IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 4, April 2017

Privacy Algorithms to Improve the Secure Framework for Cloud Computing Environment

Anshu Chaturvedi [1], D. N. Goswami [2], Rakesh Prasad Sarang[3]

Dept. of Master of Computer Applications, M.I.T.S. Gwalior (M.P.), India[1]

SOS in Computer Science & Applications Jiwaji University, Gwalior (M.P.), India[2&3]

Abstract: Cloud computing is a new concept of the modern world. Cloud computing combines all the services models and technologies together to deliver IT enterprise. The objective of this paper is to provide the security to end user to protect files or data from the unauthorized user. Privacy is an important issue for any technology through which unauthorized user can't access your file or data in a cloud. The main aim of this paper is to design and propose an architecture that can help to encrypt and decrypt algorithm. In this paper, we are presenting an encryption algorithm to deal with the privacy problems in cloud computing and protect the data stored in the cloud.

Keywords: Cloud computing, cloud deployment model, secure framework for cloud computing, encryption and decryption algorithm.

I. INTRODUCTION

CLOUD means Computing Location Online Utility Demand, that is to be available on demand or it allows accessing all the database resources and software through the internet from anywhere in the world, as long as they are required. The clouds are a huge pool of virtualized resources that can be accessed and are easy to use. Cloud computing is a different type of computing platform which are sharing computing resources and handles all applications. The cloud computing environment with the service node to control all users request could provide maximum service to all users.

Cloud computing is internet-based computing, a growing latest trend in the information technology (IT) world. The internet is being frequently represented as a cloud and virtualized hence the term “Cloud computing”. Cloud computing is a collection of new and old concepts in many research areas, such as distributed computing, grid computing, utility computing and service oriented architectures. In brief, cloud computing is the dynamic provisioning of IT capabilities (such as hardware, software deployment and services) from over the network [1, 2, 3].

Out of various techniques of cloud computing such as distributed, parallel, grid, utility and service oriented etc, the technique of cloud computing is the most vital one due to its many services on pay – per use basis. Cloud computing technology can be used in several services such as telephony, gas, electricity, water, data storage, computation, and application-hosting. Privacy issues in traditional web applications are still valid in the cloud computing environment.
This paper is organized as follows: Section 1 presents introduction to cloud computing. Section 2 presents cloud computing deployment models. Section 3 discusses our secure framework and existing method for privacy in the cloud. Section 4 proposes privacy encryption and decryption algorithm. Section 5 presents the performance results of both existing and proposed techniques. Section 6 presents conclusion.

II. CLOUD COMPUTING DEPLOYMENT MODELS

Various types of deployment models can be used for scalable access to computing resources and IT services. So brief descriptions of various cloud computing deployment models are as given below:

2.1 Public Cloud

Public cloud deployment model can be used by the general public. Users can share resources via the Internet. Several enterprises and organizations can work on the infrastructure provided, at the same time. Public clouds are run by the third party, and applications from different customers are liable on the clouds servers, storage systems, and networks.

2.2 Private Cloud

Private cloud deployment models are exclusively for an organizational use of cloud infrastructure networks and services. Private clouds are built for the special use of the client. The client has full control over data, security, and quality of service. They are built and managed by IT organization.

DOI10.17148/IJARCCE.2017.6413

2.3 Community Cloud
Community cloud deployment model involves a private cloud that is shared by several organizations with similar security requirement need with respect to storage. In other words, community cloud is the sharing of a private cloud for several operations, security requirements, policy, and agencies of the same administration.

2.4 Hybrid Cloud
Hybrid cloud model infrastructure is a combination of two or more (public, private, & Community,) deployment cloud models. A hybrid cloud environment combines public and private cloud models. Hybrid cloud introduces the complexity of determining how to distribute applications across both public and private cloud [4, 5].

