INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Special Issue of Second International Conference on Science and Technology (ICOST 2021)

Study and improved data storage in cloud computing using cryptography

Mohd. Akbar[1], Irshad Ahmad[2], Dr. Thirupathi Regula[3]

[1]Lecturer, Dept. of Information Technology, University of Technology and Applied Sciences (HCT), Muscat, Sultanate of Oman

[2]Lecturer, Dept. of Information Technology, University of Technology and Applied Sciences (HCT), Muscat, Sultanate of Oman

[3]Lecturer, Dept. of Information Technology, University of Technology and Applied Sciences (HCT), Muscat, Sultanate of Oman

akb.mtech@gmail.com[1], irshad17@gmail.com[2], regulathirupathi@gmail.com[3]

Abstract

Cloud computing is becoming a powerful network architecture to perform computing that is both large and complex. We present a cloud computing survey which outlines its core concepts, architectural principles, state-of- the art deployment and research challenges. Due to security issues, information over the Internet is becoming important. We have suggested a method to protect critical file data. Cryptography algorithms are an efficient way to encrypt sensitive data. It is a retrieval and transmission system that is readable only by intended users. The low cost and data usability of cloud computing is advantageous. Cloud storage has many advantages at low cost and data connectivity through the Internet. Ensured cloud data protection is an important part of the cloud computing environment because customers often store sensitive information with cloud storage services but they are not secure services. So, it remains a challenge to exchange data in a safe way while storing data from an unconfident cloud. Our solution guarantees consumer confidential data protection and privacy by using the AES, RC2 algorithm to store data in a single cloud. The cloud computing concept and transitional discussion under cloud computing will be provided previously proposed. The cryptographic algorithm used in cloud is then addressed and the latest trend for cloud security.

Keywords: Cloud Computing, Cryptography Algorithms, Security, Data Storage

1. Introduction

Cryptography is the defence of the unauthorised party's data technologies by translating it into the unreadable form. The main purpose of encryption is to secure the privacy of third-party data. There are two algorithms, one is a symmetrical key algorithm, also known as a standard key algorithm, and one is an asymmetrical key-based algorithm, also known as a public key algorithm. [1]. Security is known to be an essential factor of a cloud computing setting because of the relevance of cloud knowledge. The details can be classified and highly sensitive. The administration of data should also be entirely accurate. The data in the cloud must be secure from malicious attacks. Health issues secrecy, honesty and data availability. The lack of secrecy results in unwarranted access to information. [2] Cloud services failures allow data privacy and functionality to suffer. Protection has the complimentary features of durability. The value of this cloud and its resources is not limited to a domain or any area. This data can be used by all the customers, such as the heads, teachers and pupils.

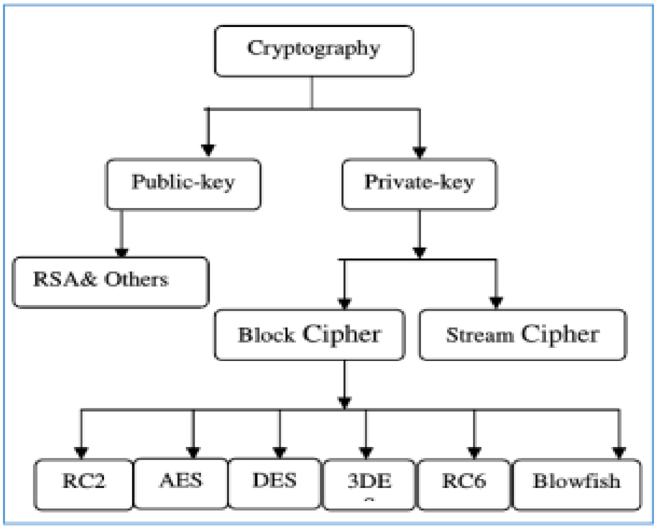

Fig.1. Block Diagram of the Cryptography

1.1 Cloud Computing Features

- Cloud storage delivers on-demand consumer tools and services. The services can be scaled across different centres.
- Cloud storage requires less spending in capital spending. There is no provision of capital spending. Users can pay for the services and capability they use, or use it or pay for it.
- Higher resource Cloud computing will guarantee user's hardware, Processor, bandwidth and memory capacities quality operation.
- Cloud management vendors manage the system and connect to it through APIs which don't have to be built on PCs and which thus minimise further the maintenance needs.

