Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

Confidentiality Technique for Data Stored in Public Cloud Storage

S. Arul Oli
Research Scholar in Computer Science
St. Joseph's College (Autonomous)
Tiruchirappalli, Tamilnadu, India

Dr. L. Arockiam
Associate Professor in Computer Science
St. Joseph's College (Autonomous)
Tiruchirappalli, Tamilnadu, India

***Abstract*—With the advancement of science and technology internet related communicative techniques have taken prominent roles in everyday activities. However threat of hackers and malicious groups have grown along with these advancements. It is the role of the security mechanisms to protect the sensitive data from passive and active attacks. There are different kinds of encryption algorithms to make sure that the data sent through internet is secure from any sort of attacks. Several cryptographic algorithms have been developed for encryption with each one having some advantages and disadvantages. This paper proposes an encryption technique namely AO_Enc CT to hide the non-numeric data from the unauthorized users. The sample data are implemented in the proposed technique and the results are derived to prove that the proposed technique is higher security in protecting the data of the user.**

Keywords—Cloud Storage; Symmetric Encryption; Cryptography; Confidentiality;

I. INTRODUCTION

Cloud computing is the delivery of computing services in multitude over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Online file storage, social networking sites, webmail, and online business applications are few examples of cloud services [1]. The cloud computing is an easy access to information and computer resources from anywhere with the network connection. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications [2].

Cloud computing could be defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [3]. Because of these benefits each and every organizations are moving their data to the cloud. So the need automatically arises to protect that data against unauthorized access, modification or denial of services etc. Securing the cloud means to secure the storage in the cloud providers.

Cloud data security plays a pivotal role with the issues and vulnerabilities of cloud computing for guaranteeing safer computing environment. The goals of data Security include three points namely Availability, Confidentiality, and Integrity. Confidentiality of data in Cloud is accomplished by cryptography [4]. Cryptography, in modern days is considered as the combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

Data cryptography mainly the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed as Encryption. The main aim of cryptography is to protect and secure data from unauthorized invaders. The reverse process of getting back the original data from encrypted data is decryption, which restores the original data. In order to encrypt data at cloud storage, both symmetric and asymmetric-key algorithms could be used. In recent times, cloud storage contains huge amount of databases and for such a huge quantity of databases asymmetric-key algorithm is slower in performance when compared to symmetric-key algorithms [5].

Symmetric-key algorithms are divided into two types: Block cipher and Stream cipher. In block cipher input is taken as a block of plaintext of fixed size depending on the type of symmetric encryption algorithm. The key of fixed size is applied on to block of plain text and then the output block of the same size as the block of plaintext is obtained. In Case of stream cipher one bit at a time is encrypted. Some popular Symmetric-key algorithms used in cloud computing includes: Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES). Here the symmetric method is used to actualize our purpose of encrypting the data before it is uploaded into the cloud [6].

II. RELATED WORKS

The authors [7] identified fived concerns of cloud computing namely Confidentiality, Integrity, Availability, Accountability, and privacy. They thoroughly reviewed the threats to each of the concerns as well as defence strategies. Oza et al [8] carried out a survey on a number of users to determine the user's experience of Cloud computing and found that the main issue of all users was trust and how to choose between different Cloud Service Providers. This was highlighted in [9] as it stated, "although researchers have identified numerous security threats to the Cloud, malicious insiders still represent a significant concern".

Dimitrios et al. was the first to propose the use of cryptography to secure cloud architecture [10]. Ever since, many authors proposed to use cryptographic algorithms in the cloud storage [11] [12]. But, these solutions remain

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

incomplete because they do not specify which algorithm is recommended to encrypt data and how to distribute cryptographic keys while maintaining adequacy with cloud characteristics. Rashmi et al. [13] did their survey for different security issues to cloud and different cryptographic algorithms adoptable to better security for 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. [14] presented a classification of security issues in different service models (SaaS, PaaS and IaaS). This paper presents an identification of the main vulnerabilities in cloud computing while presenting the common threats and its relations to cloud layers. Though countermeasures are available in this paper, the study does not provide technical implementation of these solutions.

Rahmani et al. [11] proposed Encryption as a Service (EaaS) as a solution for cryptography in cloud computing based on XaaS concept. This solution presents a response to prevent the security risks of cloud provider's encryption and the inefficiency of client-side encryption. However, there is not a comparative study of cryptographic algorithms which can be integrated in this solution. The most important type of the encryption is the symmetric key encryption. Symmetric-key algorithms are those algorithms which use the same key for both encryption and decryption. Hence the key is kept secret. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption [15].