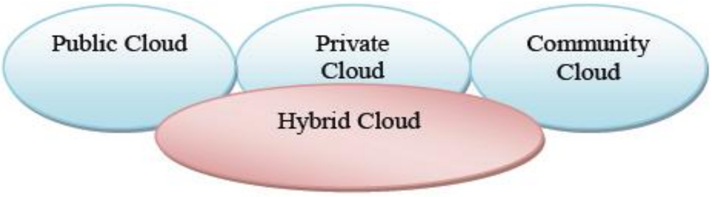

Figure 1 Cloud computing deployment models

III.SECURE FRAMEWORK FOR CLOUD COMPUTING

In Figure 2 below shows our framework for secure cloud computing environment. It has three main important privacy components; each of them includes imperative challenges connected to cloud computing privacy. These are various components:

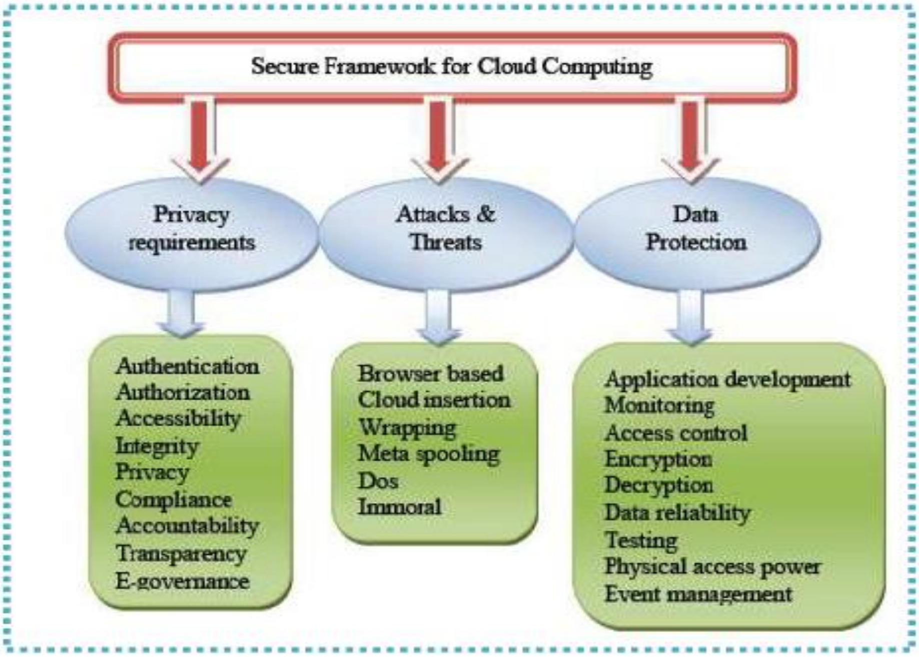

Figure 2 Secure framework for cloud computing environment

A. Privacy Requirements: privacy requirements are new challenges for the cloud storage, such as authentication, authorization, integrity etc. Privacy is the one of the security issue in cloud computing. It analyses the security model of the API- employ strong authentication, access control, and encryption techniques.

B. Attacks and Threats: attack and threats are technique used to break passwords. Caution from different types of attacks and threats to which clouds are vulnerable. So we need to increase security during message passing from the web server to the web browser by using the simple object access protocol (SOAP) message.

C. Data Protection: with cloud computing, all users' data are stored in the cloud. Because data stored in the cloud storage resources may be very sensitive and risks. For example, clouds may host electronic healthcare records and

DOI10.17148/IJARCCE.2017.6413

banking information, which control private information about patients and clients. It is better to apply proper security tools to deal with insider threats. We discuss each guideline in detail in the following sub-sections.

3.1 Privacy Requirements in the Cloud

Identity Access Management (lAM): privacy concerns confidentiality, accessibility, and reliability of information. That includes Authentication, Authorization and Assessment (AAA) of clients accessing cloud services. In a private data center, it manages the trust margin that encompasses the transparency, governance, network, systems, and applications. And it may also secure via network privacy controls including), intrusion detection systems (IDSs), virtual private networks (VPNs), and multifactor authentication systems (MASs).

Identification and Authentication Management (lAM): customer identification and authentication is a problem in the cloud computing environment. Any access made to the data will create authenticated logging username and password mechanism. Such as two factor authentication (2FA). Authentication and management are important to prevent intruders from using the cloud and to protect cloud customers reports [5].

Audit and Compliance: the audit and compliance to the internal and external processes that may follow the privacy requirements. And the privacy requirements are client contracts, rules and regulations, business sector, internal corporate policies and check policies. Compliance and audit are not an easy task since CSPs often do not know what data is being stored in their infrastructure. Out sourcing relationships play an important role for CSP. That is cloud service provider of Google do not share his data with other service providers.

