

Security is one of the most important aspects in cloud computing storage. Once data are stored on cloud, data owners are disconnected from their data and it is the most alarming factor for the users [9]. Moreover the cloud data can be tampered by inside attackers and outside attackers [10]. Malicious cloud administrators are the inside attackers in cloud service providers (CSPs). The security parameters are authentication, authorization, confidentiality, integrity, availability etc. Confidentiality is one of the important parameters in the security to protect data from malicious attackers.

To ensure data confidentiality, data owners must make certain the security to their data before storing into the cloud. Hence, a technique has to be incorporated for data security in cloud storage. The technique used for maintaining data confidentiality is called cryptography [11]. The two forms of cryptosystems are symmetric and asymmetric, in which the symmetric cryptosystems involve the use of a single key known as the secret key to encrypt and decrypt data or messages. The asymmetric cryptosystems use one key (the public key) to encrypt messages or data, and a second key (the secret key) to decipher or decrypt those messages or data respectively.

The organisation of the paper is as follows: section II gives the related works. Section III explains the

motivation. Section IV explain the problem definition. Section V details the Objectives. Section VI explains the Scope and methodology. Section VII gives the proposed framework. Section VIII concludes the paper.

II. RELATEDWORKS

There are number of researches going on to address the security hurdles in cloud environment. Rashmi et al. [12] did a survey on different security issuesand different cryptographic algorithms that exist in the cloud. They also defined some privacy and security-related issues that are believed to have long-term significance for cloud storage. Hashizume et al. [13] presented a classification of security issues in different service models (SaaS, PaaS and IaaS). They also performed the identification of the main vulnerabilities in cloud computing while presenting the common threats and its relations to cloud layers. A confidentiality technique (CT) is further proposed in a framework by AtiqU.RRehman et al [14]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. The obfuscation technique for security was again elaborately discussed by Yau SS et al [15] through approaches of separating software and infrastructure service providers, hiding data owners' information in cloud and, data obfuscation technique.

The proposed AROcrypt cryptographic algorithm [16] was to ensure the security of data stored in cloud storage. The algorithm was based on a symmetric encryption provided through 'security as a service' model to keep the keys with users for encryption and decryption. The authors [17] evaluated and found out the varied performance of two encryption algorithms of AES and DES in terms of processing time, CPU usage and encryption throughput on Windows and Mac platform for a different text size. Encryption time is calculated with throughput of an encryption scheme.

The CT [18] introduced the process to convert the plain text into cipher text using ASCII code. The process provided better performance and maximum security protection when compared with existing CTs such as DES, 3DES and Blowfish. A modern symmetric encryption algorithm called QAES, was proposed by Jasim et al. [19] integrating Quantum Key Distribution (QKD) and an enhanced AES. The output of such integration becomes feasible and is discussed as AES block cipher symmetric algorithm. Later, a new lightweight encryption algorithm was introduced [20] to compare the symmetric and asymmetric algorithms. The algorithms encrypted various input data files for the distributed keys and concluded that the symmetric algorithms are more efficient and effective in cloud environment.

AROMO framework [21] was proposed with three security algorithms to enhance the security of data in cloud storage to protect data from different threats. The performance results of data confidentiality through scalable approach [22] reveal that the overhead for data obfuscation and de-obfuscation appear to increase linear with the size of input data. The term obfuscation means attempting "to transform a program into an equivalent one that is harder to reverse engineer" [23]. Hence, the data obfuscation technique was to confuse hackers while trying to tamper the sensitive data without authorization. Many studies proved that obfuscation of data made the intruders harder to understand and even made impossible in some cases. The approach of obfuscation for security was further proposed [24] for protection by increase of complexity to withstand malicious attacks. The architecture [25] provided a user-centric trust model to ensure and to control the security of users' sensitive data instead of leaving them entirely on server-centric for implementation. The key is not revealed to the CSP in this obfuscation method for protecting security of data.

