ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm

Dr. L. Arockiam[1], S. Monikandan[2]

Associate Professor, St. Joseph's College, Trichy, Tamilnadu, India[1]

Research scholar, M S University, Tirunelveli, Tamilnadu, India[2]

Abstract – One of the primary usage of cloud computing is data storage. Cloud provides enormous capacity of storage for cloud users. It is more reliable and flexible to users to store and retrieve their data at anytime and anywhere. It is an increasingly growing technology. Nowadays, many enterprises have started using cloud storage due to its advantages. Even though the cloud continues to gain popularity in usability and attraction, the problems lie in data security, data privacy and other data protection issues. Security and privacy of data stored in the cloud are major setbacks in the field of Cloud Computing. Security and privacy are the key issues for cloud storage. This paper proposes an encryption algorithm to address the security and privacy issue in cloud storage in order to protect the data stored in the cloud.

Keywords: Cloud Storage, Security, Privacy, Encryption Algorithm, Cryptography

I. INTRODUCTION

Cloud is a technology invention. It provides the computational resources (Server, Storage, OS and Network) to user as service based on demand. Cloud computing has emerged as a popular solution to provide cheap and easy access to externalized IT (Information Technology) resources. An increasing number of organizations (e.g., research centres, enterprises) benefit from Cloud computing to host their applications [1]-[2]. Virtualization is the core concept supported in the cloud computing. Resources are provided to cloud users as virtualized manner [3]. Virtualization and cloud computing can be used quite successfully to improve the resilience of an IT environment. Because, they provide the means to recover quickly from component or system malfunctions using failover. Quickly take back up of essential applications and data. Virtual machines can be migrated from one physical server to another in a live migration; virtual machine images can be restarted in a different location to provide for disaster recovery [4].

Cloud has three types of services. They are Software as a service, Platform as a service and Infrastructure as a service. Cloud services are provided by the different cloud providers like Amazon, Google, Microsoft, IBM and etc. The users can utilize these services (SaaS, PaaS and IaaS) based on their requirement. Usage of these three services, user's data are stored in the cloud storage. Cloud providers are maintaining the user's data in cloud environment. The data in the provider's hands could make security and privacy issue in cloud storage.

With cloud computing, all users' data are stored on the cloud. So cloud users have to think about their data [5] like: security of the data in the cloud, Access control and authentication of the cloud. Cloud computing companies say that data is secure, but it is too early to be completely sure of. Only time will tell if user's data is secure in the cloud.

Cloud security and privacy concerns are arising in which both customer's data and application are residing in provider's premises. Security and privacy are always a major concern in cloud computing [6]-[7] as shown in Fig.1. It shows the survey report of 2008 and 2009 by International Data Corporation (IDC). From the figure, it is clear that security is the top most concern in cloud computing in the survey of both years.

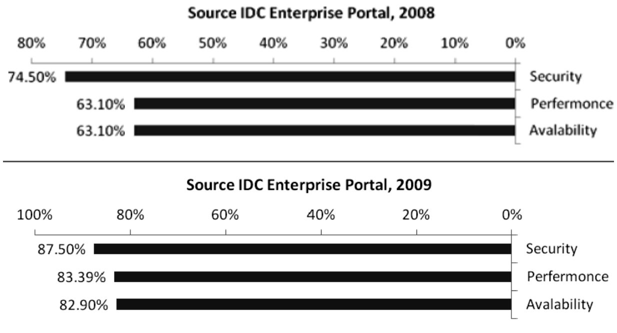


Fig.1 Security is a major concern to cloud computing [6]-[7]

While cost and ease of use are two great benefits of cloud computing [5], there are significant security concerns that need to be addressed while moving critical applications and sensitive data to public and Cloud storage.

Cloud data may be attacked in two ways. One is outsider attack and the other is insider attack. Insider as an administrator can have the possibility to hack the user's data. Insider attack 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 shouldn't get the actual data. So, all the data must be encrypted before it is transmitted to the cloud storage.

