Applying Encryption Algorithm to Enhance Data Security in Cloud Storage

Zaid KARTIT, Mohamed EL MARRAKI

***Abstract*—Cloud computing is the concept implemented to remedy the Daily Computing Problems. Cloud computing is basically virtual pool of resources and it provides these resources to users via internet. It offers a range of services for end users; among which there's Storage as a service. In recent years, Storage in Cloud gained popularity among both companies and private users. However, data privacy, security, reliability and interoperability issues still have to be adequately solved. But the most important problem is security and how cloud provider assures it. In this paper, we have proposed a simple, secure, and privacy-preserving architecture for inter-Cloud data sharing. This architecture is based on an encryption/decryption algorithm which aims to protect the data stored in the cloud from the unauthorized access.**

***Index Terms*— AES, Cloud Storage, cryptography, Data security, Decryption, Encryption, RSA**

I. Introduction

CLOUD computing is a "new" computer model that allows using remote services through a network using various resources. It is basically meant to give the maximum capacity with the minimum resources. The end user has the minimum hardware requirement, but he uses the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way. Cloud Computing provides IT services as on-demand services, accessible from anywhere, anytime and by authorized user.

Recently Storage as a service (STaaS) Cloud gained popularity both among private users and companies [1]. STaaS is a Cloud business model in which a service provider rents space in its storage infrastructure to individuals or companies. The data stored in the cloud can be sensitive to the business. The problematic is that these data are likely to be exploited by the provider or other unauthorized persons. Currently, the most of users of cloud storage protect their data with SLAs contracts and are based on the trust and reputation of the provider. This weakness has motivated us to think about solutions that enable users to secure their data to prevent malicious use.

Zaid KARTIT, Laboratory of Research in Informatics and Telecommunication (LRIT), University of Mohammed V, Faculty of Sciences, Rabat, Morocco, (e-mail: z_kartit@yahoo.fr).

Mohamed EL MARRAKI is with Laboratory of Research in Informatics and Telecommunication (LRIT), University of Mohammed V, Faculty of Sciences, Rabat, Morocco, (e-mail: elmarrakimohamed@gmail.com).

Despite the strengths that represent cloud computing generally and cloud storage specially; there are a number of research challenges such as mobility, interoperability, storage access [3], security, cost, energy efficiency, etc.

Security is a major obstacle limiting its spread. There are various opinions on the security of cloud computing which deal with the positives and negatives of it [2].

This document is presented as follows: Firstly, it gives a comprehensive definition and the characteristics of cloud computing. Secondly, it describes layers and their technologies related to this concept. Thirdly, it describes the different types of cloud computing and their characteristics. Fourthly, it describes our model proposed of securing data in cloud storage algorithm for encryption/decryption for outsourcing data in cloud storage and then the general conclusion.

II. About Cloud Computing

A. Definition

Cloud Computing is an important concept in computer development in recent years. This concept refers to the use of computing capacity and storage of computers and servers in the world over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

B. Essential Characteristics

Cloud model promotes availability and is composed of five essential characteristics[4]:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as email, applications, and network or server service, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth.

Elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

III. LAYERS OF CLOUD COMPUTING

There are different layers of cloud services that refer to different types of *service model*, each offering discrete capabilities. Apart from management and administration, the major layers are[2]:

A. Infrastructure as a Service (IaaS)

Infrastructure as a service delivers computing resources as a service, servers, network devices, and storage disks are made available to organizations as services on a need-to basis.

Virtualization, allows IaaS providers to offer almost unlimited instances of servers to clients, while making cost-effective use of the hosting hardware.

Companies can use IaaS to build new versions of applications or environments without having to invest in physical IT assets. Some cloud solutions also rely solely on this layer like the Amazon's product EC2, Amazon S3.

B. Platform as a Service (PaaS)

This layer provides a platform for creating applications. PaaS solutions are essentially development platforms for which the development tool itself is hosted in the Cloud and accessed through internet. With PaaS, developers can build Web applications without installing any tools on their computers and then deploy those applications without any specialized systems administration skills.

Examples include Google App Engine, Force.com and Microsoft Azure.