III. MOTIVATION

Data Security has become an important factor in cloud computing. The private and public clouds are the broader categorization in cloud infrastructures. The infrastructure is owned and managed by the user in private cloud. It is located on-premise where data access is under the control of trusted parties. Whereas it is off-premise in public cloud and the infrastructure is owned and managed by service provider. So, In order to protect data stored in public cloud, the user is pushed to a situation where he needs to find a different method to protect sensitive data.

The data encryption is a basic measure to ensure data security. But the threat elements in cloud demand the process for data encryption before transmitting it. The storage services based on public cloud provides users with dynamic storage. The biggest hurdle to the adoption of cloud storage is the concern over data confidentiality. Unless the issues of confidentiality are addressed, many potential users will be reluctant to make use of the service provider in-spite of enormous positive elements that the cloud storage possesses.

The paper is proposed to improve data confidentiality stored in cloud storage. It is proposed to identify, encrypt and store all sensitive data without the knowledge of the provider. These sensitive data are stored in cloud in an encrypted form, to be accessed only by users, thus protecting its confidentiality from unauthorised users.

IV. PROBLEM DEFINITION

Cloud storage is available at a fairly lower price. Cloud storage is the main attraction in migrating into cloud as it revolutionizes the IT market through online services 24x7. Despite the enormous growth in cloud storage, it lacks security measures in data availability, data confidentiality, data integrity and many other aspects. When data are stored in cloud, the owners lose their control over the data. The existing traditional cryptographic techniques also do not fully convince the users in protecting their data in cloud storage. The encryption process takes more time and consumes more data. The inadequate security leads into threats of losing data confidentiality.

Data security becomes more critical as multiple copies of data are available in modern days. The users are forced to use the same interfaces provided by CSPs and these CSPs use fixed format for data to be controlled and monitored in specific locations. At the same time the CSPs have the privilege to access and to collect the users' confidential

data. The cloud storage problems are summarized as follows:

- ❖ Data owners have no control over their data in cloud storage.
- ❖ Data stored may be exposed to security vulnerabilities.
- ❖ Difficulties in maintainingkeysfordifferentusers' data.
- ❖ Unauthorized access from the cloud storage.

Maintaining data confidentiality is one of the primary issues in cloud computing. Hence, proper, apt and suitable techniques must be derived to maintain the data confidentiality to enhance security.

V. THE OBJECTIVE

The objective of this paper is to propose a method where sensitive data are protected from the unauthorised users. The primary aim of the proposed research work is to enhance security of stored data from the unauthorised users in public cloud storage through CTs. The following objectives are derived to achieve the primary aim.

- To propose an **AO_Enc Confidentiality Technique (AOECT)** to enhance security of non-numerical data and to minimize time.
- To propose an **ARO_Obfus Confidentiality Technique (AROOCT)** to enhance security of numerical data and to minimize data size and time.
- To propose an **AO_AROEncObfus Confidentiality Technique (AOAROEOCT)** to enhance security of non-numerical and numerical data and to minimize time, data size and to economize service cost.

To design an **ARARO Security Framework (ARAROSF)** to enhance security by incorporating the above proposals. Confidentiality is maintained by protecting the data and thus security is enhanced.

VI. SCOPE AND METHODOLOGY

a. The Scope

The highest block or impediment of cloud storage is lack of trust as the data are stored in one or more remote servers and the data owners are distanced from their data. This hurdle stops the cloud users in adopting cloud storage. Hence, there is a necessity to find out suitable methods to mitigate data security threats and attacks. The proposed research work aims at providing CTs to enhance the security of users' data stored in public cloud storage.

Out of four deployment models in cloud environment, public cloud faces maximum threats in cloud storage. This research work implements Security Algorithms (SAs) as Confidentiality as a Service (CFaaS), using one of the computing models of SaaS. The data in cloud face threats in two different levels, such as data-at-rest and data-in-transit. The threats are either from inside attackers or outside attackers. The scope of the research work is to protect data-at-rest from inside attackers, who try to tamper or hack the data in the cloud.