1.2 Cloud Cryptography and Security

More businesses and organisations are taking advantage of cloud computing every day. Cloud computing provides customers with a virtual data management and service platform. However, cloud storage has introduced security issues as cloud providers store and process customer data beyond customer's control. Different organisations create cloud-based cryptographic procedures in an effort to balance protection and success effectively.

1.3 Problem Statement

Customer data stores are vulnerable to multiple attacks from cloud storage vendors. Four forms of model threats are considered in our work. Firstly, a single failure point that would impact information functionality if a system fails or crashed on the provider, making it more difficult for consumers to access their processed information from the server. Data access is also a big problem that may be impacted by the absence of the cloud service provider (CSP). [3]

2. Literature Review

The IEEE defines data security as 'the extent to which data collection is safeguarded against risk of accidental or malicious damage or loss' ([4]). In 2005 ISO/I EC 27002 for information security was developed by the International Standard Association. It is labelled standard as a defence of confidentiality (security and accuracy of information and processing methods) and availability' (ensuring that approved users have access to information and related properties if required) [5]. Many methods are used to achieve data protection. These methods can be grouped into four distinct categories: masking, erasing, backup and encoding. Cryptography appears to be the only way to protect outsourced data in an insecure environment, such as cloud storage, where our data is not physical mental controlled. [6-8] Multi-tenance capabilities and simple data provider connectivity renders us confidential, mainly by means of creative encryption and access management strategies. The data encryption refers to the practise of encrypting data on storage devices using the principle of cryptography.

3. Research Methodology

In this section, we explain the solution suggested for countering data protection problems in cloud computing logically. When utilising the cloud storage mechanism, sharing resources may be the possibility of breach or leakage, in particular the sharing of data by the data owner and approved clients. Indeed, it is impossible to protect data in the cloud if the user does not trust the service provider. The consumer must blindly trust the processes of the provider, but the risks of cloud insiders that are able to access data will hold back. Many methods and technology have been suggested for ensuring data protection; among them crypto-graphing is the most effective. Symmetrical cryptographic techniques are the most effective method taken for safe records. But in a multi-tenant situation this method alone is not efficient; multiple licenced customers have the right to access data such that the data key must be circulated to each user. Key management is too hard to achieve and there is a possibility of submitting keys to multiple clients concurrently. The asymmetric encryption methods may be an appropriate means of ensuring data protection. This approach, however, limits the access by data owner to the multi-user feature of cloud computing. This solution does. The asymmetric encryption algorithm also has a strong effect on the access to information. This normally does not allow vast volumes of data to be encrypted for users in acceptable time.

3.1 Types of Clouds

There are several problems to address when bringing a company application into the cloud world. Some service providers, for example, are more interested in reducing operating costs, others prefer high reliability and security. There are, therefore, various cloud types, each with its own advantages and disadvantages:

Public clouds: A cloud where service providers offer their tools to the general public as services. Public clouds provide some primary advantages to service providers, including no initial infrastructure investment and risk shifting to infrastructure providers.

Private clouds: Private clouds, also known as internal clouds, are designed for one organization's exclusive use. The association or external providers can create and manage a private cloud. A private cloud provides the highest level of efficiency, reliability and security control.

Hybrid clouds: A hybrid cloud is a mix of public and private cloud models that seeks to overcome each approach's limitations. The majority of the service infrastructure in a hybrid cloud runs on private clouds while public clouds run. Hybrid clouds provide additional freedom than private and public clouds.

