International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34658-34663

Content Based Security Policy in Cloud Environment

Rama Krishnan

Research Scholar Dept. of Computer Science & Engineering,
AMIET University ECR, Kanathur, Chennai, India
ramakrishnanr@gmail.com

DR. V. Mathivanan

Research Supervisor Dept. of Computer Science & Engineering
AMIET University ECR, Kanathur Chennai, India
vmathivanan@yahoo.com

Abstract
Cloud computing is highly demanded area in the terms of application compatibility, best performance, high availability with low cost compares that other system. In cloud computing, the data will be stored in database and this activity is monitored by service providers. But till now many corporate sector have to fear adopt cloud computing technology due to lack of privacy awareness. In this paper, a Proposed Content Based Policy (CBP) technique is highly robust and efficient for secure /credential metric data. Existing method either offer query efficiency at no security, or they offer complete content security. In This paper proposes a CBP approach which enhances our key complexities issues, and provide tight security for content with low communication cost. Here, Data, holder can upload volume of content in cloud environment with content name and descriptions. Proposed techniques store relative content to cloud server with respective private set of content attribute. Finally, it demonstrates their efficiency and security on sensitive and real content. Experimental results shows that proposed method have tight security with best efficiency compare than existing approaches.

Keyword- Cloud Server, Content Based policy, Communication Cost, Encryption Time and Decryption Time.

1. INTRODUCTION

Cloud computing is highly demanded area in the terms of application compatibility, best performance, high availability with low cost compares that other system. In cloud computing, the data will be stored in database and this activity is monitored by service providers. But till now many corporate sector have to fear adopt cloud computing technology due to lack of privacy awareness [19]. Now Day Cloud computing is emerging field because of its performance, high availability, low cost and many application systems. In cloud computing, the data will be stored in cloud storage which is assigned by cloud service providers. Because, it noticed that a lot of vulnerability attack and content misuse is happening in cloud. Content sharing is never easy in advanced cloud, and an accurate evaluation on the shared content provides an array of profit to as well society as individuals. In content sharing there are a lot of participants willing to contribute content in cloud but due to lack of issues such content sharing, content integrity and privacy of data holder. They have hesitation to contribute the content with cloud.

In existing, data holder can contribute his encrypted files to un-trusted proxy cloud servers. Proxy clouds servers can perform some operation on outsource content without knowledge of original content files. However, this approach is unable to employ extensively. The main issues raises in that user are especially concerned on the privacy, content integrity and query of the outsourced files in cloud which very complicated process to data holder. This entire system is managed by un-trusted third party. Next, it considers another issues is content misuse attacks are amplified if the attacker is a malicious insider. Here a lot of transparency into Cloud service provider's accessibility, and authorization only to controls exacerbates this kind threat attack [17]. In some security concern, Watermarks can be very useful in some cases. However, if user wants modify and update the original content then unable maintain privacy of content.

To overcome issues, this paper proposes novel and effective approach to securing the cloud using decoy information technology that we have come to call Content Based Policy Approach. Proposed CBP approach which enhances key complexities issues, and provide tight security for content with low communication cost. Here, Data, holder can upload large volume of content in cloud environment with content name and descriptions [18]. There is no need to enter key to decrypt the content. The CBP protocol, which has sub-tree method in the proposed approach, is secure in terms of the key complexities reductions. During content transfer, any misleading is going to happen in either server side or external attack then proposed approach will update the key of content and send updated key to user automatically. It also send alert message to data holder as well trusted user. Paper contributions of work follow as:

1. Novel CBP approach enhances key complexities issues, and provides tight security to content with low communication cost.
2. Proposed approach encrypt the content of attributed with low complexities and effective way

3. Proposed scheme provides tight security for with the help cryptographic techniques. Here, third party or trusted authority is not requires.
4. During content transmission, any misbehave is going to happen by external user or cloud server the proposed approach will update key of content automatically and send alert to user and data holder.
5. Experimental results displays that the proposed Content Based Policy approach performs well on content security concern.

