International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 02 | Feb 2021 www.irjet.net p-ISSN: 2395-0072

A SCALABLE CRYPTOGRAPHY POLICIES FOR SECURE DATA STORAGE AND ACCESS THE DATA IN CLOUD ENVIRONMENT

Karthick Raj V K[1], Rajarajeswari P[2]

[1]*Student, Dept of Computer Science and Engineering, Kingston Engineering College, Tamil Nadu, India*
[2]*Associate Professor, Dept of Computer Science and Engineering, Kingston Engineering College, Tamil Nadu, India*

Abstract – *Cloud computing security policies are applied for storing the data in cloud. It aims to control unauthorized users from data accessing and avoid destructions.. When one data is taken to the cloud, many security concerns arise and ensure data security remains questionable. Cloud architecture threatens the safety of traditional technologies. Therefore, users of cloud services must know the dangers of loading data in this new environment. Therefore, this paper reviews different aspects of cryptography that pose a threat to cloud computing. This paper proposes ways to secure data in the cloud using strong cryptographic the AES algorithm can be used to store the data in the cloud and produce secure and scalable data storage elements. The efficiency and security of our proposed cryptosystem have been analyzed and reported.*

1. INTRODUCTION

In our day-to-day world, Cloud computing plays a vital role by providing online access for data. Consumes utilise cloud computing for other purposes as well beyond storage, application hosting and database. Service providers offer various service models such as IAAS, PAAS and SAAS with different payment options available for users. Examples include Microsoft Azure, Google and AWS services. [2] [3][4]. They provide protection, data security, scalability, and privacy for the end users data present in cloud. However, Customers cannot trust service providers entirely because of various security concerns. In order to overcome the security concerns, we introduce encryption methodologies and Cryptographic algorithms. Cryptographic algorithms are critical while transferring data over Internet due to security purposes.

Cryptographic algorithm has different functions, and they are listed as follows:

Confidentiality: Due to daily lives attacks, the data should be read from the desired recipient, the recipient or user.

Authentication: You have to prove your identity to access the legitimate data.

Integrity: Whatever data the end user gets after the process of transmission in the non-reliable environment must be the same as the originals, should not be modified or altered.

Non-repudiation: This feature indicates that only one legitimate sender must send the information to the recipient.

Key-Exchange: Key Exchange is one of the vital and critical feature, as the exchange of Crypto keys play a decisive part when encrypting and decrypting the data.

Different variety of cryptographic algorithms are involved in the data transmission process as a function of the keys used for decrypting and decrypting the data should be different, namely,

a. **Secret Key Cryptography:** This cipher uses a single key to encrypt and decrypt the data. This cipher is mainly used for privacy and confidentiality. Secret key cryptography is otherwise known as Symmetrical key cryptography due to the fact that it utilises same keys in the process.

b. **Public Key Cryptography:** Public key cryptography utilises two keys during the encryption process. These keys are used for authentication, rejection and data exchange through Encryption and Decryption processes. Hence it is also referred as asymmetric key cryptography. During the process it converts a plain text to ciphertext using various cryptographic techniques. Public keys (known to others) and private keys(known only to owner) are used here. In this system, user encrypts message using receiver's public key. But this encrypted message can only be decrypted by the help of receiver's private key. We can achieve robust authentication using this methodology.

1.1 RELATED WORKS:

Many researchers have been done work on security concepts. They have done work on Cryptography polices and algorithms. These schemes is lightweight and loose coupling to concrete secure query schemes and can be very easily equipped into any source query scheme for cloud computing. Specially, once the cloud server knows that the query results verification scheme is provided in the secure search system, this information may leak query user's privacy and expose some useful contents about data files. Cloud computing brings all resources together and monitors them naturally

through planning. Recorded information and existing information are integrated to make the collected data more accurate. In addition to these lines, cloud computing offers users smarter assistance in purchasing a server or solution, but you can purchase computing resources on the Internet as needed. However, cloud computing is a promising innovation for remote service delivery. However, there are numerous security problems with cloud computing. Rajeswari etal focused on cloud computing concepts[22,23].