Cryptography is a technique applied for encryption and decryption. In the field of cryptography there are several techniques available for encryption/decryption. These techniques can be generally classified into two major groups, i.e. Conventional and public key Cryptography [8]. Conventional cryptography is also referred as symmetric encryption or single key encryption. Same key is used for encryption and decryption. Public key cryptography is referred as asymmetric encryption or public key encryption. Separate keys are used for encryption and decryption. Fig.2 represents the simplified model for conversional encryption technique.

The original intelligible message, referred as plaintext, is converted into apparently random ambiguous message, referred as ciphertext. The encryption process consists of an algorithm and a key. The key is a value independent on the specific of the plain text. The algorithm will produce a different output depending on the specific key being used at that time. Changing the key changes the output of the algorithm.

Once the ciphertext is produced, it may be transmitted to cloud storage. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm with the same key that was used in encryption.

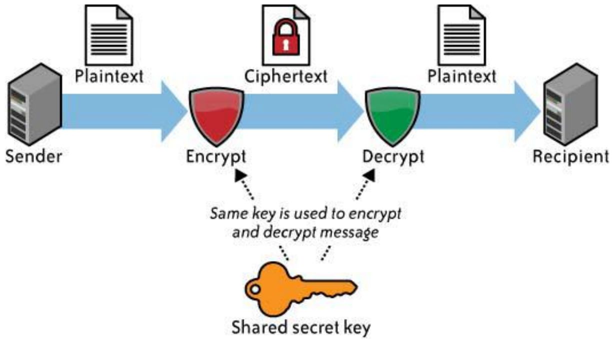


Fig.2 Model of Conventional Encryption [9]

This paper proposes a symmetric encryption algorithm to protect the user's data stored in the cloud storage from the unauthorized access.

The paper is organized as follows. Section II gives the detail on the various issues in cloud data storage. Section III describes the symmetric encryption algorithm and how it is executed. Section IV talks about the different classical encryption algorithms that are already used in the data security. In Section V, proposed encryption and decryption algorithm are described in detail. Section VI gives the conclusion for the paper.

II. ISSUES IN CLOUD DATA STORAGE

Cloud Computing moves the application and data to the cloud storage, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. This paper focuses on cloud data storage security, which has always been an important aspect of quality of service. Following are the issues [10] in cloud data storage.

A. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology. User's personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders. At this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depending on the computing task submitted by the users.

The major privacy issues [11] relate to i) Trust, i.e. whether there is unauthorized secondary usage of PII (Personally Identifiable Information), ii) Uncertainty, i.e. ensuring that data has been properly destroyed by the one who controls retention of data on how the privacy breaches have occurred and how the fault is determined in such cases iii) Compliance, i.e. environments with data proliferation and global, dynamic flows, and addressing the difficulty in complying with transborder data flow requirements.

B. Security

Security concerns relate to risk areas such as external data storage, dependency on the public internet, lack of control, multi-tenancy and integration with internal security [12].

Cloud service providers employ data storage and transmission encryption, user authentication, and authorization. Many clients worry on the vulnerability of remote data to hackers. Cloud providers are enormously sensitive to this issue and apply substantial resources to mitigate this problem.

C. Trust

Trust issue in cloud computing has equal concern against security and privacy. Trust is defined as reliance on the integrity, strength, ability and surety of a person or thing. Entrusting user data on to a third party who is providing cloud services is an issue. For example, in April 2012, Amazon's Elastic Compute Cloud service crashed during a system upgrade, knocking customers' websites off-line all over for several hours for several days. Another incident happened on the same month. The hackers broke into the Sony PlayStation Network, exposing the personal information to 77 million people around the world. These issues have certainly created doubts in mind of cloud users and damaged the trust [10].

D. Ownership

Once data has been submitted to the cloud, developers have concern about losing their rights or being unable to protect the rights of their customers. Many cloud providers address this issue with well-skilled user-sided agreements.

According to the agreement, users would be wise to seek advice from their favourite legal representative.

E. Performance and Availability

Business organizations are worried about acceptable levels of performance and availability of applications hosted in the cloud. Application and data in the cloud storage should be available to the users at anytime and anywhere. Users have no worry about the local system which is used for accessing the cloud servers.