Securing Data in Transmission: Encryption techniques are used for data security during communication. To maintain the security for data only goes where the customer wants it to go by using authentication and reliability. In cloud computing environment important data is not encrypted in the processing time. This advance technique is a completely homomorphism encryption scheme in cryptography, which allows data to be processed without being decrypted. Because of the confidentiality and user security is too maintained of data in transmission. The service providers should be given limited access to the data. Like authorization, authentication, providers controlling the network [5, 6].

3.2 Existing Method for Privacy in the Cloud

Encryption is a practical scientific solution for protecting sensitive data. However, beginning a prepared perspective, the overhead introduced by data encryption must be considered. Encryption and decryption privacy algorithms are resource intensive computations. When privacy algorithms are applied they will generate strong significant impact on the function of the applications in the cloud computing. Use of encryption combination of both public key and private key to hide the sensitive data of users, and cipher text retrieval is common. In data encryption, information items to encrypt and the strength of encryption depend on business requirements. The two papers analyze the possibility of the applying encryption algorithm for data privacy in cloud storage. There are different algorithms and approaches for privacy cloud computing. Techniques to find out the organization along with privacy data, such as RSA and DES have been widely studied [7].

The RSA algorithm was described in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman. The method is providing privacy by implementing RSA algorithm using cloud SQL to the data that will be stored in the third party. RSA algorithm performs three steps through the Key Generation algorithm, known as the encryption exponent or public key exponent, then finding two distinct prime numbers, all the values are relative, and public key and private key must be kept secret. Using second encryption algorithm, sender transmits the public key to recipient for the process of encryption data. And third decryption algorithm, known as the decryption exponent or private key exponent, a recipient uses the private key to decrypt the plaintext from the message received. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data [8, 9].

The DES algorithm was described in November 1998 by triple DES (3DES). 3DES is exactly what it is named is the minus (-) it performs 3 iterations of DES encryption on each block. Data privacy systems implemented into cloud computing using DES algorithm is available. This Cipher chain block system is used to secure data for customers and server. The privacy architecture of the system is designed by using DES Cipher chain block, which eliminates the fraud that occurs today with stolen data. In encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher chain block, in decryption site, it takes a 64-bit cipher chain block and creates a 64-bit plaintext, and same 56-bit cipher key is used for both encryption and decryption algorithm[10,11].

IV. PROPOSED ALGORITHM

The privacy algorithm is also called the encryption and decryption algorithm. This proposed method uses DES and RSA algorithm to generate encryption when a user uploads the text files in cloud storage, and opposite DES and RSA

DOI10.17148/IJARCCE.2017.6413

algorithm to generate decryption. It is the most popular algorithm to find all the cloud data storage. Encryption technique is a scientific solution for data protection in cloud. Therefore, the work is to look at database encryption approaches for ecommerce cloud functions. Database level relies on the encryption functions provided by DBMS. Like the databases Oracle, SQL Server, and Mysql. User from the private or public domain can request the file from the server. Encryption algorithm converts the data into Cipher text form by using the fixed key and only user have the key to decrypt the Cipher chain. That is, only one fixed key is used to encrypt and decrypt the cloud data [11].

4.1 Rail fence Transposition Technique
The rail fence technique is one of the transposition ciphers that get its name from the way, in which the plaintext it is encoded. In the rail fence technique, the plaintext is written downwards as a sequence of rows. Then moving up when we get to the bottom. For example, using the message of "**welcome cloud**",
with the cipher writes:
w l o e l u
  e c m c o d
Now the reads off encrypted message are "w l o e l u e c m c o d".
In this technique, the same alphabets in the plaintext are rearranged. This technique alone cannot be satisfactory for privacy data storage.

4.2 Notations used

p:	Plaintext value function
k:	Assigned fixed key length
i:	Assign the position (i) of the letter
c:	Cipher text
E:	Encryption
D:	Decryption

4.3 Steps of Proposed Algorithm
A. Encryption Algorithm
Followings are the step in proposed encryption algorithm is as given below:
Step 1: Initialize: get the plaintext letter.
Step 2: Get the fixed key length from the range numbers (0 to 256).
Step 3: Assign the position (i) of the letter.
Step 4: Generate the ASCII value of the plaintext letter.
Step 5: Assigned same fixed key length is considered as a key.
Step 6: Convert the plain text into equivalent ASCII code.
Step 7: Encrypted the value using addition.
Step 8: To apply the formula given below:
$E = (p + k) + i \bmod 256$
Step 9: The generate ASCII character of the corresponding decimal value in the result from the above given formula. This would be the cipher text.