While cost and easy access are two great benefits of cloud computing [16] there are significant security concerns that need to be addressed while moving critical applications and sensitive data to public cloud storage. They proposed two ways of attacks in cloud. One is outsider attack and the other is insider attack. Insider as an administrator can have the possibility to hack the user's data and it is very difficult to be identified. So the users should be very careful while storing their data in cloud storage. Even though the data is accessed by the third party, they should not get the actual data. So, all the data must be encrypted before it is transmitted to the cloud storage.

The authors [17] proposed new encryption technique called PSR, which includes Position, Substitution and Random encryption. It was compared with RSA Algorithm which are used in the encryption of plaintext into cipher text that are generally used in cryptography. The algorithm generates only single key and takes a key level from the users which is used in Substitution and Position method. The generated key is based on length of text as well as a private key is generated which must be kept secret. So it provided double secrete level protection. Since it undergoes three phases the overall complexity increases. The algorithm is faster, better immune to attacks, more complex, easy to encrypt with advanced security features. The time taken for encryption is less and the procedure to encrypt the text is simple. This algorithm has multipurpose for usability but the complexity is very high.

The authors [18] stressed that the encryption algorithms play a main role for security of the data and the algorithms are varied in their performance. They evaluated the performance of two 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. Experimental results are given to demonstrate the performance of each algorithm. Encryption time is used to calculate the throughput of an encryption scheme which indicates the speed of encryption.

Zhao et al. [19] suggested a progressive elliptic curve encryption scheme (PECE) where a data is encrypted a number of times using multiple keys and later decrypted using same keys. Even while sharing of data a credential is necessary for a storage provider for encryption and decryption of data. The proposed technique is an effective one so as to keep data confidential as data is encrypted through the entire stages thus never allowing a malicious user to view the plaintext data. The main problem however with this technique is that it requires the data owner to be online at all times and hence makes it inefficient for everyday users.

Yu et al. [20] proposed one of the first works, which combined ABE, Proxy Re-encryption and lazy encryption schemes for Cloud and security. The scheme works by data owner encrypting his data using a symmetric key and then encrypting the symmetric key using a set of attributes according to KP-ABE scheme. The data owner determines minimum number of attributes to the new user to access and to update the data with the corresponding secret key.

Arockiam et al. [21] proposed a secured confidentiality technique named AROcrypt to ensure the security of data stored in the cloud storage. It also described Security as a Service (SEaaS) in the cloud environment. AROcrypt technique is based on a symmetric encryption technique. The data are encrypted before they are forwarded to the cloud storage. Encrypted data are stored on storage server while secret keys are retained by data owner and access to the user is granted by issuing the corresponding decryption keys. It used the ASCII values to process the plain text into cipher text. The proposed technique provided better performance and maximum security protection when compared with existing confidentiality techniques. The AROcrypt is compared with existing confidentiality techniques like DES, 3DES and Blowfish. Simulations were conducted using a security analysis tool.

Sana Belguith et al. [22] introduced a new lightweight encryption algorithm which consists of combining symmetric algorithm to encrypt data and asymmetric one to distribute keys. This combination helps to benefit from the efficient security of asymmetric encryption and the rapid performance of symmetric encryption while conserving the rights of users to access data by a secured and authorized way. The paper introduced a comparison of two categories of encryption algorithms (Asymmetric and symmetric) using various input files. Evaluation results proved that the processing time of lightweight algorithm is faster. It is also concluded that the symmetric algorithms are more efficient in cloud environment.

O. K. Jasim et al. [23] proposed a new emerging trend of modern symmetric encryption algorithm by development of the advanced encryption standard (AES) algorithm. The new development focuses on the integration between Quantum Key Distribution (QKD) and an enhanced version of AES. A new quantum symmetric encryption algorithm, which is abbreviated as Quantum-AES (QAES), is the output of such integration. This paper discussed the AES block cipher

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

symmetric algorithm. Scalability, easy to implement and resistance against attacks are well-known features for such algorithm [24] [25].

Sekar et al. [26] proposed a new innovative method to enhance the AES algorithm by increasing the key length to 512 bits and thereby the number of rounds is increased in order to provide a stronger encryption method for secure communication. This method doesn't modify the structure of AES, but only increase the number of rounds. Therefore, this algorithm increases the processing time which will limit the use of AES in real applications. The authors proposed to enhance symmetric key encryption algorithm, in which same key is used for encryption and decryption procedure algorithm used. The internal key generation method by random number is used to increase the efficiency of algorithm. This algorithm is more efficient for large data where existing algorithms provides efficient encryption and decryption only for 2MB data. This work provides better speed in comparison to existing algorithms for large size of files with less overhead. The important feature of this proposed method is that it is almost impossible to break the encryption algorithm. Proposed method prevents data from attackers and claims for less time complexity with large data [27].

