# Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage

Dr. S. S. Manikandasaran
Dean, Department of MCA,
Christhuraj Institute of Computer Applications,
Christhu Raj College, Trichy,
Tamil Nadu, India

***Abstract*—Cloud computing dominates the IT industry in recent years. It provides many advantages to the enterprises those who are not having enough computing infrastructure for computing business. Computational resources are provided in virtualized manner. Multiple datacentres are run for storing and maintaining the users' data. This multiple datacentres are situated in different geographical location in the world. Users' data are stored in the datacentres of cloud and controlled and monitored by cloud service providers. Users don't have any control or rights on their data stored in the cloud not even know the location of the data in cloud. This nature of cloud makes many security related issues on the data stored in the cloud. The big problem in cloud is security of data in the cloud. Cloud data are attacked by insiders as well as outsiders in different ways. This paper describes the different types of attacks on cloud data and also presents what are cryptography solutions are available to protect the data from the different attacks. Security is addressed by different parameters like authentication, authorization, confidentiality and integrity. Among this, ensuring confidentiality protects the data in cloud storage.**

***Keywords-Cloud Storage; Security Attacks; Confidentiality; Cryptography; Cloud Security;***

## I. INTRODUCTION

Cloud computing provides visualized resources to the users which means actual software or server is running in the cloud server but users could access the software or server from their local machine. All the computational resources are provisioned to users instantly based on their demand. Main advantage of cloud is to provide huge virtual storage to the users [1].

Cloud makes data storage very smart. It provides an enormous amount of virtual space to store the users' data. The data are instantly available for the users at anytime, anywhere and any number of times. Cloud reduces the cost with respect to hardware support, technical experts available and license of the database. It leverages the small and medium scale enterprises straight away to start their business [2]. Nevertheless, cloud has many disadvantages due to security. Enterprises are hesitating to deploy their data in the cloud storage, because data security issue is the top most concern in Cloud Storage (CS) [3]. Security issues arise from the attack on data stored in the cloud storage by the hackers. Hackers are either privileged administrator from Cloud Service Providers (CSP) or other users of cloud storage. Many security frameworks are proposed by various researchers, especially for ensuring confidentiality of data in cloud storage. Security grips a prominent place in the usage of cloud storage, because it restricts many of the attacks on data from hackers [4].

Cloud is the fast growing technology and it has some security issues related to data protection; the existing frameworks could not perform well due to the security issues from the CSPs and the nature of cloud [5]. Moreover, in most of the existing frameworks, users have to work more for securing their data and are responsible to maintain the components of the framework in their own premises. Users are forced to use the infrastructure like software, platform and storage from single CSP [6].

Securityofdataincloudisachallengeandisofsupreme importanceasmanyflawsandconcernsareyettobe identified. Dataprotectionisacrucialsecurityissueformostoftheenterprises[7]. Themanagementof the dataand services[8]maynotbefullytrustworthyandtheenterprises donot haveanycontrolon the data,sincethedatacentersare remotelylocated.Moreover,dataarestoredinamultitenantenvironment. Thecommonsecurityconcernsare:

1.Securingdataintransitandatrest,
2.Securesoftware interfaces,
3.Useraccesscontrol,and
4.Dataseparation.

Since,dataincloudcomputingisplacedinthehandsof thirdparties,ensuringthedatasecuritybothatrest(data residingonstoragemedia),aswellas,intransitisof greatimportance.Giventhelargenumberofissuesconcerning datasecurity,manyorganizationsneedclearanswersregarding datasecuritybefore migratingto the cloud.Theusers'dataconfidentiality and integrityaremaintainedbyprovidingdatasecuritywhichisanimportant qualityof service incloudcomputing. Data securityinthecloud includes the following [9] Data security in network, host and application levels has become a vital part of cloud storage. Thedatain cloudcan bein any of theforms as shown in figure 1[10].

Hence**,** data security of all the above mentioned forms is the most vital factor to be considered. Users' Data at Rest

which storedon thephysical storage shouldnot bemodified.Encryptingthedatamaybethesolutionforthis,butinca seofPaaSand SaaS models,encryptionofdataisnotalwaysfeasibleandhencetheproba bilityof unauthorized access is veryhigh.Furthermore, datamustbesecured whiletransferring betweenservers.Itshouldnotbeviewedorchangedbyotherusers.S o,itrequiresan appropriateencryption algorithm, as well as, a secureprotocol. Also, Users'datashouldnotbeviewedor changed byother userat runtime.