The data security problems can be solved by cryptographic techniques through which data are converted into unreadable format to avoid hacking from the unauthorized users. Due to time consumption in asymmetric cryptosystem in cloud, this research work is done by utilizing the symmetric cryptosystems to maintain confidentiality. The proposed cryptosystem is measured by security level, time, data size and service cost while compared with the existing confidentiality techniques. The proposed scope of the research work meets all characteristics of cloud computing.

b. Methodology

The overall objective of this research work is to propose three SAs as CFaaS to enhance security through confidentiality measures.

The first SA is AO_Enc CT (AOECT) which provides the technique for encryption of non-numerical data by symmetric cryptosystem. The technique encrypts only the non-numerical data. This technique takes minimum time for encryption and decryption. The implementation results are compared with the existing encryption techniques such as DES, 3DES and Blowfish.

The second SA is ARO_Obfus CT (AROOCT) which provides the technique for obfuscation of only numerical data. The technique uses different mathematical methods and programming logic to obfuscate the plain text into cipher text. This technique reduces the size of data uploaded into cloud storage. The implementation results are compared with the existing obfuscation techniques like Hexadecimal Encoding, Base32 and Base64.

The third SA is AO_AROEncObfus CT (AOAROEOCT) which provides the technique for encryption and obfuscation of respective non-numerical and numerical data simultaneously. By using this technique the users reduce the service cost instead of using AO_Enc and ARO_Obfus CT one by one for hiding all the data in non-numerical and numerical format. The results are compared with the proposed first two CTs.

The proposed techniques of encryption and obfuscation are utilised to encrypt and obfuscate the data before uploading into the cloud storage. The keys for the proposed techniques are generated and sent to the users directly from the cloud service called KMaaS (Key Management as a Service).

VII. ARARO- THE PROPOSED FRAMEWORK

The proposed ARARO Security Framework (ARAROSF) (ARARO is named after the research scholar, S. **AR**ul Oli and research supervisor, L. **ARO**ckiam) depicted in Fig. 1 consists of three cloud services namely CFaaS, KMaaS and STaaS (STorage as s Service). These three services are provided by three different independent CSPs. This research work mainly concentrates on CFaaS. The CFaaS consists of three SAs, such as AO_Enc CT, ARO_Obfus CT, and AO_AROEncObfus CT (These algorithms are named after the research scholar, S. **A**rul **O**li and research supervisor, L. **ARO**ckiam, and **Enc**ryption, **Obfus**cation) for encryption of non-numerical data, obfuscation of numerical data and both encryption & obfuscation of non-numerical and numerical data respectively. The KMaaS consists of six components and the necessary components are key generation and key storage. The STaaS (STorage as a Service) functions to store the data in cloud storage.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 3, March 2016

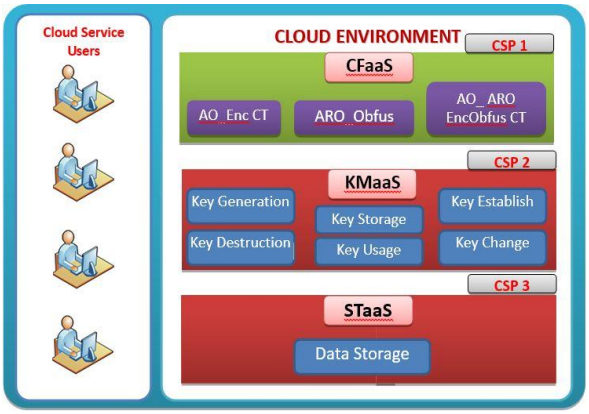

Fig.1. ARARO Security Framework

A. Confidentiality as a Service (CFaaS)
The CFaaS provides three SAs for confidentiality of data and to enhance security in cloud storage. The proposed CTs are namely AO_Enc CT, ARO_Obfus CT and AO_AROEncObfus CT.