2. EXISTING SYSTEM:

In cloud computing, we see promising innovations for remote service. As you can, security issues are numerous with cloud computing. For example, the Amazon organization has benefits in February 2010, which S3 (Simple Storage Service) has been broken down for, which made individuals re-consider the security of cloud computing. Includes Amazon. Set your site to the Amazon's server farm to save a major device company. [8] Therefore, the management of Cloud Computing is not stable and authentic. Safety is still an important concern in distributed computing, and one of the reasons why cloud computing still does not do as an important field of research for system protection has developed the data access control in the last thirty years, and various techniques have been developed to develop effectively implementing a differentiated access control, the flexibility in determining different access rights for individuals allows traditional access control architectures normally assume that the data owner and the servers store the data in the same trusted domain in which the servers are fully entrusted as an omniscient reference monitor the definition and enforcement of access control policies is responsible. Semantic search on encrypted data is an important task to retrieve information safely in the public cloud.

3. PROPOSED SYSTEM:

Information security and safety security are the essential goals of cloud users. City service providers should not reveal or disclose private user information, nor should they disable user information and click protection. It can be a mysterious arrangement marked by Two associations about their customers and their profit techniques that should not be clearly completed, information protection and security contains the life cycle of creation, storage, use, exchange, update and the destruction of information. [19] AlZain. The critical issue of the current situation is Cloud Computing Security and to address it, it is also necessary to build cloud computing security models, breakdown the key progress used as part of these models.

4. PROPOSED ALGORITHM:

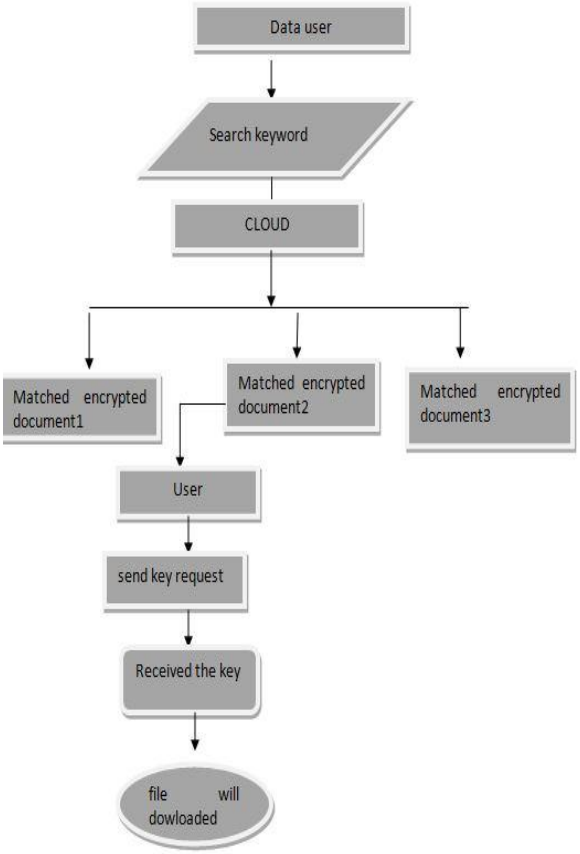
Here we are using the Advanced Encryption Standard (AES) algorithm is an iterative encryption instead of Feistel. It is based on a 'replacement-permutation network, it is made up of a series of related operations, some of which involve replacing tickets With specific outputs (substitutions) and others involve the mix of bits (permutations).

Interestingly, AES performs all its calculations in bytes instead of bits. Therefore, AES treats the 128 bits of a plain text block as 16 bytes. These 16 bytes are organized in four columns and four rows to be processed as an array. [12] Scalable secure file sharing on untrusted storage.

AES consists of 128-bit keys with 10 round, 192 bits with 12 rounds and 14 rounds for 256-bit keys. One of these rounds uses a different 128-bit round key, which is calculated from the original AES KEY

5. ADVANTAGES of AES:

The symmetric key encrypts the outsources data using key. If you have access to the data means that the key is used by the owner of the Data. Cloud administrator will generating the Indexed data set in the cloud using RLP Algorithm.



6.MODULES:

DATA OWNER UPLOADING DATA:

Data owner will be uploading file into the cloud using some key for encrypting the particular text document. The data owner can upload and download the file.

KEY GENERATION AND ENCRYPTION :

Data owner outsourcing the data to the cloud while uploading the data it will generating a symmetric key for encrypting the file then it will be placed in the cloud in encrypted format.

CLOUD ADMIN GENERATING INDEX:

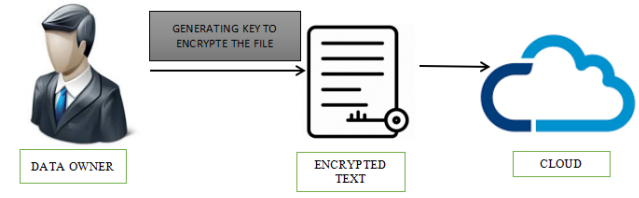
The cloud admin will maintaining every thing in the cloud, then they generating index for data which is presented in the cloud. Semantic Search Engine for Logical searching using Word Embedding and Transportation finally Producing Result with RLP Algorithm from the Indexed data set in the cloud.