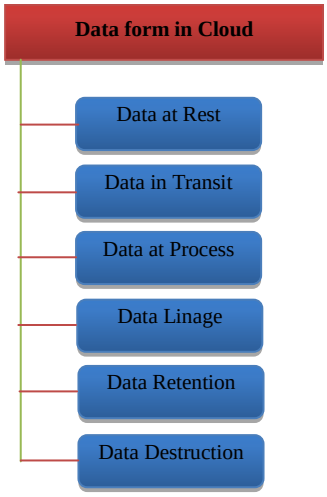


Fig.1Data Forms in Cloud

Finally, data lineage dealswithmaintainingtheoriginandcustodyof datainordertopreventtamperingandtoassure the integrityofdata.However,thisis a time-consumingjob.Tryingtoprovideaccuratereportingondatalineag eforpubliccloud services is not possible [10].

## II. Data Protection in Cloud

Data protection in cloud computing is very important factor it could be complicated for the cloud customer to efficiently check the behaviour of the cloud suppliers and as a result they are confident that data is handled in a legal way, but it does not like that this problem is intensify in case of various transformation of data [11]. Counter measure for this attack is that a consumer of cloud computing should check data handle and established whether it is handled lawfully or not.

Incomplete data deletion is very risky in cloud computing environment. It does not remove completed data because replicas of data are placed in other servers [12]. Counter measure is that Virtualized private networks should use for securing the data and used the query that will remove the complete data from the main servers along with its replicas.

Generally cloud data are attacked by insiders and outsiders [13]. Insiders are employees, entrepreneurs and associates which are still or former attended who can or could access the whole information system with privileged authority are defined as insider. Insider attacks are organized and run by these individuals to harm or temper knowledge about consumers or providers and include every kind of attacks which can be executed from inside. This attack is very difficult to identify.

Outsiders are users from outside the cloud environment could enter into the cloud and try to attack the data. Outsiders are intruders who can illegally enter into the cloud. Outsider attacks are happened to get other users sensitive information in cloud. Proper authentication mechanism may protect the outsider attacks [14].

## III. Cryptographic Technique for Cloud Storage

Process of encryption involves using a cryptographic algorithm and a cryptographic key to transform a plaintext into a ciphertext [15]. In the field of cryptography, several techniques are available for encryption and decryption. These techniques can be generally classified into two major groups, i.e. conventional cryptography and public key cryptography [16].

Conventional cryptography is referred to as symmetric encryption or single key encryption. Same key is used for encryption and decryption. This means that the encryption key is equal to the decryption key. Figure 2 represents the simplified model for conversional encryption technique. In general, there are two types of the symmetric ciphers, namely, stream ciphers and block ciphers.

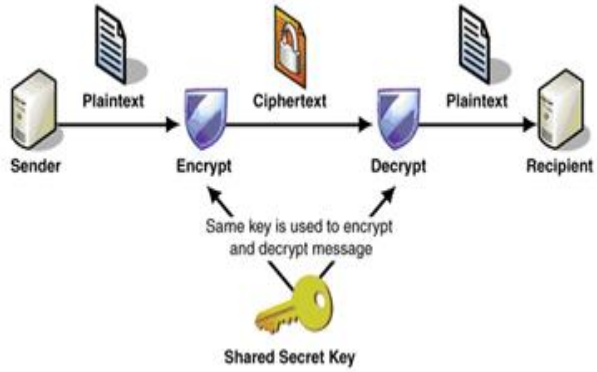


Fig. 2 Symmetric Encryption Technique [17]

Stream ciphers take the plaintext as streams of characters with size of 1 bit or n-bit word. In cipher, the plaintext is encrypted (and decrypted) one character at a time. According to Alfred et al. [18], stream ciphers are used in real-time applications such as pay TV and communications. This is because they are able to run in high speed.

In Block ciphers, the plaintext is encrypted (and decrypted) one block at a time. The block size is commonly 64-bit or 128-bit.

Public key cryptography is referred to as asymmetric encryption or public key encryption in which there are two keys used, meaning that the encryption key is not equal to the decryption key. In this cipher, sender and receiver need to have two keys; a public key (which is made public) and a private key (which is kept secret). Figure 3 represents public key

cryptosystem. The public key is used for the encryption process and the private key is used for the decryption process. Separate keys are used for encryption and decryption.