i) AO_Enc CT

AO_Enc CT is a SA to enhance the confidentiality of non-numerical data stored in cloud storage. It is based on symmetric encryption algorithm. Three keys are received from the cloud. Out of these three keys, two keys are of numeric and one is string type. The encryption is done with the data and keys in users' side before sent to the cloud. Simulation is conducted for the proposed technique to measure the security level and the time taken for encryption and decryption. The security level is calculated using universal Hackman tool and is compared with the existing techniques such as DES, 3DES and Blowfish. From the simulation results, it is evident that the proposed technique takes minimum time and produces maximus security.

ii) ARO_Obfus CT

ARO_Obfus CT is an obfuscation technique for numerical data to enhance security in cloud storage. Two keys are generated from the cloud. With the use of data and the keys, the obfuscation is done in users' side before sent to the cloud. Obfuscation is a process of converting the readable data into unintelligible data using mathematical functions and programming logic. The proposed technique uses different mathematical methods like mul(), pow(), rotate(), mod(), ascii() for obfuscation. The main advantage of this technique is to reduce the size of the data. Simulation is conducted for the proposed technique as similar to the AO_Enc CT to measure the security level and time taken for obfuscation and de-obfuscation and it is compared with the existing obfuscation techniques like Hexadecimal Encoding, Base32 and Base64. From the simulation results, it is shown that the obfuscation technique takes minimum time and size and produces maximum security.

iii) AO_AROEncObfus CT

AO_AROEncObfus CT is a symmetric cryptosystem with the combination of encryption and obfuscation procedure. This technique is used to encrypt and obfuscate the non-numerical and numerical data respectively. Encryption and obfuscation are done in simultaneous process. If the users wish to hide entire data (non-numeric and numeric), then this SA is suitable choice with respect to low service cost. Simulation is conducted as similar to the previous two techniques to measure the security level and time. This technique is compared with the first two proposals and produces maximum security.

B. Key Management as a Service (KMaaS)
KMaaS is a cloud service provided by an independent CSP. The KMaaS comprises the following six components as in Fig. 2. KMaaS is instructed by CFaaS for key generation. CFaaS sends the details of algorithm and users. KMaaS generates the keys applicable to the selected algorithm and forwards to the users directly based on the users' detail received from CFaaS. KMaaS maintains different log tables for key management.

- While encryption is foundational to cloud security, the management of encrypted keys is one of the most difficult challenges in cloud computing. Failure to adequately manage encryption of keys can lead to a range of administrative and security problems. In the proposed techniques, the keys are maintained by the users.
- KMaaS includes all devices or sub-systems that can access an unencrypted key or its metadata. Encrypted keys and their cryptographically protected metadata can be handled by computers and transmitted through communications systems. It consists of policies, procedures, components and devices that are used to protect, manage, and distribute cryptographic keys and certain specific information in metadata. KMaaS maintains metadata table, with structure and its log table, to protect the confidentiality of data.

Once a key is generated, the generated key and its details are forwarded to KMaaS. KMaaS stores the key with relevant information in metadata.

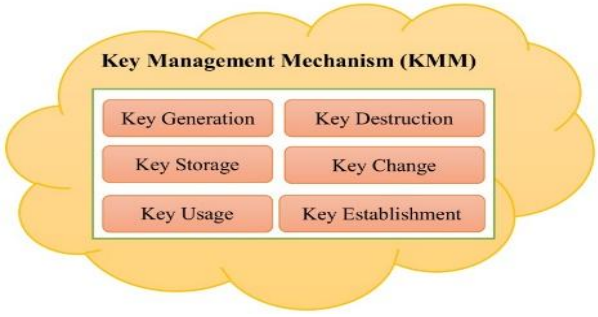

Fig.2. Key Management as a Service (KMaaS)

KMaaS is more important to keep data more confident and secure. There are few components in KMaaS that are considered very necessary. Secure key management is the management of keys in a cryptosystem. Secure key management deals with the components. Secure key management includes cryptographic protocol design, user procedures, key servers, and other relevant protocols. Secure key management is concerned with keys at the cloud user level, either between cloud users or systems [26].The components are depicted in Fig. 2.