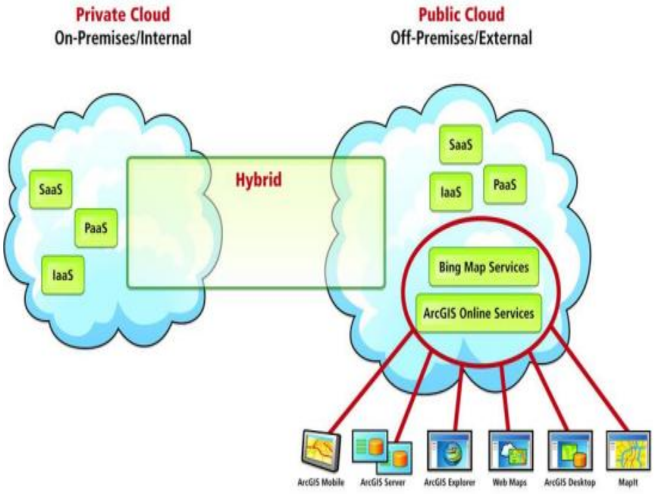

Fig.2. Types of clouds

3.2 Cloud Security Implementation

Once information is stored in a cloud, there might be certain issues regarding privacy, compliance and governance. Privacy issues embody queries of security and whether or not your competition or malicious users will access sensitive company or client information If confidential information is being consumed or accessed by individuals outside the organizations, it's vulnerable to information fraud and different complications, like ancient IT service suppliers, enterprises expect cloud service providers (CSPs) to verify their tight security audits and certifications. Compliance is the very important feature of security. Enterprises ought to let the CSPs recognize the parameters they'll be evaluated and audited against. [7] The providers ought to even control responsible by regulative agencies to confirm compliance with the foremost tight controls and measure. Governance may be a key challenge. Enterprises worry concerning information possession and what privileges (such as access, update and delete and delete) users might have once process their information totally different deployment models present different governance problems. It's essential that enterprises perceive these problems related to a cloud preparation so as to effectively manage the safety of their data. Enterprises need to judge the security of their information and also the effectiveness of their security measures against cyber-attacks. [8] Company and client information security are a very important consideration regardless of whether or not the info is maintained by the company itself or by the third-party Cloud Service Providers. It's vital to observe the protection and also the numerous steps taken by the provider to shield the info from cyber as well as natural attacks.

3.3 Related Work

Cloud supports large-scale data collection, which ensures that cloud computing is prevented by tonnes of pressures. Privacy and data privacy of online data stores are the main risks in the cloud. This is the only way for hackers to be able to use a single box for inserting anything into their cloud models. Proposed an evidence approach of using the meta info. This data is generated using a random collection of bits in the original file and is added in an encrypted manner and is stored in the cloud; thus, if a person wishes to verify the integrity, he/she throws a challenge by defining the block number and its corresponding meta data.

3.4 Enhancing Data Security's Algorithm

Cloud storage data is encrypted using a symmetric cryptographic key algorithm

The data owner produces the symmetrical key for encrypting the information, and then the asymmetrical two keys for encrypting the symmetrical key. It converts its public password to cloud servers, generating two asymmetrical keys. Then the cloud stores Upub's owner with public cloud keys. The next step enables the data owner to enter the public key for the cloud provider and encrypts the symmetrical key ksym with the public key of the cloud provider. He sends KE finally to the storage cloud. The figure's graphs display the step-by-step algorithm describing a major exchange step.

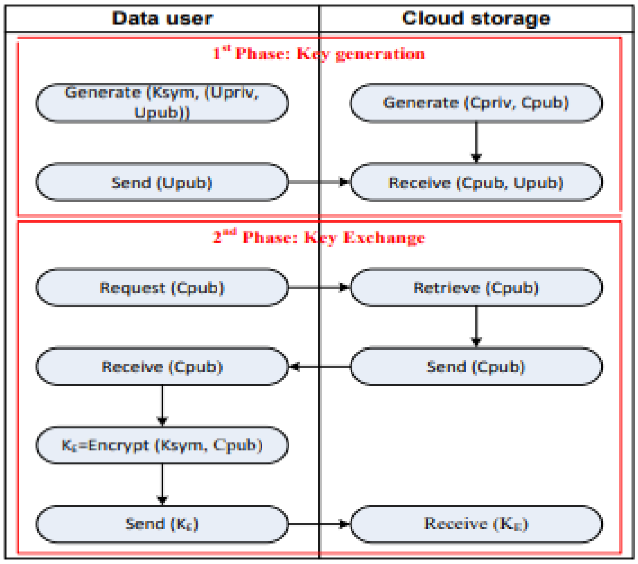

Fig.3. Key Generation Phase.