The original intelligible message, referred to as plaintext, is converted into apparently random ambiguous message, called ciphertext. The keys are independent on the specific of the plaintext. 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.

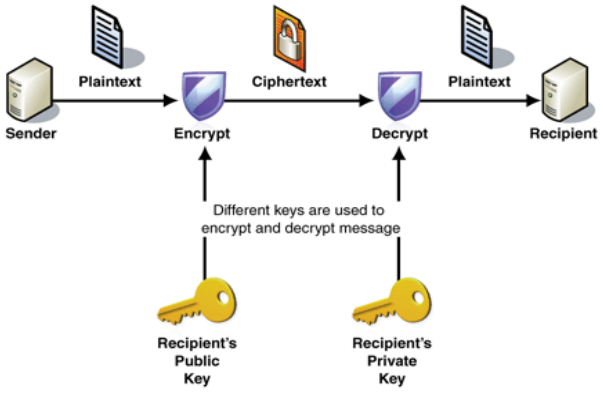


Fig. 3 Asymmetric Encryption Technique [17]

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.

Only symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data. It would be highly unusual to use an asymmetric algorithm for this encryption use case [10]. Symmetric encryption algorithm is suitable to use for cloud data storage security, [19].

## IV. Types of Attacks in Cloud Computing

It is noted that the security of a cryptosystem must be entirely based on the keys. Attacks on the secrecy of encryption schemes try to recover plaintexts from the ciphertext, or even more drastically to recover the secret key [18]. The possible attacks depend on the resources available in the adversary. Cryptographic attacks are designed to subvert the security of cryptographic algorithms and they are used to decrypt data without access to a key. The next subsection presents various kinds of attacks normally encountered in cryptographic algorithms[20][21][22][23][24][25][26].

### A. *Ciphertext-Only Attack*

In this type of attack, the cryptanalyst has the ciphertext of several messages and they have been encrypted using the same encryption algorithm. The job of cryptanalyst is to recover the plaintext as possible or could deduce the key(s) which is used to encrypt and decrypt the message.

### B. *Known-Plaintext Attack*

In this type of attack, the cryptanalyst knows the encryption algorithm and ciphertext to be deduced. Cryptanalyst's role is to deduce the key(s) used to encrypt the message or an algorithm to decrypt the new message encrypted with the same key(s).

### C. *Chosen-Plaintext Attack*

In this type, the cryptanalyst has access not only to ciphertext and associated plaintext for several data but also chooses the specific plaintext blocks to encrypt which yield more information about the key. Cryptanalyst job is to deduce the key(s) used to encrypt the messages or an algorithm to decrypt any new message encrypted with the same key(s).

### D. *Chosen-Ciphertext Attack*

In this attack, the cryptanalyst knows different ciphertexts to be decrypted and has access to the decrypted plaintext. Cryptanalyst's job is to deduce the key.

### E. *Meet-in-the-middle attack*

It is another type of known plaintext. The Meet-in-the middle attacker uses two different keys to encrypt the plaintext with a different combination of keys and decrypt the ciphertext with another set of keys to get the necessary key to get the original message.

### F. *Man in the Middle Attack*

This type of attack occurs when the secure socket layer (SSL) is not properly installed when two parties are communicating with each other then there is a possibility that all the data communication between two parties could be hacked by the middle party. Therefore countermeasures are required to be taken to protect the data from the middle attack.

### G. *Brute Force Attack*

A brute force attack is a trial-and-error method used to obtain information such as a user password or Personal Identification Number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

### H. *Dictionary Attack*

In this attack, every word in the dictionary is tried as a possible password for an encrypted message. A dictionary attack is generally more efficient than brute force attack.

### I. *Birthday attack*

It is another class of brute-force attack which uses probability theory in a set of randomly selected people. A number of permutations are applied to get information from the communication among a set of people.

### J. *Pre-computation attack*

The crypto attacker makes a list of possible keys and compiles a look up table in order to decrypt the ciphertext.

One of the values in the look up table cracks the encrypted message. It is another class of dictionary attack.

### K. *Denial of service*

In cloud computing, hacker attack on the server by sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly. Counter measure for this attack is to reduce the privileges of the user that connected to a server. This will help to reduce the DOS attack.

