Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

MULTILEVEL SECURITY ON CLOUD COMPUTING WITH CRYPTOGRAPHY ALGORITHM

M.INDHUMATHI[1],B.SALAI NALVETHAM[2], R.VENKATESH[3]
[1,2,3]*Information Technology, SKP Engineering College*

Abstract: Cloud has often been used as a metaphor for Internet in the network "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing *resources (e.g., networks, servers, storage, applications, and services*) that can be rapidly provisioned and released with minimal management effort or service provide interaction.". Cloud computing allows enterprises to get their applications up and running faster because of this advantage proponents claim the cloud computing. To meet fluctuating and unpredictable business demand enables IT to more rapidly adjust their resources.

Some Enterprises are moving to the cloud for large storage capacity, Some won't move because of a lack of security. Many Enterprises facing the security problem in cloud computing.so it is the main barrage of Enterprises to store the information in cloud

Every vendor product is "cloud-based." So securing the data is vital importance security is important because of typical nature of cloud computing and the large amounts of complex data it carries. The main obstacle of cloud computing is security because it stores the data and disseminates resources in the open environment, so it hampers the deployment of cloud environments

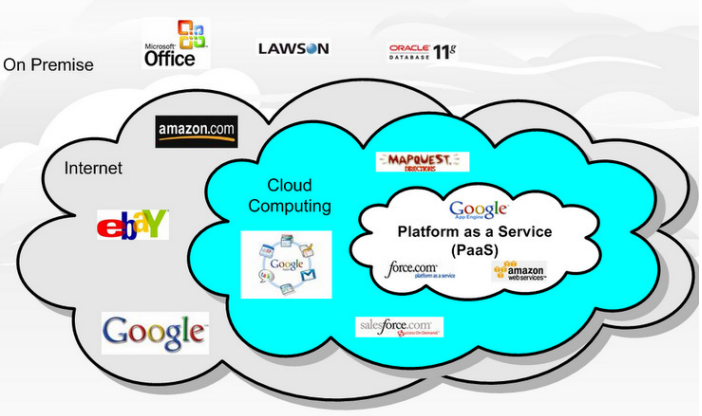
To be effective, cloud data security depends on more than simply applying appropriate data security procedures and counter measures. Computer based security measures mostly capitalizes on user authorization and authentication. Simply applying appropriate data security procedures and counter measures should be depends on cloud data security effectively. User authorization and authentication mostly capitalizes the computer based security measures. But safe and secure environment for the personal data and info of the user is till required.. The concept of this research is based of readings on "cloud" computing and it tries to address, related research topics, challenges ahead and possible applications. So we proposed multilevel algorithms to ensure that data security . By using multilevel encryption may provide more security for Cloud Storage than using only public key encryption

Keywords: Cloud computing, Infrastructure Service ,Security Algorithms, AES algorithm,MD5 algorithm, HOMOMORPHIC algorithm.

I. INTRODUCTION

Cloud Computing refers to manipulating, configuring, and accessing the hardware and software resources remotely. It offers online data storage, infrastructure, and application.
Cloud computing offers **platform independency,** as the software is not required to be installed locally on the PC. Hence, the Cloud Computing is making our business applications **mobile** and **collaborative.** Cloud Computing refers to both the applications delivered as services over the

Internet and the hardware and systems. Software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service, so we use that term. The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the public, we call it a Public Cloud; the service being sold is Utility Computing.

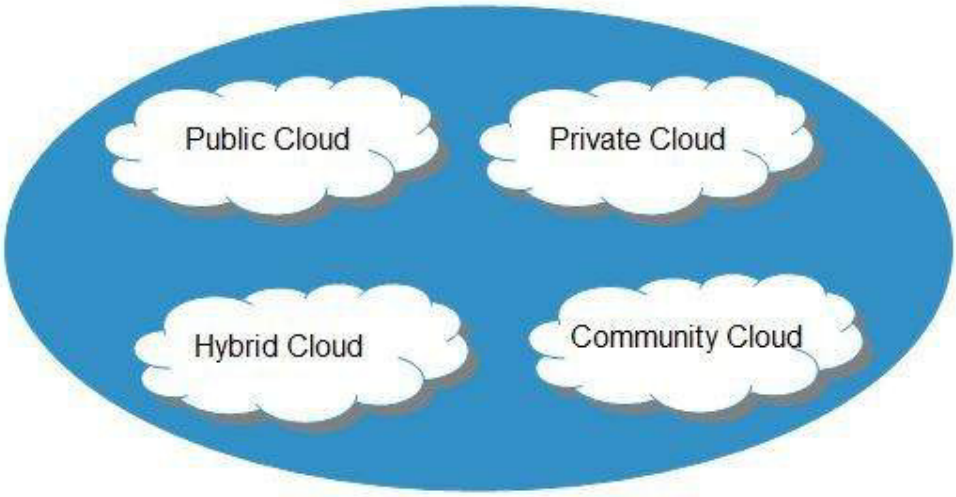


Basic Concepts

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:
Deployment Models
Service Models

Deployment Models

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid, and Community.