Key Generation
The cryptographic systems in modern IT include symmetrickey algorithms (DES and AES) and publickey algorithms (RSA). The user encrypts the data with the symmetric cryptosystem. The simplest method to read encrypted data is a brute force attack, which means attempting every time, up to the maximum length of the key. Therefore, it is important to use sufficiently longer key length since longer keys take longer time to attack, resulting brute force attack almost impractical.

Key Destructions
The key destruction is the deletion of the keys from the table. Keys, when no longer needed, must be destroyed in a secured manner. And also when the keys are once used for the encryption, it must not be used by another user. Keys when not used within the stipulated time then it makes no relevance and so the key must be removed from the table.

Key Establishment
The key establishment is done in three ways namely, key pre-distribution, key distribution, and key agreement. At this stage, the pre-distribution is the concept of distributing keys by the user. Key agreement is on the basis of cost factor between the user and the provider.

Key Storage
The keys must be stored securely to maintain the confidentiality of data. There are various techniques available for this purpose. The most common technique is an encryption application which stores the generated keys for the user.

Key Change
The facility to change keys in all cryptographic systems is a must. For an example, the regular updatesare done periodically. The key compromise, which is the unplanned one, will cause loss of data. Many systems are designed in such a way that it is extremely difficult and expensive to change certain keys.

Key Usage
The length of the key use is the major issue. The keys must be frequently changed as the required efforts of the attackers are on the increase. The frequent change also limits the loss of information. The frequency of usage decreases as the frequency of key change increases. This happens especially when the attacker tries to trace the keys. The symmetric keys must change with every data, so that only the intended data will become accessible even if the keys are stolen, crypt analyzed, or socially engineered.

C. Storage as a Service (STaaS)
STaaS is a cloud service provided by separate and independent CSP. The STaaS stores encrypted or obfuscated data. Once data are encrypted or obfuscated or done both, then the data are forwarded to the STaaS.

VIII. CONCLUSION

The greatest challenge in the cloud storage is unauthorized access of data by malicious attackers in the cloud environment, which compromises the data confidentiality. The proposed ARAROSF is designed to address the threats and attacks on data in cloud storage in order to enhance the security. ARAROSFcomprises three different services namely CFaaS, KMaaS, STaaS. These three services are provided by three different independent CSPs. This research work mainly concentrates on CFaaS. The CFaaS provides three SAs such as AOECT, AROOCT and AOAROEOCT to enhance security in cloud storage. Simulation for ARAROSFis conducted in the cloud environment. From the simulation results, it is evident that SAs in CFaaS provide minimum time, less data size, lower service cost and maximum security. In conclusion, the CTs in ARAROSF enhance security of data stored in public cloud storage.