F. *Long-term Viability*

Users should be sure that the data put into the cloud will never become invalid even the cloud computing provider get lost or get acquired and swallowed up by a larger company. Users should ask their potential providers of cloud how they would get user's data back and if it would be in a format that user could import into a replacement application [13].

H. Data Backup

Cloud providers employ redundant servers and routine data backup processes, but users worry about being able to control their own backups. Many providers are now offering data dumps onto media or allowing users to back up data through regular downloads.

G. Data Portability and Conversion

Users have concerns on data portability like, switching between service providers. There may be difficulty in transferring data. Porting and converting data is highly dependent on the nature of the cloud provider's data retrieval format, particularly in cases where the format cannot be easily revealed. As service competition grows, open standards become established, the data portability issue will ease, and conversion processes will become available supporting the more popular cloud providers. Worst case is that the cloud subscribers have to pay for some custom data conversion.

These are certain areas in which cloud computing requires to excel and solve problem related to it. Out of all the problems; narrated Security and Privacy [14] put the major threats in growth of cloud computing. It needs to be worked upon.

III. SYMMETRIC ENCRYPTION

Symmetric encryption (see Fig.2) involves the use of a single secret key for both the encryption and decryption of data. Only symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data [9].

For example, a source produces a message in plaintext, $X = [X_1, X_2, X_{3,....} X_M]$. For Encryption, a key is generated at the message source. Then the key is also provided to the destination by means of some secure channel. With the message X and the encryption key K as input, the encryption algorithm forms the cipher text $Y = [Y_{1,} Y_{2,....} Y_N]$. This may be written as $Y = E_K(X)$. Cipher text Y is produced by using encryption algorithm, where E indicates the encryption algorithm used and K indicates the key used for encryption. The receiver of this message should apply decryption algorithm with same key used for encryption to get the actual message $X = D_K[Y]$. Here D indicates decryption algorithm.

IV. CLASSICAL ENCRYPTION

Several encryption algorithms are available and are used in information security. These algorithms can be categorized as classical encryptions [15]. These encryption algorithms are based on two general principles namely substitution cipher, in which each element in the plaintext is mapped into another element, and transposition cipher, in which elements in the plaintext are rearranged. Out of the different encryption algorithms, few algorithms are described in this section.

A. Caesar Cipher

Caesar cipher [16] is a classical substitution cipher and it is one of the simplest examples of substitution cipher. It replaces alphabet of letter in the plain text, with a letter 3 places ahead of it. For example, "HELLO" is a plain text which will be converted into "KHOOR" as cipher text. One can see that such a cipher may be difficult to break. This cipher can be broken by brute force attack because at the end there are only 25 possible available options of key.

B. Playfair Cipher

Another example of classical substitution cipher is Playfair cipher [17] which has a square matrix of 5X5 alphabetical letters arranged in an appropriate manner. The user can select a key and place it in the matrix. The remaining letters of English alphabet from the key are then one by one placed in the matrix of Playfair cipher. The plain text is broken into pairs and if a pair has same alphabet then they are separated by introducing a filler letter with 'x'. Otherwise if the pair is with different alphabetical letters and resides in the same row of matrix then each letter is replaced by the letter ahead of it. If the pair of letters is in same column of matrix then each letter is replaced by the letter below it, and when the pair of letters is neither in same column nor in same row then they are replaced by the letter in their row that resides at the intersection of paired letters.

C. Vigenere Cipher

Vigenere cipher [18] when compared with Caesar cipher gives some level of security with the introduction of a keyword. This key word is repeated to cover the length of the plain text which is to be encrypted. Example is shown below:

KEY : f a u z a n f a u z a n
Plain text : c r y p t o g r a p h y
Cipher : H R S O T B L R U O H L

As it can be seen from that above example, "fauzan" is a keyword and plain text is "cryptography" which is encrypted into “HRSOTBLRUOHL”. This is done using Vigenere table which contains alphabets in form of rows and columns left most column. The left most column indicates keyword and top most row indicates plaintext and at the junction of two alphabetical letters resides our replacement. After individually transforming every letter, user gets an encrypted message.