Private cloud

A private cloud is one of the type of **cloud** computing that involves a unique and secure **cloud** based environment in which only the specified client can operate.

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services and the comparison of private and public cloud

Hybrid cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability(e.g., cloud bursting for load-balancing between clouds).

Service Models

Cloud computing is based on service models. These are categorized into three basic service models which are -

- Infrastructure-as–a-Service *IaaS*
- Platform-as-a-Service *PaaS*
- Software-as-a-Service *SaaS*
- Anything-as-a-Service *Xaas*

Anything-as-a-Service

XaaS is service model, which includes Network-as-a-Service,Business-as-a-Service, Identity-as-a-Service, Database-as-a-Service or Strategy-as-a-Service.

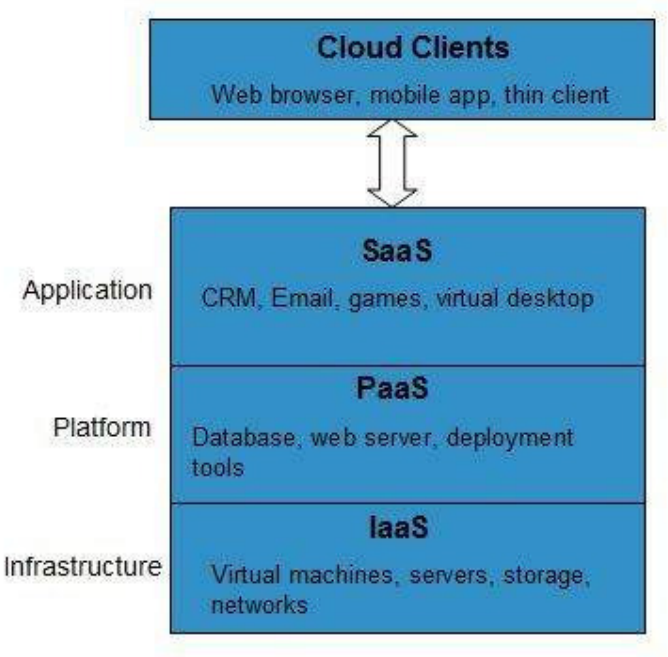
Infrastructure-as-a-Service *IaaS*

IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

Platform-as-a-Service *PaaS*PaaS provides the runtime environment for applications, development and deployment tools, etc.

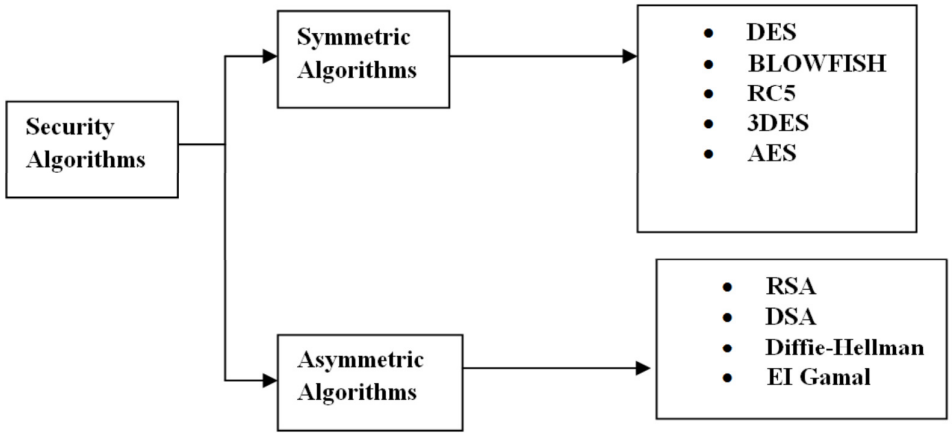
Software-as-a-Service *SaaS*

SaaS model provides the software applicationsto be used as a service to end-users.