4. Results and Discussion

We also deployed various kinds of cryptographic symmetric and asymmetric algorithms in the cloud setting to review the efficiency of the solution technically suggested in the previous section. The hybrid algorithm was then applied. Application of Compressive Sensing (CS) restoration to a cloud for the outsourcing of high machine sophistication remains difficult to secure data security and retain an image simultaneously proposed to tackle this problem in the article "Compression sensing based privacy protection outsourcing of the image storage and identity authentication services in cloud" a novel outsourced image restoration and identity authentication framework. It incorporates signal processing methods into the CS domain and outsourcing of computing. This guarantees the cloud safely rebuilds the picture without exposing the underlying privacy content. AES-based data encryption contains multiple rounds depending on the cypher blocks, i.e. AES-256, AES-128. AES-192. A standard AES encryption round contains four sub-processes. The first round is shown below.

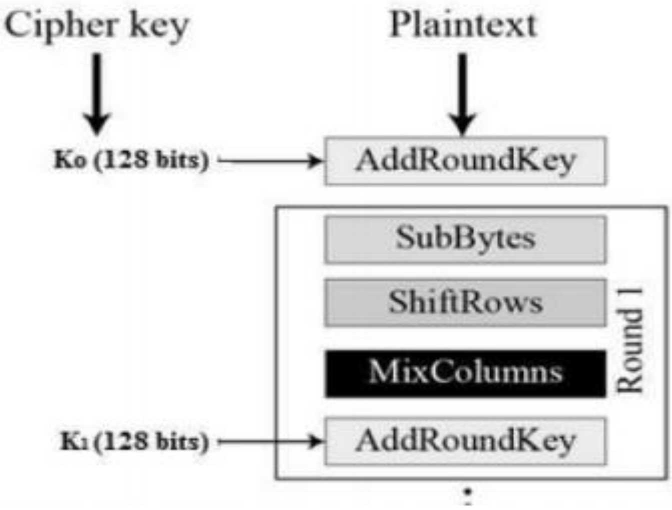

Fig.4. Sub-Processes in Round

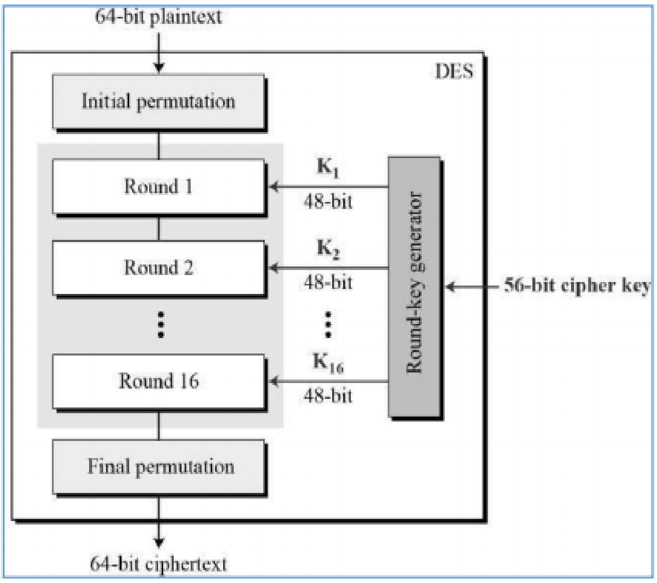

Fig.5. Data Encryption Standard

4.1 Decryption Process

The decryption process of AES cipher text is identical in reverse order to the encryption process. Each round comprises the four reverse order processes.