C. Software as a Service (SaaS)

This layer includes applications that run off the Cloud and are available on demand to Web and paid for on a per-use basis, anytime-anywhere basis. There is no need to install and run the special software on your computer if you use the SaaS. A more efficient form is fine grained multi-tenancy [5].

The concept of SaaS is attractive and some software runs well as cloud computing, but the delay of network is fatal to real time or half real time applications such as 3D online game [6]. Examples include online word processing and spreadsheet tools, customer relationship management (CRM) services and web content delivery services (Salesforce CRM, Google Docs, etc.). These three are the main layers, although there can also be other forms of service provided, such as business process as a service, data as a service, security as a service, storage as a service (object of our paper), etc.

IV. CLOUD DEPLOYMENTS MODELS

A. Private Cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. Only the organization and designated stakeholders may have access to operate on a specific Private cloud [7].

B. Public cloud

A public cloud is a model which allows users access to the services and infrastructure and are provided off-site over the Internet [8]. It's typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are managed by third parties or vendors over the Internet. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks. However, security and governance issues must be well planned and ample security controls was put in place.

C. Hybrid cloud

A new concept combining resources from both internal and external providers will become the most popular choice for enterprises. A hybrid cloud is a combination of public and private cloud models that tries to address the limitations of each approach. In a hybrid cloud, part of the service infrastructure runs in private clouds while the remaining part runs in public clouds. Hybrid clouds offer more flexibility than both public and private clouds. Specifically, they provide tighter control and security over application data compared to public clouds, while still facilitating on-demand service expansion and contraction. On the down side, designing a hybrid cloud requires carefully determining the best split between public and private cloud components [9].

D. Community cloud

This model is rarely offered; the infrastructure is shared by several organizations for a shared cause and may be managed internally or a third party service provider. It brings together, in general, the structures with same interest (mostly security) and may even be in the same field of activity [10].

V. SECURITY

Security in cloud computing involves concepts such as network security, equipment and control strategies deployed to protect data, applications and infrastructure associated with cloud computing. An important aspect of cloud is the notion of interconnection with various materials which makes it difficult and necessary securing these environments. Security issues in a cloud platform can lead to economic loss, also a bad reputation if the platform is oriented large public and are the cause behind the massive adoption of this new solution. The data stored in the cloud for customers represents vital information. This is why the infringement of such data by an unauthorized third party is unacceptable. There are two ways to attack data in Cloud. One is outsider attack and the other is insider attack. The insider is an administrator who can have the possibility to hack the user's data. The insider attack is very difficult to be identified. So the users should be very careful while storing their data in cloud storage. Hence, the need to think of methods that impede the use of data even though the data is accessed by the third party, he shouldn't get the actual data. So, all the data must be encrypted before it is transmitted to the cloud storage [11].

Security allows the confidentiality, integrity, authenticity and availability of information. The development of technologies and their standardization makes available a set of algorithms and protocols for responding to these issues.

A. ASYMMETRIC ENCRYPTION

Asymmetric cryptography is a class of cryptographic algorithms which requires two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt cipher text or to create a digital signature. In our paper we used RSA algorithm through its robustness.

RSA Algorithm

The most common Public Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adelman of MIT. RSA is basically an asymmetric encryption/decryption algorithm. Public key distributed to all through which one can encrypt the message and private key which is used for decryption is kept secret and is not shared to everyone. It based on exponentiation in a finite field over integers modulo a prime numbers.

RSA uses Euler's Theorem: $a^{\emptyset(n)} mod(n) = 1$ where $gcd(a,n)=1$ in RSA we have to initially calculate $n=p.q$ such that $\emptyset(n)=(p-1)(q-1)$ one has to carefully chose e and d to be inverses $mod\ \emptyset(n)$.

To encrypt a message M we have to obtain public key of recipient $Pu=\{n,e\}$ to calculate the cipher: $C=M^e mod(n)$, where $0 \leq M < n$. It is important that the message M must be smaller than the modulus n. Similarly for decryption the recipient uses their private key $Pr=\{n,d\}$ and computes: $M=C^d mod(n)$.