4.4 Working Example of Encryption
The followings are the detailed description of each step in the proposed encryption algorithm. The special characters (256) in order of ASCII full characters. Suppose that let the character is "i". Now according to the steps, we will get the following:
Step1: Get the plaintext letter (ASCII).
Step2: Assign a fixed key value is 10.
Step 3: Assign the position (i) is 0.
Step 4& Step5: ASCII of "i" is 105 in decimal.
Step 6: Let, the character is "i".
Step 7& Step 8: To apply the formula given below:

$$\begin{aligned} E &= (p + k) + i \bmod 256 \\ &= (105 + 10) + 0 \bmod 256 \\ &= (115) + 0 \bmod 256 \\ &= 115 + 0 \bmod 256 \\ &= 115 + 0 \\ &= \boxed{115} \end{aligned}$$

Step 9: As per the algorithm the cipher text would be “S”.
Once the data is encrypted using an algorithm, it will be transmitted and stored in the database of cloud storage. Enter the key value; the cipher text of the message will be displayed. In Figure 3 represents the simplified model for encryption technique [11, 13, 14].

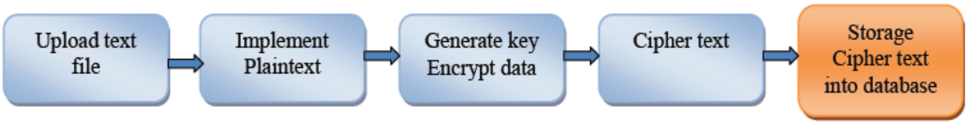

Figure 3 Execution of entire encryption process

B. Decryption Algorithm
Step 1: Initialize: generate the ASCII value of the cipher text character.
Step 2: Here the same encryption fixed key length used.
Step 3: Assigned the position (i) of the cipher text.
Step 4: let subtract the value with ASCII code.
Step 5: To apply the formula given below:
$D = ((c – k – i) + 256) \bmod 256$

4.5 Working Example of Decryption
In decryption, after encrypts “i” we have got “S” as the cipher text. Now finally the value of the according character “i” is to decryption algorithm let’s attempting to get back the original plaintext i.e. “i”.
Step 1: 115 is the ASCII value of the cipher text character “S”.
Step 2: Here, the same key value“10” is used.
Step 3: Here, position (i) “0” is used.
Step 4: The formula is applied to the ASCII value 115 of the cipher text character and key value 10.

$$\begin{aligned} D &= ((c – k – i) + 256) \bmod 256 \\ &= ((115 – 10 – 0) + 256) \bmod 256 \\ &= ((105– 0) + 256) \bmod 256 \\ &= (105– 0) + 256 \bmod 256 \\ &= (105– 0) +0 \\ &= 105 \\ &= \boxed{105} \end{aligned}$$

Step 5: “i” is the ASCII character of the decimal 105. The character “i” would be the original plaintext. The cipher text can be transformed back to the original plaintext by using a decryption algorithm with the same key that was used in encryption [7,11, 12,15,16]. In Figure 4 represents the simplified model for back to the original plaintext decryption technique.

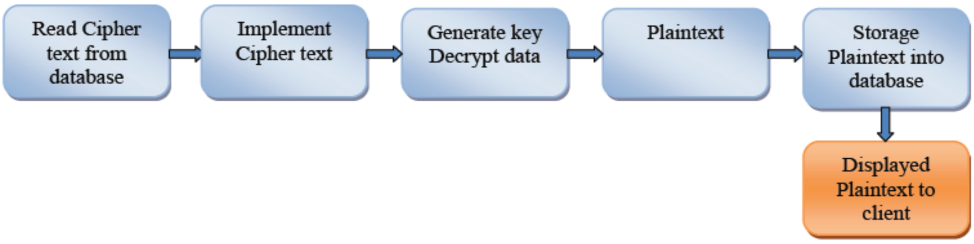
Read Cipher text from database
Implement Cipher text
Generate key Decrypt data
Plaintext
Storage Plaintext into database
Displayed Plaintext to client