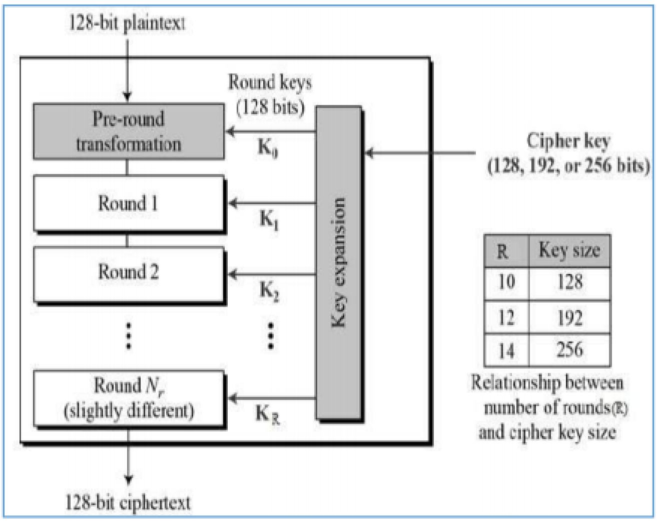

Fig.6. RC-2 Encryption Algorithm

RC2 is the symmetrical main block cypher in cryptography. "RC" means "Ron's Code" or "Rivest Cipher" but RC4, RC5 and RC6 are the other cypher constructed by Rivest.

Lotus funded the development of RC2 and found a custom chip that could be exported in the form of its Lotus Notes programme after an assessment by the NSE. The NSA recommended a few improvements incorporated by Rivest.

Sub Bytes: In the sub-byte-step, the 8-bit replacement, Rijndael S-box, is replaced by a sub-byte-S in each byte ai,j in the state matrix. This operation gives cryptographic non-linearity. The S-box is designed to prevent attacks based on simple algebraic properties by combining the reverse function with an invertible, affine transformation.

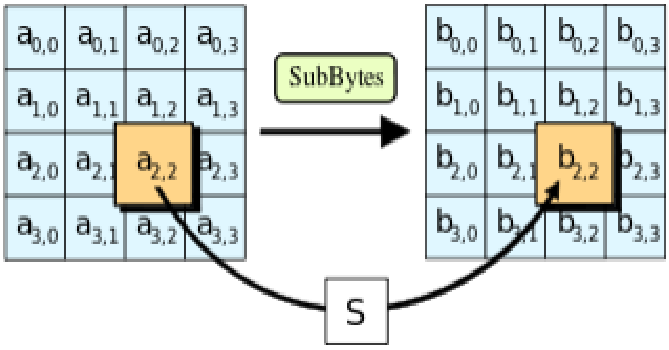
SubBytes
S
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Fig.7. Sub Bytes Process

Shift Rows: The Shift Rows step functions on the state lines; cyclically the bytes in each line are moved by a certain offset. The first row of AES remains unchanged. Each byte is pushed to the left in the second row. Similarly, offsets of two and three respectively alter the third and fourth line. For 128-bit and 192-bit blocks, the changing pattern is the same. Row n is redirected by n-1 bytes on the left circular. The first row for a 256-bit block is unchanged and the changes for the second, third and fourth row are 1 byte, 3 bytes and 4 bytes.

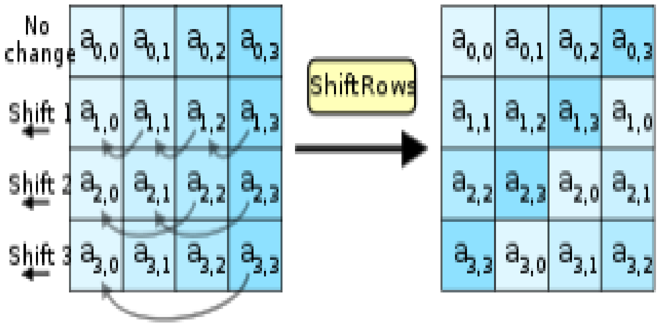
No change
Shift 1
Shift 2
Shift 3
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Fig.8. Shift Rows Process

Mix Columns: The four bytes of the status column are combined with an inverted linear transformation in the mix column step. The column mix feature uses four bytes as input and generates four bytes, with each byte influencing all four bytes.