III. PROPOSED ENCRYPTION TECHNIQUE: AO_ENC CT

The proposed encryption technique is used to protect non-numerical data in the cloud storage. When the user wants to hide only the non-numerical data that are more sensitive, then this proposed encryption might be very comfortable. This technique is based on symmetric crypto system. This algorithm uses three keys for encryption and decryption. Among the three keys two keys are integer and one is string type. When users decide to protect non-numerical data then the proposed AO_Enc CT is more suitable to them to secure their data in cloud.

The proposed technique uses square matrix to manipulate the plaintext and it process the users' data at three levels. First, the data are split based on even and odd column in the matrix. Second, the Key K_1 and K_2 are applied on the data alternatively. Third, data are filled in a square matrix in column-wise and read it in row-wise based on the order of characters in the key K_3. Finally, the ciphertext is produced for submitted plaintext. Decryption is done while reversing the process of encryption steps with same keys. The pseudo code of the proposed AO_Enc CT is given below.

A. Pseudocode of AO_Enc CT for Non-Numerical data:

```
1:  encryption_text(PT)
2:  start
3:  N←sizeof(PT) //  find the size of the PT
4:  for i← 1 to N
        AS[i] ← ASCII(PT[i]) //convert into ASCII
5: next i   //Based on the value of N, form a square matrix RXC
        > N
6:  for i← 1 to N
        if(i*i>=N)
        break
7:  next i
8:  R←C←i
9:  SM[R][C] ←FILL_ROW(AS[i]) // Fill PT into the matrix
        from left to right
10: Split the Matrix into two blocks EB and OB
11: EB ← Even Column from SM[R][C]
12: OB←Odd Column from SM[R][C]
13: EOB←MERGE (EB, OB)
14: Generate key K1 and K2 from Cloud
 //Alternatively applies the key K1 and K2 on EOB and gets an
encrypted text
15: for i←0 to N
        EOB[i] ←EOB[i]+ K1
        EOB[i] ←EOB[++i]+ K2
16: next i
17: Form a matrix based on number of characters in the key
        K3, number of characters in key K3 is equal to number
        of rows in the matrix
18: R←sizeof(K3)
19: C← (N/R)+1
        //Fill the encrypted text into matrix RM[R][C] in
column by column
20: RM[R][C] ←FILL_COLUMN(EOB)
21: AS←READ_ROW(RM[R][C], K3)
        //Read the matrix RM[R][C] row by row in order of
key K3
22: for i← 1 to N
        CT← APPEND (ASCII (AS[i])) //convert into ASCII
23: next i
24: CT←Ciphertext
25: End
```

IV. EXPERIMENT OF AO_ENC CT WITH SAMPLE DATA

The experiment procedure of proposed encryption technique is as follows with a sample data.

Step 1: Consider the following text as the plaintext for encryption,
'welcome to the world of public cloud'

Step 2: Find the total number of characters in the plain text and put as N. Here N is 36.

Step 3: The each character in the plain text is converted into equal ASCII code. Get the following ascii values for each character. It is valued in AS.
AS <-- 119 101 108 99 111 109 101 32 116 111 32 116 104 101 32 119 111 114 108 100 32 111 102 32 112 117 98 108 105 99 32 99 108 111 117 100

Step 4: Based on the value of N, a square matrix is formed. Here, Get 6 x 6 matrix.
*N=36, R*C>=N,R = C = 6*

Step 5: All these ASCII values of plaintext are filled in the 6 x 6 matrix from left to right where SM [R] [C]. Now get the matrix value as mentioned below.

119	101	108	99	111	109
101	32	116	111	32	116
104	101	32	119	111	114
108	100	32	111	102	32
112	117	98	108	105	99
32	99	108	111	117	100

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

Step 6: The above matrix is split into two blocks of even and odd column. The even column is highlighted in the matrix below. The odd and even column values are taken out separately from top to bottom by column by column. And the values are below.

EB → Even column
OB → Odd column

119	101	108	99	111	109
101	32	116	111	32	116
104	101	32	119	111	114
108	100	32	111	102	32
112	117	98	108	105	99
32	99	108	111	117	100

EB<-- 119 101 104 108 112 32 108 116 32 32 98 108 111 32 111 102 105 117

OB<-- 101 32 101 100 117 99 99 111 119 111 108 111 109 116 114 32 99 100

Step 7: Merge the even block values (EB) and odd block values (OB) and it is called as EOB.