The rest of paper follow as: In section 2, we mentioned related works which are close to proposed mechanism. In section 3 introduces the proposed system model with proposed techniques elaboration. In Section 4, explain about implemented result and discussion. In section 5, concluded the overall work with future enhancement.

2. RELATED WORK

In this paper [1] Author enhanced the security of ID-based ring signature by providing forward security: If a secret key of any data holder has been disclosed, then also all previous generated signatures that include this data holder still valid. This property is especially important to any large volume of content sharing system, as it very difficult to communicate all data owners to re-authenticate their content even if a secret key of one single user has been disclosed. In this paper [2] Author examined assigning anonymous IDs with respect to trade-offs between communication and computational requirements. Their techniques are built on top of a secure sum data mining operation using Newton's identities and Sturm's theorem which enhance scalability of application. In this paper [3] Author, implemented a cloud-based storage method that allows the data holder to benefit from other facilities which is offered by the CSP. Their proposed scheme contains following features: (i) it allows the owner to outsource credential data to a CSP; (ii) it ensures that authorized users receive the latest version of the outsourced data, (iii) it capable to establish indirect mutual trust between data owner and CSP, and (iv) it allows the owner to allow or revoke access to the outsourced content. In this paper [4] Author developed a novel privacy-preserving mechanism which supports public auditing on contributing content stored in the cloud server. In particular, they exploit ring signatures to compute verification metadata necessary to audit the contributed data. In this paper [5] Author, presented a secure multi-owner data sharing scheme, called as Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can contribute the data with others users. In this paper [6] Author described new public-key cryptosystems that produce constant-size cipher-texts such that efficient delegations of decryption rights for any set of cipher texts which are possible. The novelty of given approach was aggregate any set of secret keys and make them as compact single key. In this paper [7] author developed a simple content privacy model where data is encrypted using by Advanced Encryption Standard (AES) before it is storing in the cloud, thus ensure content confidentiality and privacy. In this paper [8] author improved privacy technique that contains five approach namely as Resilient role-based access control mechanism, Partial homomorphic cryptography, metadata generation and sound steganography. This approach is focuses on, efficiency third-party auditing service, Data backup and recovery process against client's data attackers in cloud.

In this paper [9] author implemented Multifactor Authentication System which authenticates the customer in multiple levels using multidimensional and multilevel password generation technique. In this paper [10] author developed Fully Homomorphic Encryption (FHE) scheme based on reporting. Fully Homomorphic Encryption is a good basis to enhance the security measure of un-trusted systems or applications that stores and manipulates sensitive data. In this paper [11] author presented effective and flexible scheme with two different algorithms. These features which make cloud computing so flexible with the fact that services are accessible anywhere any time lead to several potential risks. In this paper[12] author implemented multilayered security approach means the security at different levels of different cloud layers to secure the data stored at cloud data centers based on dynamic hybrid key then performance of implemented algorithm is evaluated at last based on execution time, security improvement percentage and delay. In this paper [13], author developed a more confidential technique named AROcrypt to ensure the security of data stored in the cloud storage server. It also explains Security as a Service (SEaaS) in cloud environment. It uses the ASCII values to process plain text into cipher text. In this paper [14], author focused on the user authentication and data security over the Broker Cloud Computing Paradigm by exploiting the cryptographic techniques as Selective Encryption using AES. In this paper [15] author developed Token Based Data Security Algorithm. The auto-generated token based certificate activation method with SSL (Secure Socket Layer) gives an appropriate collaboration between Data's holder and cloud service provider, so that user can assure about content transfer by utilizing various cloud applications and services. In this paper [16] author analyzed different kind of security with different kinds of risk. The security issues also one of the major drawbacks in cloud computing because over content located on the centralized location due to this reliability and availability of data not achieve.

However, proposed work neither only focus on encryption and decryption process nor key complexities issues. This paper noticed that a lot of work is there behalf of cloud security and most of author provide privacy approach with help of third party auditor and trusted authority. Here, there is no proper security mechanism with low complexities to data holder's content or data. Hence, it's clear that proposed method is different to existing techniques.