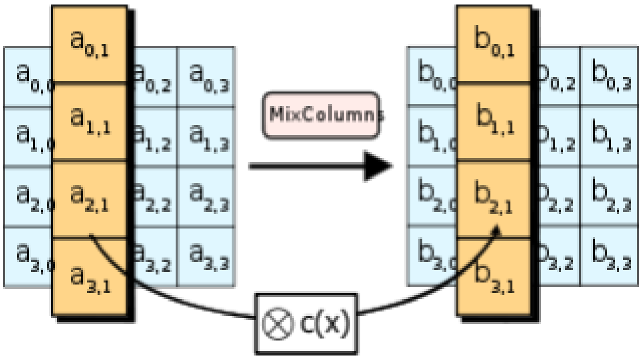
MixColumns
⊗c(x)
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Fig.9. Mix Columns Process

4.2 Discussions

This review reveals that the novel strategy benefits from the symmetrical algorithm over the time of processing and from the power of the main length asymmetric algorithm. This modern lightweight algorithm is potentially faster than other cryptographic data processing techniques. Moreover, the main delivery mechanism makes it durable and stable. This work could be improved by a new key delivery system to provide each authorised customer with the encryption key without the involvement of the cloud provider. AES is commonly used and supported in hardware and software in modern cryptography. No functional cryptography AES attacks were discovered till now. Furthermore, AES has incorporated key length versatility which allows for a level of 'future-proofing' against progress to complete key searches.

Conclusions

In the cloud environment data security is an open problem. Many techniques and technology, including the most cost-effective ones are cryptography, were suggested to provide data protection. The key purpose is to store and view data safely in cloud, not managed by the data holders. We use the elliptical-curve encryption strategy to secure cloud data files. Two parts of the clout server improved the performance during data collection and access. The Advanced Encryption Standard (AES), also known as the Rijndael, is a specification on electronic data encryption. Encryption is a method for encoding messages or vital information such that only can be read by canonical parties. Encryption does not avoid interception by itself, but denies interceptor information A further advantage to improve encryption and decryption efficacy is ECC Encryption Algorithm used for encryption. We believe that it is safe and productive to store and access data. We are continuing to address the issue of community data-sharing in the shared data segment so only a member of the group can access the gathered data in this scheme through the shared data. One, many connections are not feasible.

References

Journals

[1] Silki Jain and Abhilasha Vyas, “An Improved Security Framework for Cloud Environment using ECC algorithm”, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 6 Issue I, pp. 635-641, January 2018.

[2] G. Vennila, Dr. D. Arivazhagan, N. Manickasankari, “Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm”, International Journal of Engineering and Technology (IJET), Vol 6 No 5 Oct-Nov 2014.

[3] G. L. Prakash, M. Prateek and I. Singh, ’Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System’, International Journal of Engineering and Computer Science vol. 3, issue 4, pp. 5215- 5223, April 2014.

[4] Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847), Volume 3 Issue 3, pp.171-176, March 2014.

[5] Sachdev and M. Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications, vol. 67, No. 9, 2013, pp. 19-23.

Conference Proceedings

[6] J. Mohammad, K. Omer, S. Abbas, E. S. M. El-Horbaty, and A. B. M Salem, “A comparative study between modern encryption algorithms based on cloud computing environment”. 8th International Conference for Internet Technology and Secured Transactions (ICITST’13), IEEE, 2013, pp. 531-535.

[7] H. Rahmani, E. Sundararajan, Z. M. Ali, and A. M. Zin, “Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud”. Procedia Technology, vol. 11, 2013, pp. 1202-1210.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In P. Ning, S. De Capitani di Vimercati, and P. Syverson, editors, ACM Conference on Computer and Communication Security (CCS '07).ACM Press, 2007.