EOB <-- 119 101 104 108 112 32 108 116 32 32 98 108 111 32 111 102 105 117 101 32 101 100 117 99 99 111 119 111 108 111 109 116 114 32 99 100

Step 8: As per the choice of the user to get the secret keys, the Key generator in Management as a service (KMaaS) in another service provider generates the keys of K1 and k2 from cloud. Here the sample values of k1 and k2 are 12 and 7 respectively.

Step 9: The values of K1 and k2 are alternatively applied with the values of the merged values in the matrix value of EOB. For example 119 is added with 12, 101 is added 7 and 104 is added with 12 and 108 added with 7 and so on. Now get the value as follows.

EOB <--131 108 116 120 119 44 115 128 39 44 105 120 118 44 118 114 112 129 108 44 108 112 124 111 106 123 126 123 115 123 116 128 121 44 106 112

Step 10: Form a matrix based on size of K3, where the sample value of K3 is TuJB. The value of k3 is a string value here. The number of characters in k3 is 4 which becomes the number of rows. The row value is calculated and derived the value 4 for R, and derived the value of column C from the equation. With the values of R and C, the matrix is defined as 4 x 9 matrix.

R<-- sizeof(K3) <-- 4
C<--(N/R)+1 <-- 36/4 = 9

Step 11: The 4 x 9 matrix is filled with the values of EOB by column by column. The character of k3 is fixed from top to bottom in column wise.

T	*131*	*119*	*39*	*118*	*112*	*108*	*106*	*115*	*121*
u	*108*	*44*	*44*	*44*	*129*	*112*	*123*	*123*	*44*
J	*116*	*115*	*105*	*118*	*108*	*124*	*126*	*116*	*106*
B	*120*	*128*	*120*	*114*	*44*	*111*	*123*	*128*	*112*

Step 12: The value in the matrix is read by Row in order of k3 (AS). The values are read into the below order.

4 <--1 3<--2 1<-- 3 2<--4
AS<-- 120 128 120 114 44 111 123 128 112 116 115 105 118 108 124 126 116 106 131 119 39 118 112 108 106 115 121 108 44 44 44 129 112 123 123 44

Step 13: The values of AS are converted into ASCII characters. Get the ciphertext for the plain text.

CT <-- xÇxr,o{Çptsivl|~tjâw'vpljsyl,,,üp{{,

V. RESULT AND FINDINGS

The proposed encryption technique work properly and produces the ciphertext with combination of all types of ASCII character codes. From the experiment the following results are found.

Plaintext to ciphertext:

The Plaintext is: *welcome to the world of public cloud*

The Ciphertext is :
xÇxr,o{Çptsivl|~tjâw'vpljsyl,,,üp{{,

The Findings: The Character 'l' appears 4 times in the plaintext. The character positions of 'l' are 3 19 28 33 in the plaintext. The ciphertext characters in the same position of 'l' in plaintext is "xâlp". It leads to conclusion that the same character in plaintext carries different character in the ciphertext.

Ciphertext to plaintext:

The Ciphertext is :
xÇxr,o{Çptsivl|~tjâw'vpljsyl,,,üp{{,

The Plaintext is: *welcome to the world of public cloud*

The Findings: The character 'p' in ciphertext appears 3 times in the position of 9 23 33. The plaintext character in same position of ciphertext is "lft". It leads to conclusion that the same character in the ciphertext has got different character in the plaintext. From both these findings the confidentiality is maintained and hence security is enhanced.

VI. CONCLUSION

Data Security in Cloud Computing is a practical concern since it faces lot more challenges. Confidentiality of sensitive data in public cloud environment is much more importance in the world of cloud computing. Many viable solutions are to be explored for the existing problems. Cryptographic techniques are used to provide secure communication between the user and the cloud. Symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data in cloud storage. This paper proposed a symmetric encryption algorithm for secure storage of cloud user data in cloud storage. The proposed encryption algorithm is described in detail and the decryption process is reverse of encryption. This algorithm is used to encrypt non numerical data of the user in cloud. This paper proposes an encryption technique namely AO_Enc CT to hide the non-numeric data from the unauthorized users. The sample data are implemented in the proposed technique and the results are derived to prove

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

that the proposed technique is higher security in protecting the data of the user.