Fig 1 shows the graph of RSA decryption time by key length.

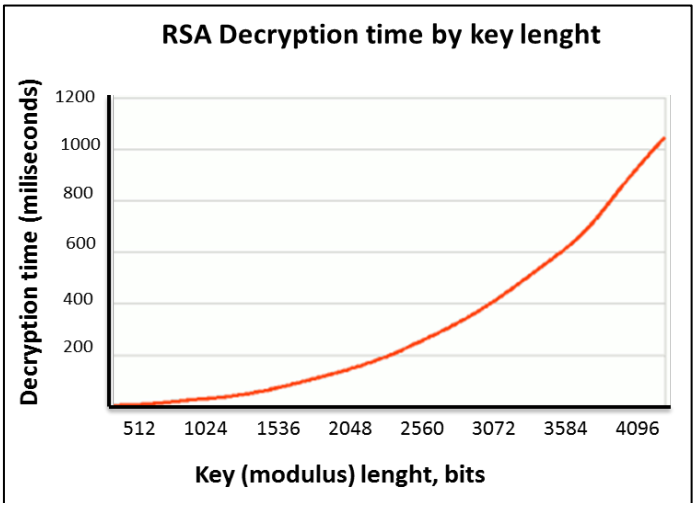

Fig 1: RSA decryption time by key length

B. SYMMETRIC ENCRYPTION

Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

AES Algorithm

AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. The key size used for an AES cipher specifies the number of repetitions of transformations rounds. The number of cycles of repetition is as follows (see fig 2):

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

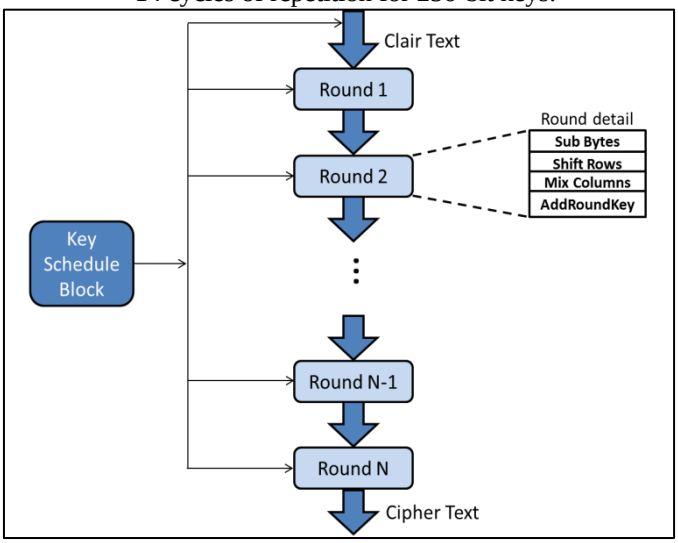

Fig 2: Illustration of the AES Algorithm

The advantages of AES are many. AES is not susceptible to any attack but Brute Force attack. However, Brute Force attack is not an easy job even for a super computer. This is because the encryption key size used by AES algorithm is of the order 128, 192 or 256 bits which results in billions of permutations and combinations. High speed [12] and low RAM requirements were criteria of the AES selection process. Thus AES performs well on a wide variety of hardware; from 8-bit smart cards to high-performance computers. AES is also much faster than the traditional algorithms; therefore in our work AES is adopted [15]. Recently Compact AES S-box is developed to be more efficient [16].

C. Related work

Security storage in cloud computing has been the object of several researches. In [13], they have addressed the security issues associated in cloud data storage and have explored many of them. Whenever a data vulnerability is perceived during the storage process, a precision verification across the distributed servers are ensured by simultaneous identification of the misbehaving nodes through analysis in term of security malfunctioning. It is proved that their scheme is effective to handle certain failures, malicious data modification attack, and even server colluding attacks.

In [13], the proposed technique emphasizes classical encryption techniques by integrating substitution cipher and transposition cipher. Both substitution and transposition techniques have used alphabet for cipher text.

In [14], it suggests the SPKS scheme for cloud storage services to allow users to efficiently access files containing certain keywords in a cloud anytime and anywhere using any device.