Figure 4 Execution of entire decryption process

V. PERFORMANCE RESULT

This section presents the performance results of both existing and proposed techniques. To explore the performance of proposed algorithm, ASCII character is used and all the experiments are performed on Pentium IV 2GHz Intel corei3 PC machine with 4GB RAM, organization Microsoft Windows 10. This algorithm is implemented in MATLAB and used Microsoft .Net framework a service based cloud. All the runtime reports include both CPU time and I/O time.
The encryption and decryption privacy algorithms are resource intensive computations. Encryption algorithm, sender transmits the public key to recipient for the process of encryption data. Encryption time is the total of time required to

encrypt the given data. Decryption time is the process of converting the encrypted text into the original text. That is the sum of required to convert the encrypted data into the original plaintext. The algorithms we examine our proposed set of rules offers higher overall performance outcomes with existing systems. For the comparative study of the existing system and proposed system, we have taken an input data then the results are calculated by using two parameters encryption execution time and decryption execution time.

Figure 5 shows that there is the execution processing time in encryption technique. We see the read time increase rates by encryption.

Table1: Execution time in seconds for different input size

Input size (in bytes)	Encryption time (Existing System)	Encryption time (Proposed System)
328	0.045728	0.035314
561	0.076743	0.065321
899	0.168722	0.104311
1535	0.470493	0.350245
1873	0.450324	0.350112

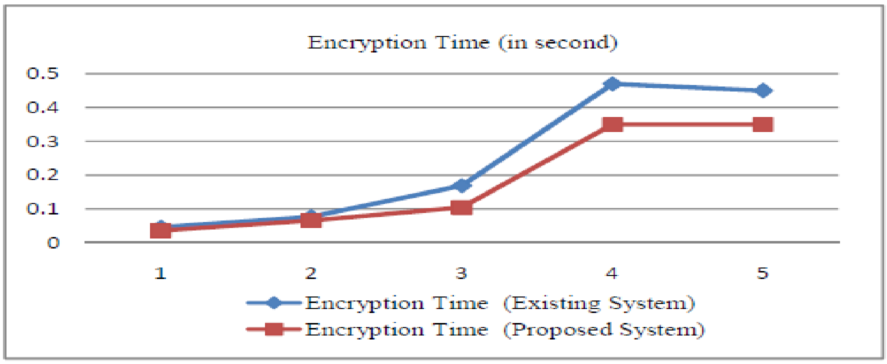

Figure 5 Execution process of encryption time

Table2: Execution time in seconds for different input size

Input size (in bytes)	Decryption Time (Existing System)	Decryption Time (Proposed System)
328	0.029471	0.020235
561	0.072092	0.036045
899	0.158875	0.104436
1535	0.451762	0.221030
1873	0.481288	0.241044

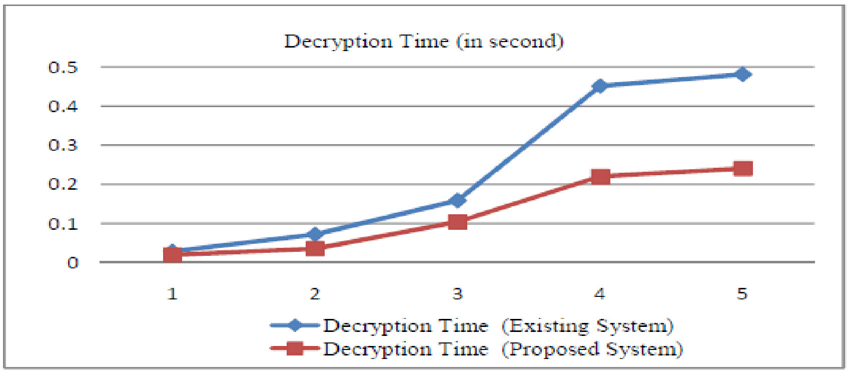

Figure 6 Execution process of decryption time

This algorithm compared to previous technique our proposed algorithm takes minimum time for encryption and decryption. The table below (Table1) and (Table2) shows the execution time corresponding to different input sizes.