REFERENCES

[1] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", *Technical Report-800-145*, Version 15, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2011.

[2] L. Arockiam, S. Monikandan, G. Parthasarathy "Cloud Computing: A Survey", International Journal of Internet Computing, Volume 1, Issue 2, ISSN: 2231 – 6965, October 2011, pp. 26-33.

[3] Angela Lin, Nan-Chou Chen, Cloud computing as an innovation: Percepetion, attitude, and adoption, International Journal of Information Management, Elsevier Journal, volume 32, 2012, pp. 533–540.

[4] Arockiam L, 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.

[5] Tim Mather, Subra Kumaraswamy, and Shahed Latif, "Cloud Security and Privacy", O'Reilly Media, Inc, 2009.

[6] William Stallings, "Cryptography and Network Security: Principles & Practices", 4th edition, Prentice Hall, ISBN: 978-0-13-187316-2, 2005.

[7] Xiao Z, Xiao Y (2012), "Security and privacy in cloud computing", IEEE Commun Surveys Tutorials 99:1–17.

[8] Oza N, Karppinen K, Savola R (2010), "User experience and security in the cloud-An empirical study in the finish cloud consortium", IEEE second international conference on cloud computing technology and science (CloudCom) 2010:621–628.

[9] Rocha F, Abreu S, Correia M (2011), The final Frontier: confidentiality and privacy in the cloud, pp 44–50.

[10] D. Zissis and D. Lekkas. "Addressing cloud computing security issues". Future Generation Computer Systems, 28(3), 2012, pp. 583-592.

[11] H. Rahmani, E. Sundararajan, Z. M. Ali, and A. M. Zin, "Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud". Procedia Technology, vol. 11, 2013, pp. 1202-1210.

[12] 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.

[13] Rashmi Nigoti, Manoj Jhuria, 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.

[14] 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.

[15] A.L.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, Pp.3033-3037.

[16] Eman M.Mohamed, Hatem S. Abdelkader and Sherif El-Etriby, "Data Security Model for Cloud Computing", The Twelfth International Conference on Networks, ISBN: 978-1-61208-245-5, pp 66-74, 2013.

[17] P. Srinivasarao, P. V. Lakshmipriya, P. C. S. Azad, T. Alekhya, K. Raghavendrarao & K. Kishore, "A Technique for Data Encryption and Decryption", International Journal of Future Generation Communication and Networking, Vol.7, No.2 (2014), http://dx.doi.org/10.14257/ijfgcn.2014.7.2.12, pp.117-126.

[18] Shaza D. Rihan, Ahmed Khalid, Saife Eldin F. Osman, "A Performance Comparison of Encryption Algorithms AES and DES", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 12, December-2015, pp. 151-154.

[19] Zhao G, Rong C, Li J, Zhang F, Tang Y (2010) Trusted data sharing over untrusted cloud storage providers. IEEE second international conference cloud computing technology and science (CloudCom) 2010, pp 97–103.

[20] Yu S, Wang C, Ren K, Lou W(2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: INFOCOM, 2010 proceedings IEEE, pp 1–9.

[21] 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: 2278-0181, Vol. 3 Issue 12, December-2014, pp. 1053-1058.

[22] Sana Belguith, Abderrazak Jemai, Rabah Attia, "Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm", CAS 2015: The Eleventh International Conference on Autonomic and Autonomous Systems, Copyright (c) IARIA, 2015. ISBN: 978-1-61208-405-3, pp. 98-103.

[23] Omer K. Jasim, Safia Abbas, El-Sayed M. Horbaty, "Evolution of an Emerging Symmetric Quantum Cryptographic Algorithm", Journal of Information Security, 2015, 6, 82-92, Published Online April 2015 in SciRes. http://www.scirp.org/journal/jis http://dx.doi.org/10.4236/jis.2015.62009. pp. 82-92.

[24] Matthew, G. (2013) Statistical Tests of Randomness on QKD through a Free-Space Channel Coupled to Daylight Noise. Journal of Light Wave Technology, 3, 34-35.

[25] Hadi, S., Alireza, S., Behnam, B. and Mohammadraze, A. (2013) Cryptanalysis of 7-Round AES-128. International Journal of Computer Application, 10, 21-29.

[26] Sekar, A., Radhika, S. and Anand, K. (2012) Secure Communication Using 512 Bit Key. European Journal of Scientific Research, 52, 61-65.

[27] Krishna Kumar Pandey, Vikas Rangari, Sitesh KumarSinha, "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security", Volume 74, No. 20, 2013, pp. 29-33.

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.