Data security:

The major concern of cloud computing is securing the data. Encryption algorithm provides secure communication over the network. Encryption is used to converting a plaintext message into meaningless ciphertext which can be decrypted back into the original message.
There are two types of encryption algorithms they are Symmetric Encryption and Asymmetric Encryption In Symmetric key encryption, only one key is used to encrypt and decrypt the data. in asymmetric encryption two keys are used one is private and another is public key .For encryption , public key is used and for decryption private key is used .



SYMMETRIC ALGORITHM:

In symmetric encryption algorithm, same algorithm is used for both encryption and decryption and same key are used to both encipher and decipher the message. At both ends , private key is used to encrypt and decrypt the message. Symmetric encryption key method is extremely fast and efficient for processing encrypts and decrypt message. It provides confidentiality, integrity and availability but it fails to provide authenticity and non-repudiation

ASYMMETRIC ALGORITHM

In an **asymmetric** key encryption scheme, two keys are used .one is private key and another public key. Anyone can encrypt messages using the public key, but only the holder of the paired private key can decrypt.

Existing algorithm for cloud security

DES:(Data Encryption Standard)

The Data Encryption Standard (DES) is an outdated and earlier used symmetric algorithm for encryption. To encrypt and decrypt a message DES use the same key, so same private key is must known by both sender and receiver. Once the go-to, symmetric-key algorithm for the encryption of electronic data, Advanced Encryption Standard (AES) is the most secure model in which it suppressed the DES. DES takes on input a **64-bit plaintext** data block and **56-bit key** (with 8 bits of parity) and outputs a **64-bit cipher text block**. Since that time, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher

RSA

RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret.

DISADVANTAGE OF EXISTING SYSTEM

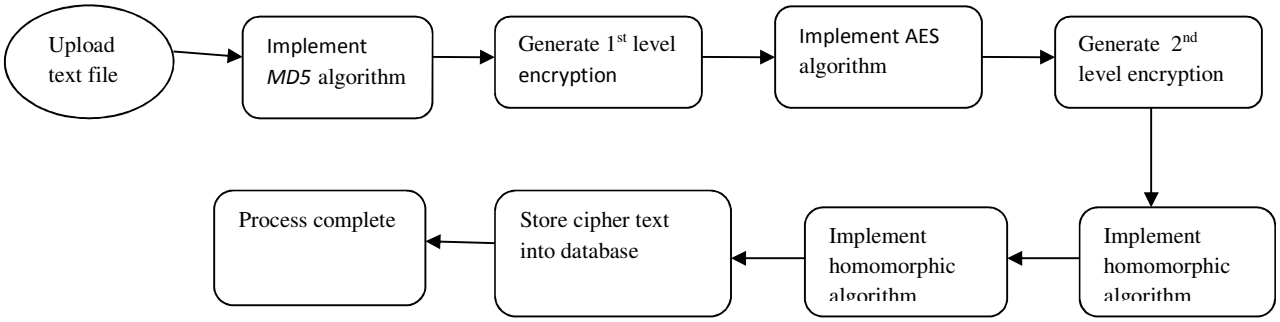
- The 56-bit key size is the biggest defect of DES. Chips to perform one million of DES encrypt or decrypt operations a second are available (in 1993). A $1 million DES cracking machine can search the entire keyspace in about 7 hours.
- Hardware implementations of DES are very fast; DES was not designed for software and hence runs relatively slowly.
- The main disadvantage of DES is the Key size because the key size is only 56 bits and this DES can be vulnerable to attacks and they can break the Key by Brute force attack.
- Triple DES runs three times slower than DES
- Public-key cryptography may be vulnerable to impersonation, even if users' private keys are not available. Public-key cryptography is usually not necessary in a single-user environment

- ***Proposed System Design.*** The proposed system is designed to maintain security of text files only. This proposed system uses multilevel security systems using MD5, AES,homomorphic algorithm to generate encryption when user uploaded the text files in Cloud Storage and inverse homomorphic ,MD5,AES algorithm to generate decryption when user download file from Cloud Storage, for increasing security. The proposed system is designed to maintain security of text files only. The proposed system design focuses on the following objectives which are helpful in increasing the security of data storage.