### L. *Side Channel Attack*

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms. Evaluating a cryptographic system's resilience to side-channel attacks is therefore important for secure system design.

### M. *Network Sniffing*

When the unencrypted data is send on the cloud through the network then the hacker can sniff the passwords from the data on transit.

### N. *Port Scanning*

There may be some issues regarding port scanning that could be used by an attacker as Port 80(HTTP) is always open that is used for providing the web services to the user. Other ports such as 21(FTP) etc are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly. Counter measure for this attack is that firewall is used to secure the data from port attacks.

### O. *SQL Injection Attack*

SQL injection attacks are the attacks where a hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it.

### P. *Cross Site Scripting*

It is a type of attack in which user enters the correct URL of a website and hacker on the other site redirects the user to its own website and gain access to its credentials.

The aforementioned attacks weaken the security of encrypted data stored on cloud. Eventually, these attacks are the major barriers for a broader adoption of data outsourcing to cloud. Hence mitigating the threats, attacks and vulnerabilities is the vital factor to be considered in cloud storage in order to achieve data confidentiality.

## V. SECURITY ISSUES AND SOLUTIONS

Security risks are the biggest concerns when users want to apply outsourcing computing in cloud storage. There are various security problems involved in the cloud computing. They are data security, network security, data locality, data integrity, data segregation, data access, authentication and authorization, availability, backup, identity management and sign-on process, etc [27]. Especially, among these security issues, confidentiality is the most important parameter to secure the data in cloud. Confidentiality for cloud storage ensures that the cloud providers do not learn any information about the users' data [28].

The main concern around data storage is the protection of information from unauthorized access [29]. In several usage scenarios, the risk of data being disclosed, lost, corrupted or stolen is unacceptable [30]. Until data are stored on resources owned, controlled and maintained by the data owners, the possibility of unauthorized access is reduced by any physical countermeasure or trust in authentication and authorization mechanism [31]. Things radically change when moving from resources fully controlled by the data owner to resources administrated by third party entity like public clouds. Resources that remain outside the users' domain are not owned and controlled by the users. The risk that someone (an employee of the CSP) can access and disclose or corrupt data is considerable. This risk is usually known as insider abuse or insider threat or insider attack [32]. Confidentiality of data in the cloud is to be ensured the data protection from insider attack. This is the major risk that, presently, is preventing the large adoption of cloud based solutions by the enterprises. Before companies move their data to the cloud, benefitting from the cloud storage advantages, all issues deriving from storing data on un-owned and un-trusted resources must be addressed by the legal security frameworks.

To protect data in cloud storage, currently a standard approach is to apply cryptographic techniques into users' data [33]. Cryptographic techniques have been widely used in the area of cloud storage, and it plays an important role in the data security. In the cloud environment, security attacks are protected by using cryptographic techniques. In cryptography, the message which is to be kept secret is called plaintext [16]. The process of hiding its content is called encryption and the encrypted message is called ciphertext. The process of receiving the content of plaintext from the ciphertext is called decryption. A cryptographic algorithm or cipher is a mathematical function used in the encryption and decryption processes. A modern cryptographic algorithm always includes a key. Cryptographic algorithms, plaintexts, ciphertexts, and keys are collectively called cryptosystem. It works with combination of keys and algorithm to encrypt the plaintext and to decrypt the ciphertext [34].

The core concept of securing the data in cloud storage is using encryption techniques. The data are encrypted in the trusted environment before sending it to untrusted cloud storage providers [35]. Theoretically both symmetric and asymmetric algorithms could be used, but, since the asymmetric are much slower than the symmetric, symmetric algorithms are preferred for performance reasons in cloud environment. The usage of encryption is a technique to secure data guarantees and the security of data in the cloud storage [36].

## VI. CONCLUSION

Cloud provides many benefits to its users but it has some security problems due its advanced nature of cloud. Data outsourcing is widely popular due to the computing power of cloud. At the same time, security of outsourced data is a question from all the cloud users. This paper talks about the different attacks on data in cloud. This attacks may initiated by both insiders and outsiders. Outsiders' attacks may protect by authentication mechanism but insiders' attacks are very difficult to identify and also very tough to protect. Confidentiality is compromised due the insiders' attacks on the data stored in the cloud. It is most important to ensure the confidentiality of data in the cloud and also need to develop new technique or mechanism to address the insiders' attacks in the cloud. Once these issues are addressed then cloud users and providers will get more benefits from the cloud.