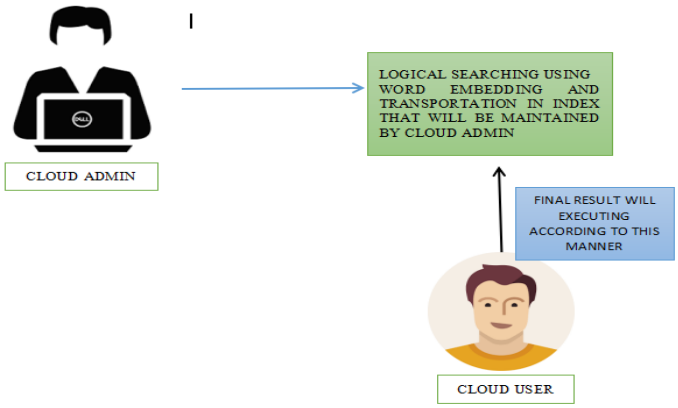
DATA USER DOWNLOADING USING KEY:

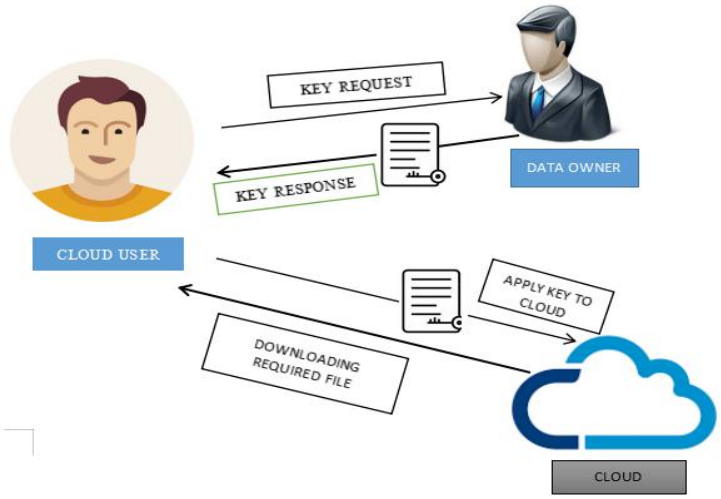
The data user downloading files before that they need to request the key from the data owner after that key will be apply in the cloud finally they can download required file.

DATA OWNER AND USER ACCESS DATASET:

Using symmetric key the user and data owner can access the files from the cloud. [20]