1) For Encryption of text files:

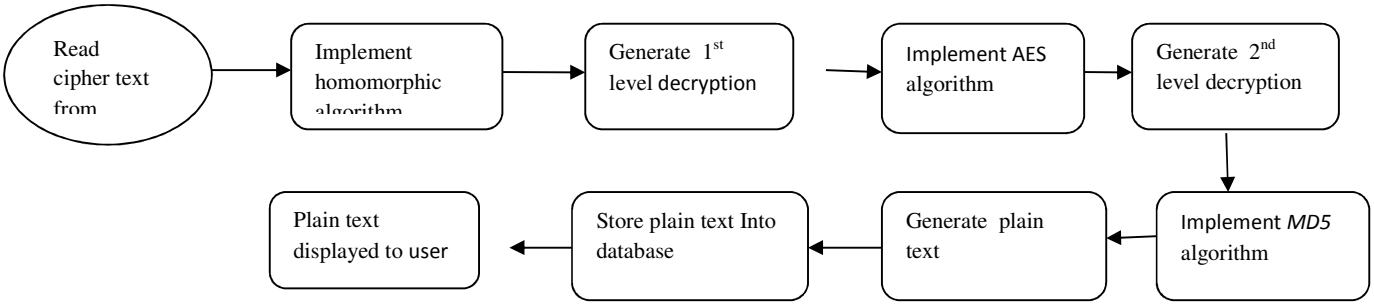
- Upload Text file.
- Implementing the MD5algorithm of Encryption to generate first level encryption.
- Implementing the AES algorithm of Encryption to generate second level encryption.

Implementing the homomorphic algorithm of Encryption to generate third level encryption
Store Cipher Text into Database



2) For Decryption of text files:

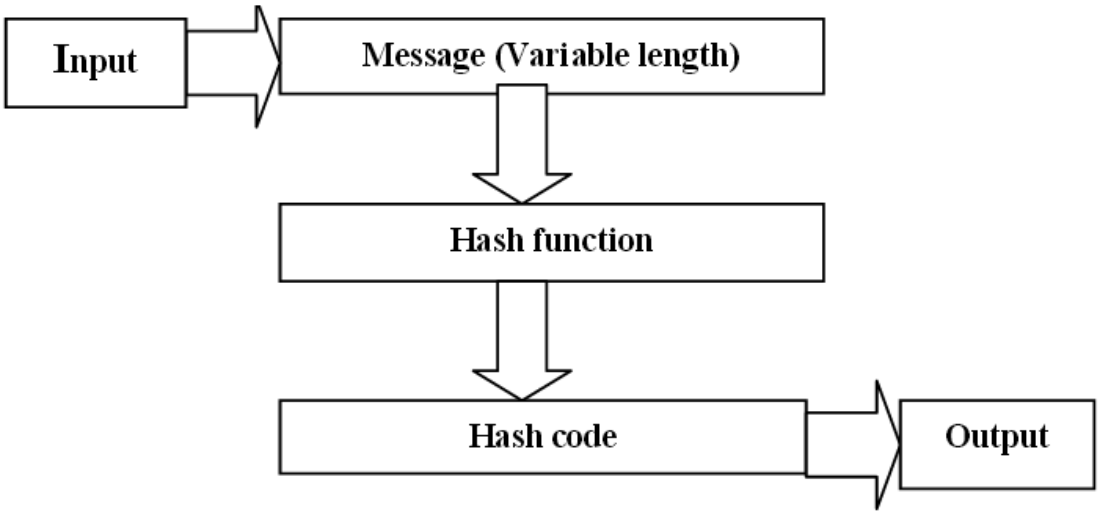
Read Cipher Text from Database.
Implementing the homomorphic algorithm of decryption to generate third level encryption
Implementing the AES algorithm Decryption to generate first level decryption.
Implementing the MD algorithm of Decryption to generate Plain text.
Display Plain Text to User



We have proposed a combination of three different security algorithms to eliminate the security challenges of Personal Cloud Storage. We have taken a combination of algorithms like: MD5, AES and homomorphic. By using these multilevel security system data should be highly secure and brute force attack is not possible it is unbreakable because of using AES algorithm. Speed is also increased because of hash functions(MD5).

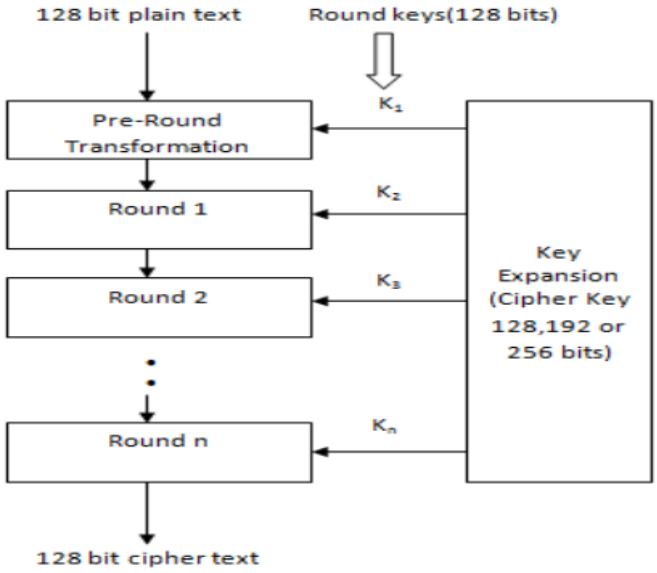
MD5 (Message-Digest algorithm 5),

It is widely used cryptographic hash function with a 128-bit hash value, processes avariable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks .the message is padded so that its length is divisible by 512. In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message..