3. PROPOSED SYSTEM MODEL

In this phase, represents about proposed system model, features and implemented techniques. Here, model implemented procedure is classified in the phase namely: data holder trusted User, algorithm. Proposed model represent working function in figure 1 where it display working model. In phase, proposed approach represent content transmission

model from data holder to trusted user in cloud environment. This method also prevents external or internal content attack.

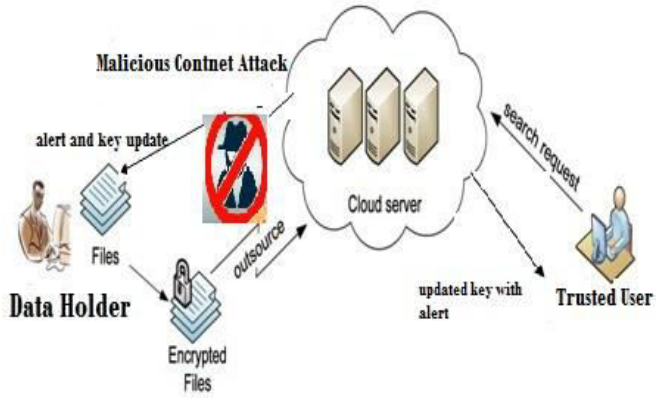

Figure-01 Proposed System Architecture.

3.1 Data Holder

In this module, the Data holder wishes to upload or publish his data to the cloud server so that trusted users can execute queries on those data. On the other hand, the data holder trusts only the trusted users and nobody others. Data holder contains set of original attributes, and a key which can be used for data transformation. First, the data holder process a transformation function (with a key) to convert attributes into a set of transformed objects, and uploads the to the cloud server.

3.2 Trusted User

In this module, trusted users required authentication to access the content details. Trusted user's account should be available in cloud. If it is not then they should register first. Hence, trusted can enter authenticated key and receive the content.

3.3 Content Based Policy Algorithm

Content Based Policy Algorithm is a public key crypto system which is primitive for one-to-many communications. In CBP, data are associated with content and attributes for each of which a public key component is described. The encryptor has set of content with attributes to the message by encrypting it with the corresponding user public key details. Each trusted user is assigned an access structure which is usually describes as an access mechanism all over content attributes. Trusted user's secret key is defined to reflect the access structure so that the trusted user is able to decrypt content if and only if the content attributes satisfy his access mechanism [20. In CBP method data holder will fix the authentication policy based content sharing (which kinds of content for whom). The scheme can be constructed with the help of content details with descriptions. In this scheme encrypted data can is confidential even though server is un-trusted. During content transfer, any misleading is going to happen in either cloud server parts or external attack then proposed approach will update the key of content and send updated key to user automatically. It also send alert message to data holder as well trusted user Proposed scheme is simple, efficient and secure against collusion attacks. CBP scheme consists of the following four techniques.

- Setup: This algorithm takes input parameter k and revert the public key PK as well as a system master secret key MSK. PK is utilized by message content senders for encryption. MSK is used to generate data holder's secret keys and it is known by authorized user only.
- *Encryption:* This algorithm accepts a message content M, the public key PK, and a set of attributes γ as input. It performs the ciphertext CT.
- *Key Generation:* This algorithm receive as input an access mechanism A, and the master secret key MSK. It provides a content secret key SK which enables trusted user to decrypt a encrypted message content under a set of attributes γ if and only if γ matches A.
- *Decryption:* It accept as input the data holder's secret key SK for access mechanism A and the cipher text CT, which was encrypted under the content attribute set γ. This approach performs the message content M if and only if the set of attribute γ assures the data holder's access mechanism A.