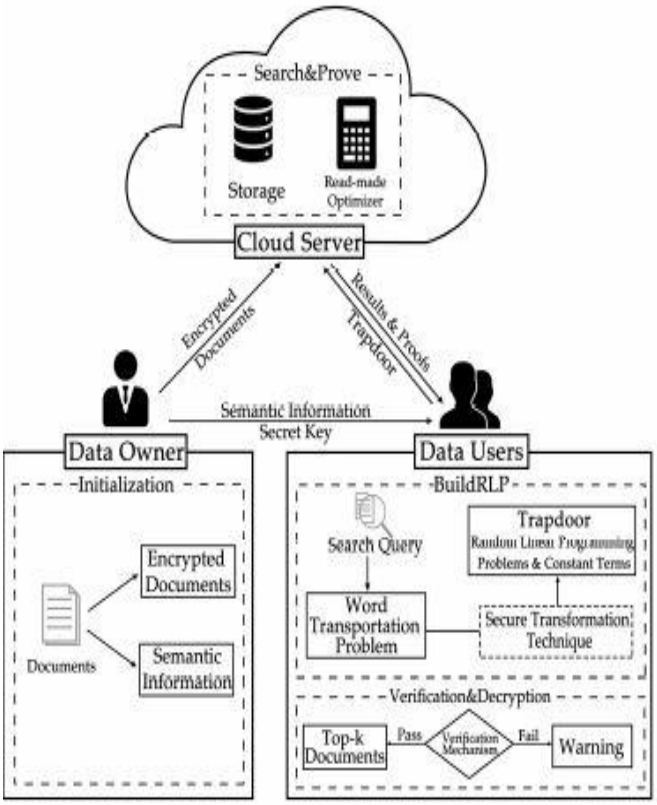






7. SYSTEM ARCHITECTURE

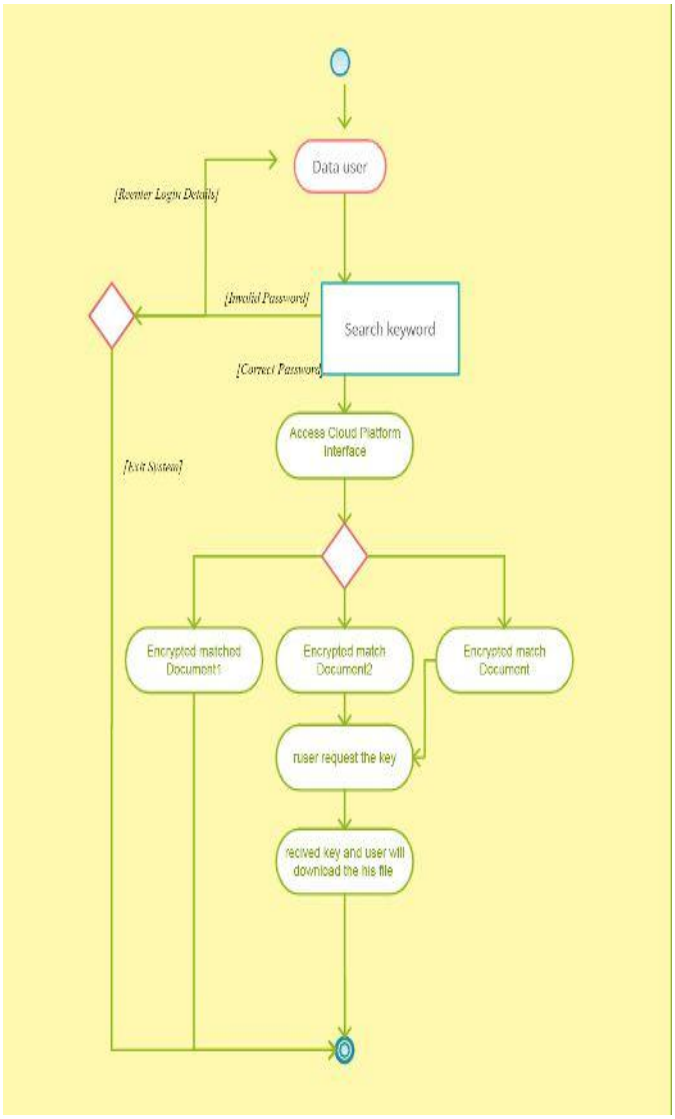
Design Engineering offers with the diverse UML [Unified Modeling language] diagrams for the implementation of venture. Design is a significant engineering illustration of a component this is to be built. Software layout is a method thru which the necessities are translated into illustration of the software program.[6] Design is the area in which great is rendered in software program engineering. Design is the way to as it should be translate consumer necessities into completed product.



gure 1. The system architecture of our secure verifiable semantic searching

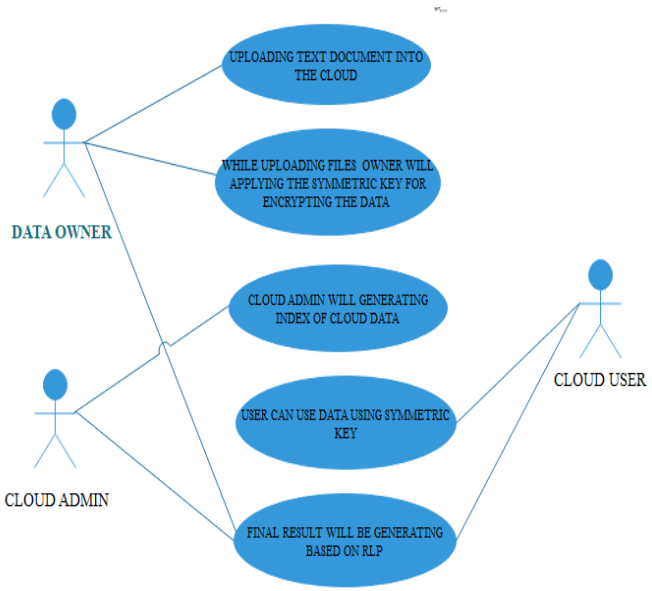
11. ACTIVITY DIAGRAM

Activity Diagrams describe how the activity is coordinated to offer a provider which may be at special degrees of abstraction. Typically, an occasion wishes to be done through a few operations, specially in which the operation is supposed to gain numerous various things that require coordination.