VI. PROPOSED ALGORITHM

The above problems motivate us to provide a correct, safe and efficient algorithm for securing data saved in cloud storage. This algorithm suggests the encryption of the files to be uploaded on the cloud. The integrity and confidentiality of the data uploaded by the user is ensured doubly by not only encrypting it but also providing access to the data only on successful authentication. The existed file on the device will be encrypted using AES algorithm. To enhance security; AES key will be encrypted using RSA algorithm and will be stored in intern server. The authorized user can also download any of the uploaded encrypted files and read it on the system (see Fig 3).

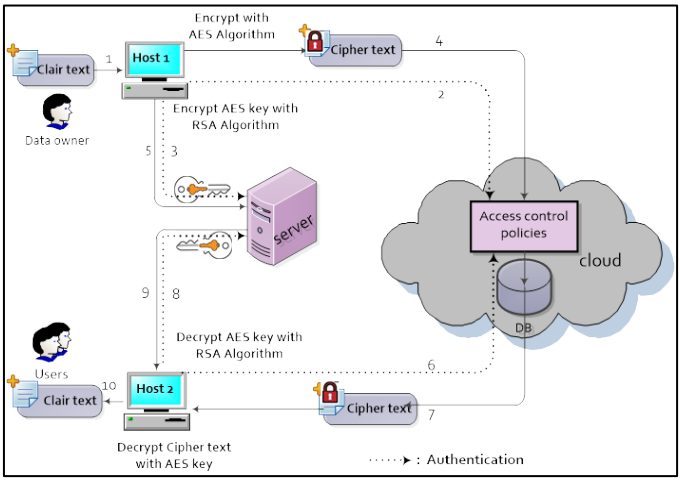

Fig 3: Model proposed of data storage in cloud computing

A. File Upload

This algorithm got two phases. In the first phase, the algorithm encrypts Clair text with AES Algorithm. In the second phase, we encrypt AES key using RSA-1024 algorithm.

Our algorithm uses a set of the following functions:

NumberOfBlock(F) : It returns the number of block in the file F.
ENC_AES (B,K) : It encrypts the block B using AES Algorithm with key K.
send_to_cloud(F') : It permits to send the encrypted file F in Cloud storage
ENC_RSA(k) : It encrypts k using RSA Algorithm.
Save_in_server(K') : It permits to save K' in the server

Algorithm 1.0: FILE_UPLOAD

```
1. Encrypt_file (F) {
2. /* algorithm to encrypt file onto cloud storage */
3. /* to transform Clair text in file F into Cipher text in file F' */
4.
5. /* Phase 1: Encrypt Clair text with AES Algorithm 6. */
7. for B←1 to numberOfBlock(F) do
8.   {
9.      B'=ENC_AES(B,K)
10.  }
11. send_to_cloud(F')
12. /* Phase 2: Encrypt AES key with RSA Algrithm */
13. for k←1 to SizeOf(K) do
14.   {
15.     k'=ENC_RSA(k)
16.   }.
17.  Save_in_server(K')
18. }.
```

B. File Download

This algorithm got also two phases. in the first phase, the algorithm decrypts AES key using RSA Algorithm. In the second phase, it decrypts cipher text using AES key retrieved from the server.

Our algorithm uses a set of the following functions:

NumberOfBlock(F) : It returns the number of block in the file F.
DEC_RSA(k') : It decrypts k' using RSA Algorithm.
DEC_AES(B',K) : It decrypts the block B' using AES Algorithm with key K.

Algorithm 1.0: FILE_DOWNLOAD

```
1. Decrypt_file (F') {
2. /* algorithm to decrypt file downloaded from cloud storage
*/
3. /* to transform Cipher text in file F' into Clair text in file F
*/
4.
5. /* Phase 1: Decrypt AES Key with RSA Algorithm */
6.
7. for k'←1 to SizeOf(K') do
8.      {
9.          k=DEC_RSA(k')
10.     }
11.  return(K)
12.
13. /* Phase 2: Decrypt Cipher text with AES Algorithm */
14. for B'←1 to numberOfBlock(F')  do
15.     {
16.         B=DEC_AES(B',K)
17.     }.
18.  return(F)
19. }.
```

C. Implement results and analysis

The implementation of results in this section highlights the time of execution in upload and in download of files with different sizes. Our application is developed in java 7.