ContentBupdate(I, MSK)
// assume current version of attribute i is k ¡ 1;

randomly pick $a'_i \xleftarrow{R} Z_p$;
Compute $A'_i \leftarrow g\, t'_i$

and $\gamma\, k_i \leftrightarrow i' \longleftarrow \frac{a'_i}{a_i}$;

Output a'_i, $A'_{i,\ and}$ $\gamma\, k_i \leftrightarrow i'$.
ContentBaseFileupdate(i, CT_i,AHL_i)
if i has the latest version, exit;
Search AHL_i and locate the old version of // assume the latest version of i in MSK is $a_i(n)$.
$\gamma\, k_i \leftrightarrow i(n) \longleftarrow \gamma\, k_i \leftrightarrow i'.\ \gamma\, k_i' \leftrightarrow i''.....\ \gamma\, k_i(n\text{-}1) \leftrightarrow$

$i(n) = \frac{a_i(n)}{a_i}$;

Compute $CT_i^{(n)} \longleftarrow (CT_i)\ \gamma\, k_i \leftrightarrow i(n) = g^{a}{}_i(n)s.$

Output $CT_i^{(n)}$.

Figure 2 Pseudo code for content based policy algorithm.

4. RESULT AND DISCUSSION

4.1 Experimental Setup

In order to compares proposed mechanism with existing algorithm. This paper is used open source cloud namely as Everdata cloud server. The experiment is conducted on a laptop with Intel Dual Core processor (1.836 Hz), 2GB memory, and Window 7 Ultimate system. Here, this method implemented in JAVA using NetBeans 8.0 with Jelastic Cloud & JMeter plug-in and MYSQL 5.5 Database.

4.1.1 Data

For proposed method evaluation, the approach selects three different dataset with size of content namely Document (20KB), Images (800KB), and Video (2MB) which are

mentioned. For retrieving the query from centralized server used JAVA based Secure Storage & Retrieval system.

4.2 Result

In this phase, CBP proposed scheme represent mathematical model to enhance security for cloud storage. In this scheme, security model works with data holder and trusted client. Even though cloud storage is not trusted then also data holder content will be in safe during content uploading and content retrieval. Its display following model separately such as communication cost, Encryption Time and Decryption Time.

4.2.1 Encryption Time(ET)

In this section, proposed method represent mathematical model in equation (1).This algorithm accept content or message M, the public key PK, with set of attribute I as input. It performs the cipher-text CT with the following way:

$$CT = \left(I, CT\{\mathrm{CT}_i\} i \varepsilon \mathrm{I}\right) \qquad (1)$$

Where

˜CT = MY^s, $CT_i = A^s_i$, and s is randomly chosen from Zp.

4.2.2 Decryption Time(DT)

In this section, proposed method represent mathematical model in equation (2). This method receives as input as a cipher-text CT encrypted under the attribute set I. the user's secret key SK for access tree A, and the public key PK. It performs decryption in following manner:

$$CT(\mathrm{CTi}, \mathrm{ski}) = CT(g, g)^{\mathrm{pi(O)s}} \qquad (2)$$

Where CT= Chiper-text, ski= user secret key component for attribute I for leaf nodes. Then, it integrates pairing results in sequential manner using the polynomial interpolation method. Finally, it improve the blind factor Y^s = CT (g, g)^{ys} and display the message M if and only if I satisfies A.

4.2.3 Communication Cost (CC)

In this section, proposed method represent mathematical model in equation (3).Here, it evaluate the communication cost (%) based on length of content and sized index of attribute content. It is generally consider average performance encryption and decryption of particular set content. The communication cost is c(|q|+|n|) bits.

$$MC = c(|q| + |n|) \qquad (3)$$

Where |q| is the length of an element of Zp and |n|is the length of an index.

Table-01 communication cost (%), encryption time (in sec) and decryption time (sec) for document, images and video dataset. The approach is analyzed in terms of communication cost (%), encryption time (in sec) and decryption time (sec) and display their average values for respective parameter with dataset.

TABLE 1 Communication Cost (CC) Encryption Time (ET) & Decryption Time (DT) for Document, Image and Video Database.