12. USE CASE DIAGRAM:

Use case diagrams shows the behavioral aspects of the system. A use case diagram consists of a use case and an actor. Here, data owner and user having separate registration and login then data owners will uploading the text document using the symmetric key for encrypting the cloud data.



13. APPLICATION:

Semantic Web applications:

LDO is the cornerstone of The Semantic Web, but there nevertheless only a few business LDO apps. In the brand new difficulty of Nodalities, a mag approximately the Semantic Web through UK Company Talis, there may be a piece of writing through Talis CTO Ian Davis approximately the nation of Semantic Web packages.

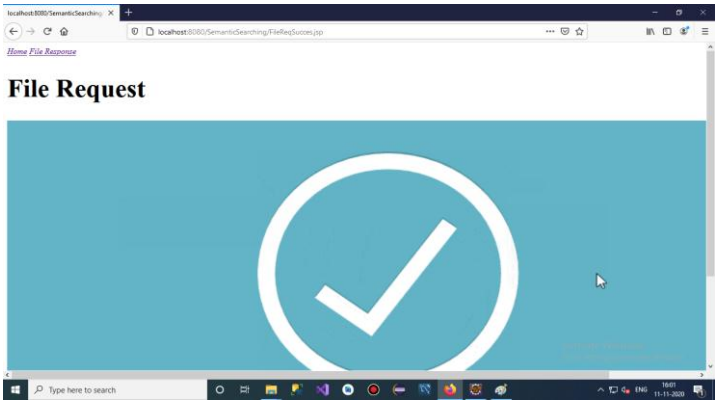
LDO software improvement for IBM records servers:

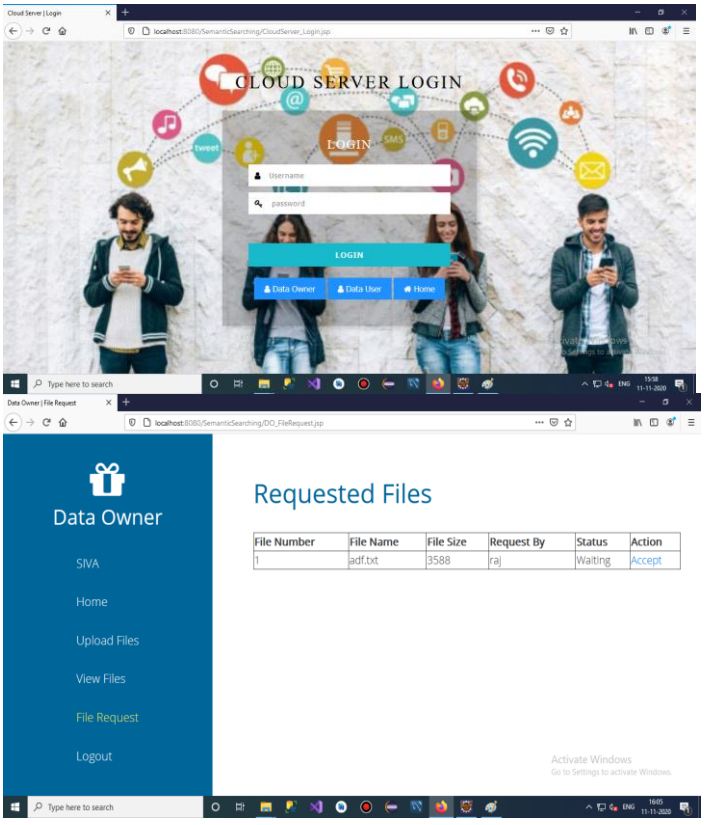
An LDO save withinside the DB2 database server is a fixed of person tables inside a database schema that shops an LDO records set. A particular save call is related to every set of those tables. Each LDO save has a desk that consists of metadata for the save. This desk has the equal call because the save.