D. Rail fence technique

This is one of the transposition ciphers [8], in which the plain text is written down as a sequence of diagonal and then read as a sequence of rows. For example, to encipher the message “ hai welcome” with a rail fence of depth 2,

h i e c m
a w l o e

Now the encrypted message is “hiecmawloe”.
In this technique the same alphabets in the plaintext is rearranged. This technique alone cannot be sufficient for data security.

V. PROPOSED ALGORITHM

Proposed technique emphasizes on improving classical encryption techniques by integrating substitution cipher and transposition cipher. Both substitution and transposition techniques have used alphabet for cipher text. In the proposed algorithm, initially the plain text is converted into corresponding ASCII code value of each alphabet. In classical encryption technique, the key value ranges between 1 to 26 or key may be string (combination alphabets). But in proposed algorithm, key value range between 1 to 256. This algorithm is used in order to encrypt the data of the user in the clouds. Since the user has no control over the data after his session is logged out, the encryption key acts as the primary authentication for the user. Proposed algorithm is described below.

A. Encryption Algorithm

Followings are the steps in proposed encryption algorithm.

Encryption Algorithm:

step 1. Count the No. of character (N) in the plain text without space.
step 2. Convert the plain text into equivalent ASCII code. And form a square matrix ($S_X S >=N$).
step 3. Apply the converted ASCII code value from left to right in the matrix. Divide matrix into three part namely upper, diagonal and lower matrix.
step 4. Read the value from right to left in each matrix.
step 5. Each matrix use three different key $K=K_1$, K_2, K_3 for encryption. Do the encryption.
step 6. Apply the encrypted value into the matrix in the same order of upper, diagonal and lower.
step 7. Read the message by column by column. Here the order in the columns read from the matrix is the key K_4.
step 8. Convert the ASCII code into character value.

The followings are the detailed description of each step in the proposed encryption algorithm.

Step 1:- Count No.of characters (N) in the message without space.

Plaintext - HIHOWAREYOU.

N= 11 (N = No. of Characters in the Message)

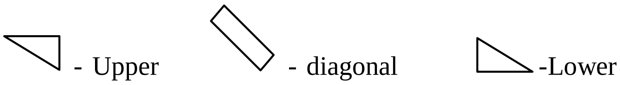
Step 2:- Convert the plain text into equivalent ASCII code. And form a square matrix.

ASCII code value for the plaintext:
72 73 72 79 87 65 82 69 89 79 85

To form a square matrix, choose a number (S), square value of S is immediately next to N. i.e. S^2 is nearest square value N and S^2 >= N.
For this plaintext N=11, so S=4.

The order of matrix is 4 $_X$ 4>=11, Form a 4 $_X$ 4 matrix.

Step 3:- Apply the converted ASCII code message row by row in S $_X$ S matrix. Separate the matrix into three parts as Upper, Diagonal and Lower. Following shapes represent the upper, diagonal and lower matrix position in the square matrix.



72	73	72	79
87	65	82	69
89	79	85	65
66	67	68	69

Step 4:- Read the message from left to right for upper, diagonal and lower.

72	73	72	79
87	65	82	69
89	79	85	65
66	67	68	69

The values of three matrixes are,

Upper Matrix	-	73 72 79 82 69 65
Diagonal	-	72 65 85 69
Lower matrix	-	87 89 79 66 67 68

Step 5:- To encrypt the message use three different keys for upper, diagonal and lower matrix separately. Keys are $K=K_1$ for upper matrix, K_2 for diagonal matrix and K_3 for lower matrix.

Upper Matrix =23 -- K_1
Diagonal Matrix =17 -- K_2

Lower Matrix =6 -- K_3

Now add this key value with ASCII code message of each matrix.

After Encryption:

Upper Matrix	- 96 95 102 105 92 88
Diagonal	- 89 82 102 86
Lower matrix	- 93 95 85 72 73 74

Step 6:- Apply the message into the square matrix in the same order of how it was read.

89	96	95	102
93	82	105	92
95	85	102	88
72	73	74	86

Step 7:- Now Read the message from the matrix by column by column. Here the order of the columns read in the matrix is the key K_4.