REFERENCES

[1] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", Recommendations of the National Institute of Standards and Technology, 2011.
[2] David W. Cearley, "Gartner Cloud Computing", Cloud Computing Key Initiative Overview, http://www.gartner.com/it/initiatives/pdf/KeyInitiativeOverview_CloudComputing.pdf, 2010.
[3] Toby Velte, Anthony Velte and Robert Elsenpeter, "Cloud Storage in Cloud Computing: A Practical Approach", McGraw-Hill Education. New York. 2009, pp. 135- 149.
[4] Diogo A. B. Fernandes, Liliana F. B. Soares, Joao V. Gomes, Mario M. Freire and Pedro R. M. Inacia, "Security Issues in Cloud Environments: A Survey", International Journal of Information Security (IJIS), Springer, 2013, pp. 113 - 170.
[5] Won Kim, Soo Dong Kim and Eunseok Lee, "Adoption Issues for Cloud Computing", In Proceeding of the 7th International Conference on Advances in Mobile Computing Multimedia. ACM, New York, 2009, pp. 2-5.
[6] EveraldoAguiar, Yihua Zhang and Marina Blanton, "An Overview of Issues and Recent Developments in Cloud Computing and Storage Security In: High Performance Cloud Auditing and Applications", Springer, New York, Berlin, 2013, pp. 3-33.
[7] Pearce, M., S. Zeadally, and R. Hunt, "Virtualization: Issues, Security, Threats, and Solutions", ACM Computing Surveys, New York, 2013, pp. 1:71–1:739.
[8] Perez-Botero, D., J. Szefer, and R. B. Lee, "Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers", In Proceedings of the 2013 International Workshop on Security in Cloud Computing (SCC), ACM, New York, NY, USA, pp. 3-10.
[9] Townsend, M, "Managing a Security Program in a Cloud Computing Environment", In Information Security Curriculum Development Conference, ACM, New York, NY, USA, 2009, pp. 128-133.
[10] Sandeep K. Sood, "A Combined Approach to Ensure Data Security in Cloud Computing", Journal of Network and Computer Applications, Elsevier. 2012, pp. 1831–1838.
[11] Seny Kamara and Kristin Lauter, "Cryptographic Cloud Storage", In Financial Cryptography and Data Security, Springer Berlin Heidelberg. 2010, 6054: pp. 136-149.
[12] Rashmi Nigoti, ManojJhuria, Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), ISSN (Print): 2279-0047, ISSN (Online): 2279-0055, Vol 4. 2013, pp. 141-146.
[13] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An Analysis of Security Issues for Cloud Computing". Journal of Internet Services and Applications, Vol. 4, 2013, pp. 1-13.
[14] AtiqU.R. Rehman, and M. Hussain, "Efficient Cloud Data Confidentiality for DaaS", International Journal of Advanced Science and Technology, Vol. 35, 2011, pp. 1-10.
[15] Yau SS, An HG, "Confidentiality Protection in Cloud Computing Systems", International Journal Software Informatics, Vol. 4, Issue 4, 2010, pp. 351-365.
[16] 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, pp. 245-253.

[17] Shaza D. Rihan, Ahmed Khalid, SaifeEldin F. Osman, "A Performance Comparison of Encryption Algorithms AES and DES", International Journal of Engineering Research & Technology (IJERT), ISSN: 22780181, Vol. 4 Issue 12, 2015, pp. 151-154.

[18] Dr. L. Arockiam, S. Monikandan, "A Security Service Algorithm to Ensure the Confidentiality of Data in Cloud Storage", International Journal of Engineering Research & Technology (IJERT), ISSN: 22780181, Vol. 3 Issue 12, 2014, pp. 1053-1058.

[19] Omer K. Jasim, Safia Abbas, El-Sayed M. Horbaty, "Evolution of an Emerging Symmetric Quantum Cryptographic Algorithm", Journal of Information Security, 2015, Vol. 6, pp. 82-92.

[20] Sana Belguith, AbderrazakJemai, RabahAttia, "Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm", The Eleventh International Conference on Autonomic and Autonomous Systems, ISBN: 978-1-61208-405-3, 2015, pp. 98-103.

[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] Muhammad Hataba, Ahmed El-Mahdy, "Cloud Protection by Obfuscation: Techniques and Metrics", Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, IEEE Computer Society, 2012.

[23] C. Colberg and C. Thomborson, "Watermarking, Tamper Proofing, and Obfuscation – Tools for Software Protection", IEEE Transactions on Software Engineering, vol. 28, No. 8, 2002, pp.737.

[24] Sheryl Duggins, Frank Tsui, Orlando Karam, and Zoltan Kubanyi, "Semantic Obfuscation and Software Intention", Intl. Conf. Software Engg. Research and Practice, 2013.

[25] K. Govinda, E. Sathiyamoorthy, "Agent Based Security for Cloud Computing using Obfuscation", Elsevier, Procedia Engineering, ICMOC, 2012, pp. 125-129.

[26] S. Arul Oli and L. Arockiam, "A Framework for Key Management for Data Confidentiality in Cloud Environment", In Proceedings of International Conference on Computer Communication and Informatics (ICCCI 2015), IEEE Xplore, January 2015, pp. 167-170.

BIOGRAPHIES

S. Arul Oli received his Master's degree 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 ten Research Papers in International Journals with Impact Factor. His main area of research is Cloud Computing Security. 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.

DOI 10.17148/IJIREEICE.2016.4310