Learning Algorithms	Document			Images			Video		
	CC	ET	DT	CC	ET	DT	CC	ET	DT
DES	68.4	1.27	0.78	46.8	1.61	2.67	48.8	2.93	3.19
TRIPLE DES	63.7	1.47	0.83	50.3	1.48	1.99	59.3	2.36	1.95
BLOWFISH	90.8	0.12	0.15	82.9	0.67	0.82	80.9	0.81	0.89
RC6	74	0.69	0.68	49.3	1.59	1.72	63.25	2.16	2.46
RSA	58.54	1.63	2.32	29	2.76	3.15	39.9	3.45	3.99
ABE	97	0.21	0.35	96	0.97	0.16	95	0.25	0.48
CBP	100	0.09	0.14	99.8	0.70	0.12	99	0.19	0.22

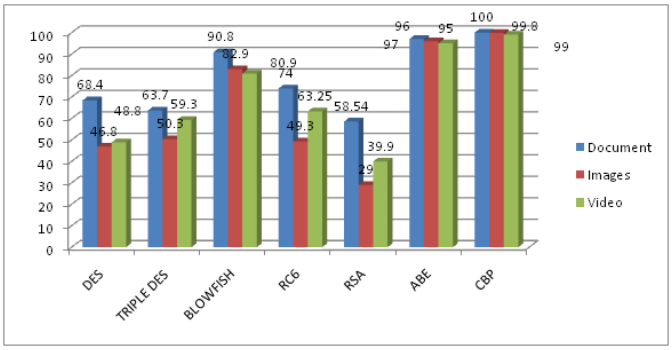

Figure 3 Communication cost (%) for document, images and video database

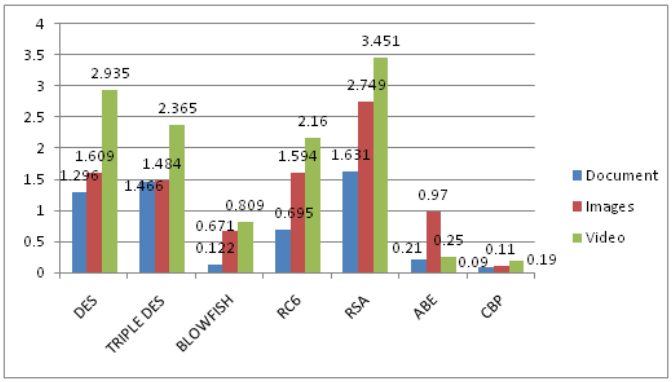

Figure 4 Encryption time (sec) for document, images and video database.

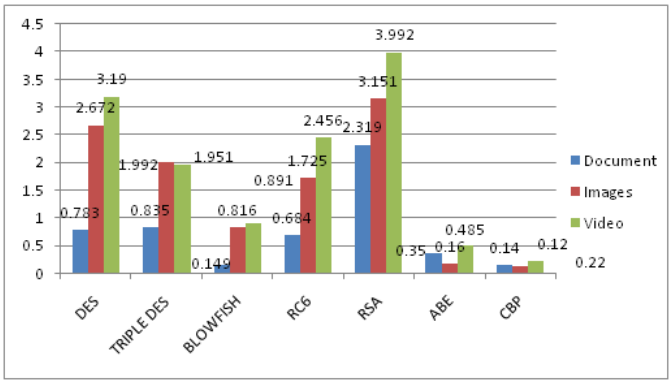

Figure 5 Decryption time for document, images and video database.

According to proposed Content Based Policy protocol evaluation result in figure 03, 04 and 05 for document, images and video dataset. Content Based Policy protocol is the best approach. In terms of communication cost, encryption time and decryption time CBP display that it always yields the best performance in both all graphical result. In terms of communication cost, CBP prove as best techniques. In terms of all evaluated factor with respective database, ABE (Attribute Based Encryption) is closest approach to proposed method. However, ABE result is too far compare than proposed approach. Therefore, we claim that CBP is best approach for all dataset.

5. CONCLUSION

In this paper, a Proposed Content Based Policy (CBP) technique is highly robust and efficient for secure /credential metric data. Existing method either offer query efficiency at no security, or they offer complete content security. In This paper proposes a CBP approach which enhances key complexities issues, and provide tight security for content with low communication cost. Here, Data, holder can upload large volume of content in cloud environment with content name and descriptions. Here trusted user can directly retrieve data with content. Proposed method also consider misbehave or external attack with data holder content. In this case, proposed approach updates key of content automatically and send alert to user and data holder. Proposed techniques store relative content to cloud server with respective private set of content attribute. Finally, it demonstrates their efficiency and security on sensitive and real content. Experimental results shows that proposed method tight security with best efficiency compare than existing approaches.