4	2	1	3
89	96	95	102
93	82	105	92
95	85	102	88
72	73	74	86

Key- K_4

Encrypted text is:
95 105 102 74 96 82 85 73 102 92 88 86 89 93 95 72

Step 8:- Covert the ASCII code into the equivalent character value. Then,

Encrypted cipher text is _ifJ'RUIf\XVY]_H

B. *Decryption Algorithm*

The encrypted data is stored in the cloud storage. To retrieve the data from cloud, decryption is necessary to get the actual data in the cloud. Decryption is possible only with key values which are used for encryption. So key should have a vital role in encryption and decryption algorithm. Following steps illustrate the decryption algorithm.

Decryption Algorithm:

step 1. The encrypted text is converted into ASCII code values.
step 2. Count the No.of character (N) in the decrypted text and form a square matrix $S_X S$.
step 3. Apply the ASCII code in the $S_X S$ matrix as column by column based on key K_4.
step 4. Divide the matrix into upper, diagonal and lower.
step 5. Apply reverse encryption using the keys K_1, K_2 and K_3 on the upper, diagonal and lower matrix respectively.
step 6. Apply the message into table by upper, diagonal and lower matrix.
step 7. Read the message as row by row from left to right.
step 8. Convert the ASCII code into character value.

The followings are the detailed description of each step in the decryption algorithm.

Step1:- Each character in the encrypted text is converted into equivalent ASCII code values.

Encrypted text = _ifJ'RUIf\XVY]_H

Convert it into ASCII code, as below
95 105 102 74 96 82 85 73 102 92 88 86 89 93 95 72

Step2:- Count the No.of character (N) in the decrypted text and form a square matrix $S_X S$.

No. of characters are N=16, so S=4,
Order of matrix is $4_X 4$.

Step3:- Apply the ASCII code in the $S_X S$ matrix as column by column based on key K_4.

Now the matrix is,

4	2	1	3
89	96	95	102
93	82	105	92
95	85	102	88
72	73	74	86

Key- K_4

Step4:- Divide the matrix into upper, diagonal and lower.

Read the message in the matrixes from left to right.

89	96	95	102
93	82	105	92
95	85	102	88
72	73	74	86

Now, message in each matrix is

Upper Matrix	- 96 95 102 105 92 88
Diagonal	- 89 82 102 86
Lower matrix	- 93 95 85 72 73 74

Step5:- Apply reverse encryption using the keys K_1, K_2 and K_3 on the upper, diagonal and lower matrix respectively.

Upper Matrix	=23 -- K_1
Diagonal Matrix	=17 -- K_2
Lower Matrix	=6 -- K_3

Decrypt the message using the keys. The values of three matrixes after decryption

Upper Matrix - 73 72 79 82 69 65
Diagonal - 72 65 85 69
Lower matrix - 87 89 79 66 67 68

Step6:- Apply the message into table by upper, diagonal and lower matrix.

Matrix is,

72	73	72	79
87	65	82	69
89	79	85	65
66	67	68	69

Step7:- Read the message as row by row from left to right.

72	73	72	79
87	65	82	69
89	79	85	65
66	67	68	69

Now the message is,
72 73 72 79 87 65 82 69 89 79 85 65 66 67 68 69

Step8:- Convert the ASCII code into equivalent character value. Then,

Decrypted result is,
HIHOWAREYOU
By completion of all these steps in the decryption algorithm the original text is retrieved by the user. In both encryption and decryption, key is more important. Algorithm could be known to everyone but key should be known only to authorize user.

VI. CONCLUSION

Security and Privacy of data stored in Cloud Computing is an area which has full of challenges and of paramount importance. Many research problems are yet to be identified. 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 the encryption. This algorithm is used in order to encrypt the data of the user in the cloud. Since the user has no control over the data once their session is logged out, the encryption key acts as the primary authentication for the user. By applying this encryption algorithm, user ensures that the data is stored only on secured storage and it cannot be accessed by administrators or intruders.

REFERENCE

[1] J.Srinivas, K.Venkata Subba Reddy and Dr. A.Moiz Qyser, ”Cloud Computing Basics”, International Journal of Advanced Research in Computer and Communication EngineeringVol.1, Issue 5, pp 343-347, 2012.