AES: (Advanced Encryption Standard)

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively .Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. AES algorithm ensures that the hash code is encrypted in a highly secure manner



HOMOMORPHIC

Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption),the client is the only holder of the secret key. It provide the results of calculations on encrypted data without knowing the raw entries on which the

calculation was carried out respecting the confidentiality of data.

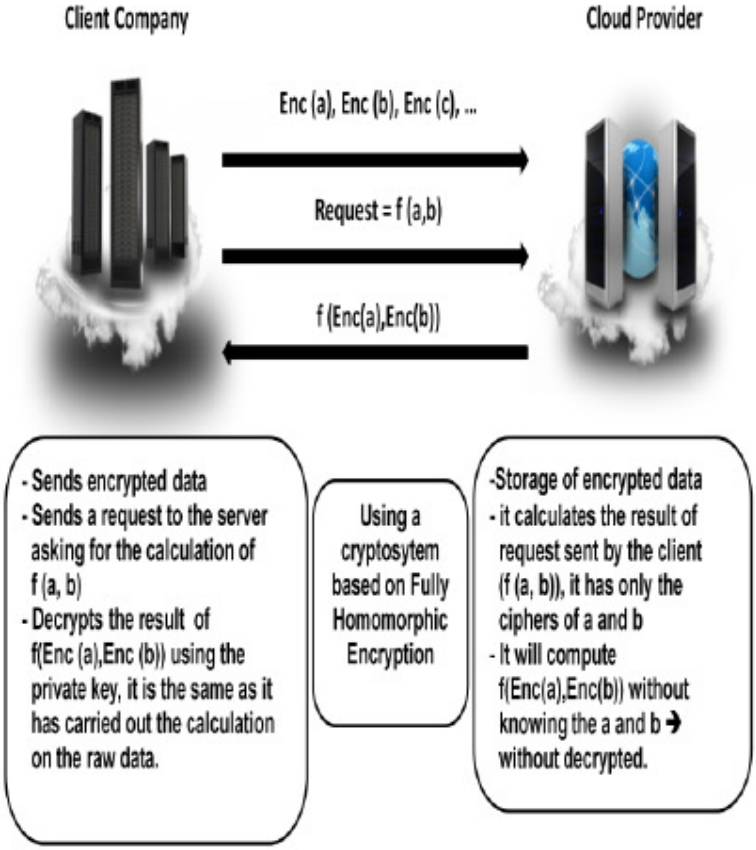


Fig. 3. Homomorphic Encryption applied to the Cloud Computing

PROPOSED SYSTEM ADVANTAGES

By using these multilevel security system data should be highly secure and brute force attack is not possible it is unbreakable because of using AES algorithm. Speed is also increased because of hash functions (MD5) Homomorphic encryption in and of itself solves the problem of computation on encrypted data.

II. CONCLUSION

Existing system use only public key systems .It greatly reduces the speed and security level. so to solve this problem we proposed the multilevel Encryption and decryption algorithms. Thus, in our proposed algorithm combine public- and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. Such a protocol is called a *digital envelope*. Thus, in our proposed work, only the authorized user can access the data. For encryption Even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is expected that using multilevel encryption will provide more security for Cloud Storage than using only public key encryption.

References

[1] L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security & Privacy Magazine, vol. 7, pp. 61-64, July2009.

[2] Puneet Jai Kaur, Sakshi Kaushal, "Security Concerns in Cloud Computing", Communication in Computer and Information Science Volume169, pp.103-112, 2011.

[3] Pearson, S., Benameur, A., Privacy, "Security and Trust Issues Arises from Cloud Computing", Cloud Computing Technology and Science(CloudCom), IEEE Second International Conference, pp.693-702, 2010.

[4] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[5] Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp. 571-575

[6] RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "Design of Privacy-Preserving Cloud Storage Framework" 2010 Ninth International Conference on Grid and Cloud Computing.

[7] WiebBosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. J. Symbolic Comput., 24(3-4): 235-265, 1997. Computational algebra and number theory, London, 1993.

[8] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[9] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[10] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010