The result obtained is in table 1 and Fig 6 using a PC hp Compaq dc 5800 with the following specifications: Intel (R) Core (TM) 2 Duo CPU E6550 @ 2.33GHz (2 CPUs), with 3072MB of RAM. The download time is greater than the upload time. This is explained by the addition of key recovery time on server.

Table I
EXECUTION TIME FOR ENCRYPTION AND DECRYPTION

File size (Kb)	128	256	512	1024	2048
Time in Upload (second)	0,2025	0,4051	0,8118	1,6201	3,2903
Time in download (second)	0,4225	0,8452	1,6905	3,3802	6,7711

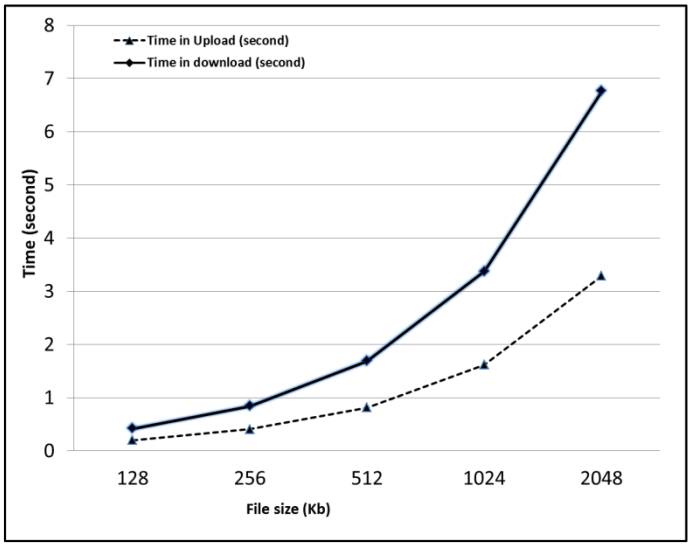

Fig 6: Graph of time execution of our algorithm

Fig 7 and Table 2 show the execution time required by different size text files and different AES key size for encryption process.

Table II
EXECUTION TIME BY FILE SIZE AND SIZE OF THE AES KEY

File size / Key size	128	256	512	1024	2048
128	0,198	0,397	0,794	1,587	3,1744
192	0,224	0,448	0,896	1,792	3,584
256	0,25	0,499	0,998	1,997	3,9936

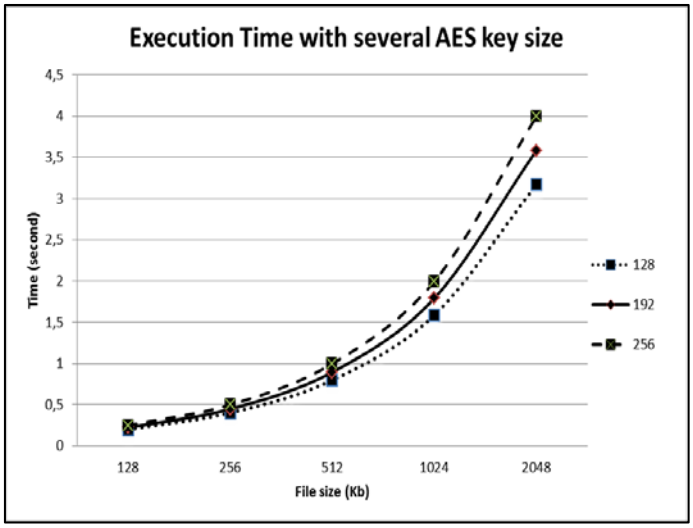

Fig 7: Graph of encryption time execution of our algorithm with different AES key size

Our algorithm has the following advantages and strengths:

- The data sent to cloud is encrypted from the source machine to the destination machine and the decryption key does not exist in the cloud.
- AES algorithm used is a safe, fast symmetric algorithm and is one of the most secure encryption algorithms. It has not been broken to date. It means that our algorithm is fast in both directions: upload and download.
- Ability to change the symmetric key frequently to enhance security.
- The AES key used for encryption of the data is encrypted by RSA-1024 algorithm robust and has never been broken.
- The decryption of data requires double authentication. The user must have access rights to the company's server and cloud storage.