## REFERENCES

[1] Dr. 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.

[2] Fatima Trindade Neves, Fernando Cruz Marta, Ana Maria Ramalho Correia and Miguel de Castro Neto, "The Adoption of Cloud Computing by SMEs: Identifying and Coping with External Factors", Proceedings of International Conference of the Portuguese Association of Information Systems - The Information Management in the age of Cloud Computing, 2011, pp. 1-11.

[3] John, H., L.M. Kaufman and Bruce, P., "Data Security in the World of Cloud Computing", IEEE Journal of Security & Privacy, Volume 7, Issue 4, 2009, pp 61-64.

[4] Dr. L. Arockiam, S. Monikandan, "Security Framework to Ensure the Confidentiality of Outsourced Data in Public Cloud Storage", International Journal of Current Engineering and Technology, Vol.4, No.3, E-ISSN 2277 – 4106, P-ISSN 2347 - 5161, June 2014, pp. 1265-1270. (IF-2.552)

[5] Dr. L. Arockiam, S. Monikandan, "AROMO Security Framework to Enhance Security of Data in Public Cloud", International Journal of Applied Engineering Research, Print ISSN 0973-4562, Online ISSN 1087-1090, Volume 10, Number 9, (Special Issue), 2015, pp. 6740-6746.

[6] Yau SS, An HG., "Confidentiality Protection in Cloud Computing Systems", International Journal of Software Informatics, Volume 4, Issue 4, 2010, pp. 351-365.

[7] Raman Chawla and Kirti Nagpal, "Data Security Issues & Requirements in Cloud Computing", International Journal of Computing Science and Communication Technologies, Volume 5, Issue 2, 2013, pp. 883-886.

[8] Kaur A, Manisha Bhardwaj, "Hybrid Encryption for Cloud Database Security", International Journal of Engineering Science & Advanced Technology, Volume 2, Issue 3, 2012, pp. 737-741.

[9] Shucheng Yu, Wenjing Lou, and Kui Ren, "Data Security in Cloud Computing", Handbook on Securing Cyber-Physical Critical Infrastructure, Chapter 15, Elsevier, Morgan Kaufmann Publisher, 2012, pp. 389-410.

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

[11] Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo, "Secure Data Sharing in the Cloud", Security, Privacy and Trust in Cloud Systems, Chapter-1: Cloud Security, Springer-Verlag Berlin Heidelberg, 2014, pp. 45-72.

[12] Dimitrios Zissis and Dimitrios Lekkas, "Addressing Cloud Computing Security Issues", Journal of Future Generation Computer Systems, Elsevier Science, Volume 28, Issue 3, 2012, pp. 583-592.

[13] 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.

[14] Dr. L. Arockiam, S. Monikandan, Dr. P. D. Sheba K Malarchelvi, "Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage", International Journal of Computer Applications, Volume 88, Number 1, ISSN: 0975 – 8887, February 2014, pp. 17-21.

[15] Bleikertz S, Sven Bugiel, Hugo Ideler, Stefan Nurnberger and Ahmad-Reza Sadeghi, "Client-Controlled Cryptography-as-a-Service in the Cloud", Proceedings of International Conference on Applied Cryptography and Network Security, Springer-Verlag Berlin, Heidelberg, 2013, pp. 19-36.

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

[17] Joe Ruether, Cryptography Primer, http://jrruethe.github.io/blog/2014/10/25/cryptography-primer/ , Oct 25th, 2014 , 2016 jan.

[18] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstore, "Handbook of Applied Cryptography", CRC Press Inc., 1997.

[19] Eman M. Mohamed, Hatem S. Abdelkader and Sherif El-Etriby, "Data Security Model for Cloud Computing", Proceedings of International Conference on Networks, 2013, pp. 66-74.

[20] Oktay U. and Sahingoz O.K., "Attack Types and Intrusion Detection Systems in Cloud Computing", Proceedings of International Conference Information Security & Cryptology, 2013, pp. 71-76.

[21] S. Vani mounika, Preetiparwekar, Survey on cloud data storage security techniques, Indian Journal of Research in Pharmacy and Biotechnology, Special Issue 1, 2014, pp. 95-98.