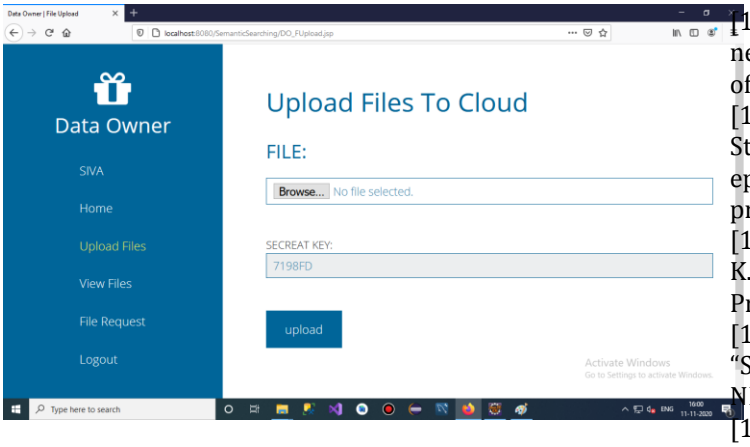
FUTURE ENHANCEMENT:

In the future, we plan to investigate on making use of the concepts of steady semantic looking to layout steady cross-language looking schemes

13. SNAPSHOTS:







14. CONCLUSION:

A protected certain semantic looking through plan that treats coordinating among questions and archives as a word transportation ideal coordinating undertaking. Accordingly, we study the essential hypotheses of heterosexual programming to plot the phrase transportation difficulty and a end result test machine that the proposed steady alternate method may be applied to plot different privateness maintaining directly programming packages. [13] We join the semantic-seek searching through noticing an information that using the transitional facts brought in the perfect coordinating cycle to test the accuracy of listed lists. That our scheme has better accuracy than different schemes.

15. REFERENCES:

[1] Boss G, Malladi P, Quan D, Legregni L, Hall H. Cloud computing, 2009. http://www.ibm.com/developerswork/websphere /zones/hipods/ library.html.
[2] Amazon Web Services (AWS), Online at http://aws.amazon.com.
[3] Google App Engine, Online athttp://code.google.com/appengine/.
[4] Microsoft Azure, http://www.microsoft.com/azure/.
[5] 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA),"Online at http://aspe.hhs.gov/ admnsimp/pl104191.htm,1996
[6] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. of NDSS'01, 2001.
[7] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. ofSP'02, 2002.
[8] SABAHI, F. Cloud computing security threats and responses. Communication Software and Networks(ICCSN), 2011 IEEE 3rd International Conference on,2011, IEEE. p.245-249.
[9] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. of SP'03, 2003.
[10] J. Li, N. Li, and W. H. Wins borough, "Automated trust negotiation using cryptographic credentials," in Proc. ofCCS'05, 2005.
[11] J. Anderson, "Computer Security Technology Planning Study," Air Force Electronic Systems Division, R eportESD-TR-73-51, 1972, http://seclab.cs.ucdavis.edu/ projects/history/.
[12] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable secure file sharing on untrusted storage," in Proc. of FAST'03, 2003.
[13] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. of NDSS'03, 2003.
[14] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS'05, 2005
[15] Su Qinggang; Wang Fu; Hang Qiangwei. (2012). Study of Cloud Computing Security Service Model, "Engineering and Technology (S-CET), 2012 Spring Congress on, vol., no., pp.1,4, 27-30.
[16] Che Jianhua, Duan Yamin, Zhang Tao, Fan Jie. (2012).Study on the security models and strategies of cloud computing. 2011 International Conference on Power Electronics and Engineering Application. Procedia Engineering 23 (2011) 586 Hopkins Hupert. (2012). [17] Securing the Cloud. diebold.[21] Chang, V.; Bacigalupo, D.; Wills, G.; De Roure, D.(2010).
[18] A Categorization of Cloud Computing Business Models. Cluster, Cloud and Grid Computing (CCGrid).2010 10th IEEE/ACM International Conference on , vol.,no., pp.509,512, 17-20.
[19] AlZain, M.A.; Soh, B.; Pardede, E. (2011). MCDB: Using Multi-clouds to Ensure Security in Cloud Computing. Dependable, Autonomic and Secure Computing (DASC). 2011 IEEE Ninth International Conference on , vol., no., pp.784,791, 12-14.
[20] K. Tserpes, F. Aisopos, D. Kyriazis, T. Varvarigou,Service selection decision support in the Internet of services, in: Economics of Grids, Clouds, Systems, and Services, in: Lecture Notes in Computer Science, vol.6296, 2010, pp. 1633. doi:10.1007/978-3-642-15681-6_2
[21] Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010.
[22] RajaRajeswari, Pradeepkumar,Vasumathi, Design and Implementation of Weather forecasting System based on Cloud computing and Data mining Techniques, International Journal of Engineering & Technology,2018
[23] Design and Implementation of municipal services for human welfare by using smart phones, International journal of Scientific research in Science and Technology 2018/4. Volume 5,issue 5.