Figure 6 shows that there is also execution processing time in decryption with respect to different key range. So the time consumption for converting cipher data back to the original data. The proposed algorithms are implemented in this real time, and the performed on the machine requires minimized decryption time (ms). Finally as a result are compared and analyzed, we can see that proposed approach (proposed system) takes only minimum time in comparison to an existing system. Hence, we save approx 10 % time in the proposed system.

VI. CONCLUSION

This paper proposed algorithm is an encryption and decryption techniques to provide privacy cloud storage. This paper focuses on the execution process time in encryption and decryption techniques. The main intention of this work is to provide privacy to the stored data in the cloud environment. This algorithm includes such as, secure storage in the cloud, high security, privacy, low cost and minimum processing time. The main advantages of this work are only the authorized user can access the cloud storage data. Due to this, proposed approach takes very less time for performing computations during execution process time. The results are analyzed and evaluated in terms of encryption time and decryption time. The future work will focus on more privacy for cloud storage using by different cloud computing device with location based search.

REFERENCES

[1] Xin, Z., Song-qing, L., & Nai-wen, L, "Research on Cloud Computing Data Security Model Based on Multi-dimension", International symposium on information technology in medicine and education, IEEE, pp 897-900, 2012.

[2] Rao, Srinivasa and V Nageswara Rao, "Cloud Computing: an Overview", Computing, pp71-76, 2009.

[3] Jain, S., Kumar, R., A. & Jangir, S. K., "A Comparative Study for Cloud Computing Platform on Open Source Software", An International Journal of Engineering & Technology (AIJET), Vol. 1, No. 2, pp 28-35, 2014.

[4] Paper, White, "Introduction to Cloud Computing" Interfaces.

[5] Kulkarni, G., & Gambhir, J.,"A Security Aspects in Cloud Computing", Computer Engineering, IEEE, pp 547-550, 2012.

[6] Youssef, A. E., & Alageel, M., "A Framework for Secure Cloud Computing", International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 4, No 3, pp 487-500, 2012.

[7] Klein, A., "A Benchmark of Transparent Data Encryption for Migration of Web Applications in the Cloud", 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, IEEE, pp735-740, 2009.

[8] Saravanan, N., Mahendiran, A., Subramanian, N. V., & Sairam, N, "An Implementation of RSA Algorithm in Google Cloud using Cloud SQL", Research Journal of Applied Sciences Engineering and Technology, 4(19), pp 3574-3579, 2012.

[9] Jadida, E. (n.d.), "Encryption as a Service for Securing Data in Mobile Cloud Computing", 15th International Conference on Intelligent Systems Design and Applications (ISDA), IEEE, pp 546-550, 2015.

[10] Padmapriya, A., & Subhasri, P., "Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security", International Journal of Engineering Trends and Technology (IJETT), Vol. 4, Issue 4, pp 1067-1071, 2013.

[11] Khan, S. S. & Tuteja, R.R., "Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol. 3, Issue 1, pp 148-154, 2015.

[12] Arockiam, L., & Monikandan, S., "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 2, Issue 8, pp 3064-3070, 2013.

[13] Subhasri, P., & Padmapriya A.,"Multilevel Encryption for Ensuring Public Cloud", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol.3, Issue 7, pp 527-532, 2013.

[14] Jacob, J., Dadra, U. T., & Haveli, N., "An enhanced tbahibe-lbkqs techniques for privacy preservation in cloud", International Journal of Computer Application (IJCA), Vol. 6 No.5, PP 32-40, 2016.

[15] Kaur, N., Aulakh, T., & Cheema, R., "Comparison of Workflow scheduling Algorithms in Cloud Computing", International Journal of Advanced Computer Science and Application (IJACSA), Vol. 2, No.10, PP 81-86, 2011.

[16] Hebiya, P. R., & Ganesh, J., "Secure Data Storage Framework using Anti- XSS in cloud", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Vol. 4, Issue 11, pp 11429-11436, 2015.

BIOGRAPHY

Mr. Rakesh Prasad Sarang is pursuing Ph.D in computer science from jiwaji university Gwalior under the guidance of Dr. Anshu Chaturvedi and Dr. D.N.Goswami. He has completed MCA from Department of Computer Application Madhav Institute of Technology & Science, Gwalior MP. His research interests are in the areas of Cloud Computing, Big Data and Linux.

DOI10.17148/IJARCCE.2017.6413