[2] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Henghu Gong, ”The Characteristics of Cloud Computing”, 39th International Conference on Parallel Processing Workshops, IEEE XPlore, 1530-2016/10, pp 275-279, 2010.

[3] Karen Scarfone, Murugiah Souppaya, Paul Hoffman, “Guide to Security for Full Virtualization Technologies “, http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf , NIST, 2011.

[4] Stratus Technologies, “white paper on Server Virtualization and CloudComputing:Four hidden impacts on uptime and availability” ,http://www.stratus.com/~/media/Stratus/Files/Library/WhitePapers /ServerVirtualizationandCloudComputing.pdf , 2011.

[5] 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.

[6] Peter Mell, Tim Grance, “Effectively and Securely Using the Cloud Computing Paradigm”, NIST, Information Technology Laboratory, http://www.csrc.nist.gov/groups/SNS/cloud-comput ing/cloud-computing-v26.ppt. 2009.

[7] Frank Gens et al., “Cloud Computing 2010 An IDC Update ”http://www.cionet.com/Data/files/groups/Cloud%20Computing%2 02010%20-%20An%20IDC%20Update.pdf ,2010.

[8] William Stallings, “Cryptography and Network Security: Principles & Practices”, Fifth edition, Prentice Hall, ISBN-13: 978-0136097044, 2010.

[9] Tim Mather, Subra Kumaraswamy, and Shahed Latif “Cloud Security and Privacy”, O’Reilly Media, Inc, pp 61-71, 2009. [10] Mohit Marwaha, Rajeev Bedi, “Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing”, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, pp 367-370, 2013.

[11] Siani Pearson, “Privacy, Security and Trust in Cloud Computing”, HP Laboratories, HPL-2012-80R1, appeared as a book chapter by Springer, pp 1-56, 2012.

[12] K Hashizume et al., “An analysis of security issues for cloud computing”, Journal of Internet Services and Applications, a Springer open journal, pp 1-13, 2013.

[13] Pankaj Arora et al., ”Cloud Computing Security Issues in Infrastructure as a Service”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, 2012.

[14] Pardeep Sharma, Sandeep K. Sood, and Sumeet Kaur, “Security Issues in Cloud Computing”, Springer-Verlag Berlin Heidelberg, HPAGC 2011, CCIS 169, pp 36–45, 2011.

[15] Vamsee Krishna, Yarlagadda And Sriram Ramanujam, “Data Security in Cloud Computing”, Journal of Computer and Mathematical Sciences, Vol.2 (1), pp 15-23, 2011.

[16] Dr.A.Padmapriya, P.Subhasri,” Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security”, International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4, pp 1067-1071, 2013.

[17] V.U.K. Sastry, N. Ravi Shankar and S. Durga Bhavani, “A Generalized Playfair Cipher involving Intertwining, Interweaving and Iteration”, International Journal of Network and Mobile Technologies, pp 45-53, 2010.

[18] Quist-Aphetsi Kester, “A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher”, International Journal of Advanced Technology & Engineering Research (IJATER), Volume 3, Issue 1, pp 141-147, 2013.

BIOGRAPHY

Dr. Arockiam. L is working as Associate Professor in the Department of Computer Science, St.Joseph’s College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has 24 years of experience in teaching and 17 years of experience in research. He has published more than 140 research articles in the International / National Conferences and Journals. He has also presented 2 research articles in the Software Measurement European Forum in Rome. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has authored a book on “Success through Soft Skills”. His research interests are: Software Measurement, Cognitive Aspects in Programming, Data Mining, Mobile Networks and Cloud Computing. He has been awarded “Best Research Publications in Science” for 2010, 2011, & 2012 and ASDF Global Awards for “Best Academic Researcher” from ASDF, Pondicherry for the academic year 2012-13.

S. Monikandan is working as Assistant Professor in Christhuraj Institute of Computer Application, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India. He is completed his MCA and M.Tech degree in Bharathidasan University, Tiruchirappalli in 2007 and 2009 respectively. Now, he is pursuing his research in Manonmaniam Sundaranar University, Tirunelveli. He has attended many International and National Conferences, Seminars and Workshops. His research interest is web technology and cloud storage security.