[22] Ajey Singh, Dr. Maneesh Shrivastava, Overview of Attacks on Cloud Computing, International Journal of Engineering and Innovative Technology, Volume 1, Issue 4, 2012, pp. 321-323.

[23] Adrian Duncan, Sadie Creese, Michael Goldsmith, Insider Attacks in Cloud Computing, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 857-862.

[24] D. M. Cappelli and R. F. Trzeciak, "Best practices for mitigating insider threat: Lessons learned from 250 cases," [Online]. July 2013, Available:http://www.cert.org/archive/pdf/RSA-CERTInsiderThreat. pdf.

[25] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, A survey of intrusion detection techniques in Cloud, Journal of Network and Computer Applications, Volume 36, Issue. 1, 2013, pp. 42–57.

[26] U. Oktay and O.K. Sahingoz, Attack Types and Intrusion Detection Systems in Cloud Computing, International Information Security & Cryptology Conference, 2013, pp. 71-76

[27] Subashini S and Kavitha V., "A Survey on Security Issues in Service Delivery Models of Cloud Computing", Elsevier Journal of Network and Computer Applications, Volume 34, Issue 1, 2011, pp. 1-11.

[28] Cyril Onwubiko, "Security Issues to Cloud Computing", Cloud Computing: Principles, Systems and Applications, Computer Communications and Networks, Springer-Verlag London, Chapter-16, 2010, pp. 271-288.

[29] Gonzalez N, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund and Makan Pourzandi, "A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing", Journal of Cloud Computing: Advances, Systems and Applications, Springer-Verlag, Volume 1, Issue 1, 2012, pp. 1-11.

[30] Isaac Agudo, David Nuñez, Gabriele Giammatteo, Panagiotis Rizomiliotis and Costas Lambrinoudakis, "Cryptography goes to the Cloud", Secure and Trust Computing, Data Management, and Applications, Springer Berlin Heidelberg, Volume 187, 2011, pp. 190-197.

[31] Jingwei Huang and David M Nicol, "Trust Mechanisms for Cloud Computing", Journal of Cloud Computing: Advances, Systems and Applications, Springer-Verlag, Volume 2, Issue 1, 2013, pp. 1-14.

[32] Minh-Duong Nguyen, Ngoc-Tu Chau, Seungwook Jung, and Souhwan Jung, "A Demonstration of Malicious Insider Attacks inside Cloud IaaS Vendor", International Journal of Information and Education Technology, Volume 4, Issue 6, 2014, pp. 483-486.

[33] Peng Yong, Zhao Wei, Xie Feng, Dai Zhong-Hua, Gao Yang and Chen Dong-Qing, "Secure Cloud Storage Based on Cryptographic Techniques", Journal of China Universities of Posts and Telecommunications, Elsevier, Supplementary 2, 2012, pp. 182-189.

[34] Dr. L. Arockiam , S. Monikandan, "AROcrypt: A Confidentiality Technique for Securing Enterprise's Data in Cloud", International

Journal of Engineering and Technology, ISSN: 0975-4024, Volume 7, Issue 1, February-March 2015, pp. 245-253.

[35] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", Proceedings of IEEE International Conference on Computer Science and Electronics Engineering, 2012, pp. 647-651.

[36] S. Monikandan and Dr. L. Arockiam, "Confidentiality Technique to Enhance Security of Data in Public Cloud Storage Using Data Obfuscation", Indian Journal of Science Technology, ISSN (Print) : 0974-6846, ISSN (Online) : 0974-5645, Volume 8, Issue 24, September 2015, pp. 1-10.

AUTHOR PROFILE

**Dr. S. S. Manikandasaran** is working as Dean in Christhuraj Institute of Computer Application, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India. He has 8 years of experience in teaching and 5 years of experience in research. He is completed his MCA and M.Tech in Bharathidasan University, Tiruchirappalli in 2007 and 2009 respectively and also completed his Ph.D degree in Manonmaniam Sundaranar University, Tirunelveli in 2015. He has attended many International and National Conferences, Seminars and Workshops. He has published more than 30 research articles in the International / National Conferences and Journals. He has delivered more than 15 lecturers in various National Level seminars, symposium and conferences. His research interest is Cloud Computing, Network Security, Cloud Security, IoT and Web Technology.