VII. CONCLUSION AND FUTURE WORK

Although Cloud storage has many advantages, there are still many actual problems concerning security that need to be solved. If we can eliminate or master this weakness of security, the future is going to be Cloud storage solutions for large as well as small companies.

In this paper, we have suggested a solution that allows storage of data in an open cloud. Data security is provided by implementing our algorithm. Only the authorized user can access the data. Even if an intruder (unauthorized user) gets the data accidentally or intentionally, he can't decrypt it and needs two keys coming from two different locations. As perspectives, we will focus on several possible directions in this area, especially in the homomorphic encryption

REFRENCES

[1] KOLODNER, Elliot K., TAL, Sivan, KYRIAZIS, Dimosthenis, et al. A cloud environment for data-intensive storage services. In : Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on. IEEE, 2011. p. 357-366.

[2] P. Arora, R. C. Wadhawan, and E. S. P. Ahuja, « Cloud Computing Security Issues in Infrastructure as a Service », Int. J. Adv. Res. Comput. Sci. So*ftw. Eng.*, vol. 2, n° 1, 2012.

[3] M. D. K. Kumar, G. V. Rao, and G. S. Rao, « Cloud Computing: An Analysis of Its Challenges & Cloud Computing: An Analysis of Its Challenges & Security Issues ».

[4] N. Mehta and V. K. Gupta, « A Survey on Use of SaaS of Cloud in Education ». *International Conference on Cloud, Big Data and Trust 2013*

[5] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong «The Characteristics of Cloud Computing» *39th International Conference on Parallel Processing Workshops 2010*

[6] BEZEMER, C.-P., ZAIDMAN, Andy, PLATZBEECKER, Bart, et al. Enabling multi-tenancy: An industrial experience report. In : Software Maintenance (ICSM), 2010 IEEE International Conference on. IEEE, 2010. p. 1-8.

[7] H. KAMAL IDRISSI, A. KARTIT, M. EL MARRAKI «FOREMOST SECURITY APPREHENSIONS IN CLOUD COMPUTING » *Journal of Theoretical and Applied Information Technology 31 st January 2014. Vol. 59 No.3*

[8] Kuyoro S. O, Ibikunle F. & Awodele O « Cloud Computing Security Issues and Challenges » *International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011*

[9] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gongng « The Characteristics of Cloud Computing » *2010 39th International Conference on Parallel Processing Workshopse Brazilian Computer Society 2010*

[10] SO, Kuyoro. Cloud computing security issues andchallenges. International Journal of Computer Networks, 2011, vol. 3, no 5.

[11] L. Arockiam, S. Monikandan « Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm » *International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013*

[12] http://en.wikipedia.org/wiki/AES_implementations : This web site gives various implementations of the Advanced Encryption Standard, and also AES speed at 128, 192 and 256-bit key sizes.

[13] Cong Wang, Qian Wang and Kui Ren,"Ensuring Data Storage Security in Cloud computing"978-1- 4244 -3876-1/2009 IEEE

[14] LIU, Qin, WANG, Guojun, et WU, Jie. Secure and privacy preserving keyword searching for cloud storage services. Journal of network and computer applications, 2012, vol. 35, no 3, p. 927-933.

[15] NAGENDRA, M. et SEKHAR, M. Chandra. Performance Improvement of Advanced Encryption Algorithm using Parallel Imputation. International Journal of Software Engineering and Its Applications, 2014, vol. 8, no 2, p. 287-296.

[16] Xiaoqiang ZHANG, Ning WU, Gaizhen YAN, and Liling DONG, "Hardware Implementation of Compact AES S-box," IAENG International Journal of Computer Science, vol. 42, no.2, pp125-131, 2015