In future paper can be modified in to various features as data holder content transfer from one cloud server to another cloud server with privacy. In this paper can modify as terms of content transmission privacy policy for various types of database.

REFERENCES

1. Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou," Cost-Effective Authentic and Anonymous Data Sharing with Forward Security" IEEE Transactions on Computers, Volume:64 , Issue: 4 , 03 April 2014, pages 971 – 983.
2. Larry A. Dunning, and Ray Kresma," Privacy Preserving Data Sharing With Anonymous ID Assignment", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 2, February 2013, Pages 402 - 413 .
3. Ayad Barsoum and Anwar Hasan," Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems", IEEE Transactions on Parallel and Distributed Systems, Volume: 24, Issue: 12. December 2013, pages 2375 – 2385.
4. Boyang Wang, Baochun Li, and Hui Li," Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE Transactions on Cloud Computing, Vol. 2, No. 1, January-March 2014, pages 43-56.
5. Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan," Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions on Parallel And Distributed Systems, Vol. 24, No. 6, June 2013, pages 1182 – 1191.
6. Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng," Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014, pages 468 - 477.
7. Sanjoli Singla & Jasmeet Singh," Implementing Cloud Data Security by Encryption using Rijndael Algorithm", Global Journal of Computer Science and Technology, Cloud and Distributed, Volume 13 Issue 4, 2013, pages 18-22.
8. Manpreet Kaur, and Rajbir Singh "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", *International Journal of Computer Applications (0975 – 8887) Volume 70– No.18, May 2013,* pages 16-21.
9. Abha Sachdev and Mohit Bhansali," Enhancing Cloud Computing Security using AES Algorithm", *International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013*, pages 19-23.
10. Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Suriayati Chuprat and Jamalul-lail and Ab Manan" Design And Implementation of A Privacy Preserved Off-Premises Cloud Storage", Journal of Computer Science, Volume 10 No 02, 2014, pages 210-223.
11. Sumathi M, Sharvani G.S, Dinesha H A, "Implementation of Multifactor Authentication System for Accessing Cloud Services", International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013, pages 1-8.
12. S.Hemalatha1, and Dr. R.Manickachezian, "Performance of Ring Based Fully Homomorphic Encryption for securing data in Cloud Computing", International *Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 11, November 2014*, pages 8496- 8500
13. Sonal Guleria1, and Dr. Sonia Vatta,"To Enhance Multimedia Security in Cloud Computing Environment Using Crossbreed Algorithm" International Journal of Application or Innovation in Engineering & Management (IJATEM), Volume 2, Issue 6, June 2013, pages 562-568
14. Jashanpreet Pal Kaur1, and Rajbhupinder Kaur," Multilayered Security Approach for Cloud Data Centers using Hash Functions", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 3 Issue 11, November 2014, pages 2394- 2397.

15. S. Monikandan, and Dr. L. Arockiam," 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, pages 1053-1058.
16. Amanpreet Kaur, and Gaurav Raj," Secure Broker Cloud Computing Paradigm Using AES And Selective AES Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 3, March 2013, pages 79-83.
17. Rimmy Chuchra & R.K Seth, "Modeling Implementation of TBDSA-Token Based Data Security Algorithm in Cloud Computing ", International Journal of Computer Applications (0975 – 8887) Volume 114 – No. 7, March 2015, pages 12-17.
18. Shital P. Adkine," Security Analysis of Cloud Computing", International Journal of Computer Science and Informatics ISSN (PRINT): 2231 –5292, Vol-1, Issue-4, 2012, pages 107-111.
19. Moligi Sangeetha, "Simulation of Secure Data Sharing Scheme for Dynamic Groups in Cloud ", International Journal of Computer Engineering and Applications, Volume VII, Issue II, August 2014, pages 69-76.
20. Hamdan M. Al-Sabri, and Saleh M. Al-Saleem," Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013, pages 259-266.