International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 02 – Issue 12 || December 2017 || PP. 62-65

# A Survey on Various Cryptographic Algorithms

**Ms. L.Archana[1], Mr. K.P.K.Devan[2]**
[1]*PG Student/CSE*
*Easwari Engineering College, Tamil Nadu, Chennai.*
[2]*Associate Professor/CSE*
*Easwari Engineering College, Tamil Nadu, Chennai.*

**Abstract:** Cloud computing has seized its impact in many sectors and subsectors. More data's can be stored via outsourcing the data's to remote cloud servers. Securing the stack-piled data's, over the large cloud is a real challenge. There are many emerging algorithms at present to ensure storage and security. This paper surveys on the efficiency of various cryptographic algorithms that ensures the former in our proposed system.
**Keywords:** Cloud Computing, Cloud Service Provider, Cryptography, Storage, Security

## 1. Introduction

Cloud computing is a paradigm, a model to facilitate prevalent access to pools of configurable resources (such as computer networks, servers, storage, applications and services).Overall consistency and efficiency can be ensured by cloud, that allows various owners and users with varying capabilities to store and process datasets via privately possessed cloud or third party authentication.

The Service Models in cloud computing are
1. **Software as a Service (SaaS**)
2. **Platform as a Service (PaaS)**
3. **Infrastructure as a Service (IaaS).**

### 1.1. The Deployment Models in cloud computing are

**Private cloud**: The infrastructure is provided for the use of a single organization consisting of multiple consumers. It may be operated, owned and managed by a third party organization or both of them, and it may exist off or on premises.
**Community cloud:** The infrastructure is provided for the use of a specific community of consumers that Have shared concerns. It may be operated, owned and managed by one or more of the organizations in the community, a third party, or some combination of them, and it may exist of for on premises.
**Public cloud**: The infrastructure is provided for open use by the general public. It may be operated, owned and managed by academic, business or government organization, or combination of them.
**Hybrid cloud:** The infrastructure is the combination of private, public and community cloud. It may exist on & of premises. of cloud

### 1.1.2 Need for security

Security is now becoming a major concern. Data can be gathered through tapping wires, planting bugs in output devices, shifting through trash receptacles, monitoring electro-magnetic radiation, bribing key employees, inferring data point from other values, stealing, buying, bribing etc. There are various threats to data's especially while transferring them from one center to the other.

### 1.1.3 Few Common Threats In Cloud

- Data ownership and control
- Data loss
- Data breaches
- Malicious attack and abuse
- Insider threat
- Unauthorized access
- Denial of service attack
- Eaves dropping and wire tapping
- Protocol flaws
- Spoofing
- Confidentiality threats

- Integrity threats
- Complex attacks

## 2. Related Work Based on This Concept

### 2.1 A Proposed System Concept on Enhancing Encryption and Decryption Method for Cloud Computing:

Saakinaah Ali Pitchey, Wail Abdo Ali, Farida Ridzuan and Madihah Mohmad sandi [2],[10] suggest to introduce a support pattern for a cloud storage system where security and privacy is at the maximum concern. In proposed system they have tried to provide security for the files stored in USB,in which data may get lost if the USB device is lost. They have used waterfall model to design a system correctly and apply AES and RSA algorithm to provide security. But the major concern is, it doesn't detect the correct USB that would contain the keys for encryption and decryption.RSA can also be cracked inspite of its complexity. Better algorithm can be used.

### 2.2 An Efficient Algorithm For Data Security in Cloud Storage:

Ali Azougaghe, zaidkartit, Mustapha Hedabou, Mostafa Belkasmi,, Mohammed El Marakki[1], share their concept of inter-cloud data sharing using AES and Elgamel Cryptographic algorithm in proposed system to protect data from unauthorized users.AES performs well in wide variety of networks and produces high performance. It is much faster and not susceptible to many attacks. Elgamal algorithm is used to provide additional security but DDos attack is still being under research.

### 2.3 New Frame Work For Cloud Storage Confidentiality to Ensure Information Security:

Deepak singh and Harsh K Varma [5],[8], in order to overcome the difficulty of privacy ,Authentication and Integrity between user and CSP, they have adapted a new framework using AES,SHA-1 for security. It provides less computation power and time. Though AES and SHA-1 are both efficient that provides integrity and confidentiality, brute-force attack still remains a major concern.

### 2.4 Secure Cloud Storage Using AES Encryption:

Babitha.M.P and KR Ramesh Babu[3],[6] addresses different data security and privacy protection issues in cloud where provider is not a trusted one. They have used AES algorithm and SMS message alert mechanism if in case of security breach. They have divided the file into blocks and transferred them to cloud by encrypting data using AES algorithm in proposed system offering authentication, authorization and confidentiality. Also a comparison on AES, DES and RSA is made and AES is found to be more secure than the rest. Time delay in computation increases as the file size is increased hence this is under consideration.

### 2.5 Improving Database Security In Cloud Computing By Fragmentation of Data:

Amjad Alsirami, Peter Bodorick,Srinivas Sampalli[7],[2] have proposed a combination of encryption algorithms and distribution system to improve confidentiality.Pope et al says he has used AES-CBC algorithm for encryption and proxy server helps to retrieve the information via queries.Detailed study on Delays with many predicates AND,OR,WHERE can be done as future enhancement on fragmented data's as Analytical method can't be used to measure the data.

### 2.6 Enhancement In Homomorphic Encryption Scheme For Cloud Data

Samjot kaur and vikas wasson [8],[9] have focussed on Diffie Hellman algorithm.It creates a session key between twoparties who are communicating.Different attacks like SYN flood, malware injection,account hijacking are discussed.FHE is used as it is more reliable and secure.Propagation and other delays are to be considered in future enhancement.

### 2.7 Re-encryption security model over Outsourced Cloud data

Lizhi Xiong, Zhenquan xu proposes re-encryption technique, for providing security. A piece of data is encrypted twice using different keys and final cipher text is progressive elliptic curve algorithm is used in this paper. Usage of single algorithm twice causes complexity in key usage. Hence different algorithms can be used. Data backup, error detection, and data recovery, privacy, integrity and availability is ensured. Inspite of this still collision attack still remains.

### 2.8 Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud

Dr. D.I. George Amalarethinam and H. M. Leena proposed that RSA, an asymmetric key algorithm is the base for many combination algorithm. Random key generated increased security. In this paper Enhanced RSA technique is used where it differs from classical RSA, with the addition of two or more prime numbers. The computation time for encryption and decryption is less when compared to classical one. Data confidentiality, integrity and availability is ensured. But ERSA is less secured compared to many other algorithms.

## 3. Comparison table

Table 1: DES, AES, RSA comparison

| FEATURES | DES | AES | RSA |
|---|---|---|---|
| KEY LENGTH | 56 bits | 128,192,256 bits | More than 1024 bits |
| CIPHER TYPE | Symmetric block Cipher | Symmetric block Cipher | Asymmetric block Cipher |
| BLOCK SIZE | 64 bits | 128 bits | Minimum 512 bits |
| SECURITY | Medium | Excellent | Low |
| COMPUTATION TIME | Depends on block size | Depends on block size | Depends on block size |

## 4. Comparison Graph

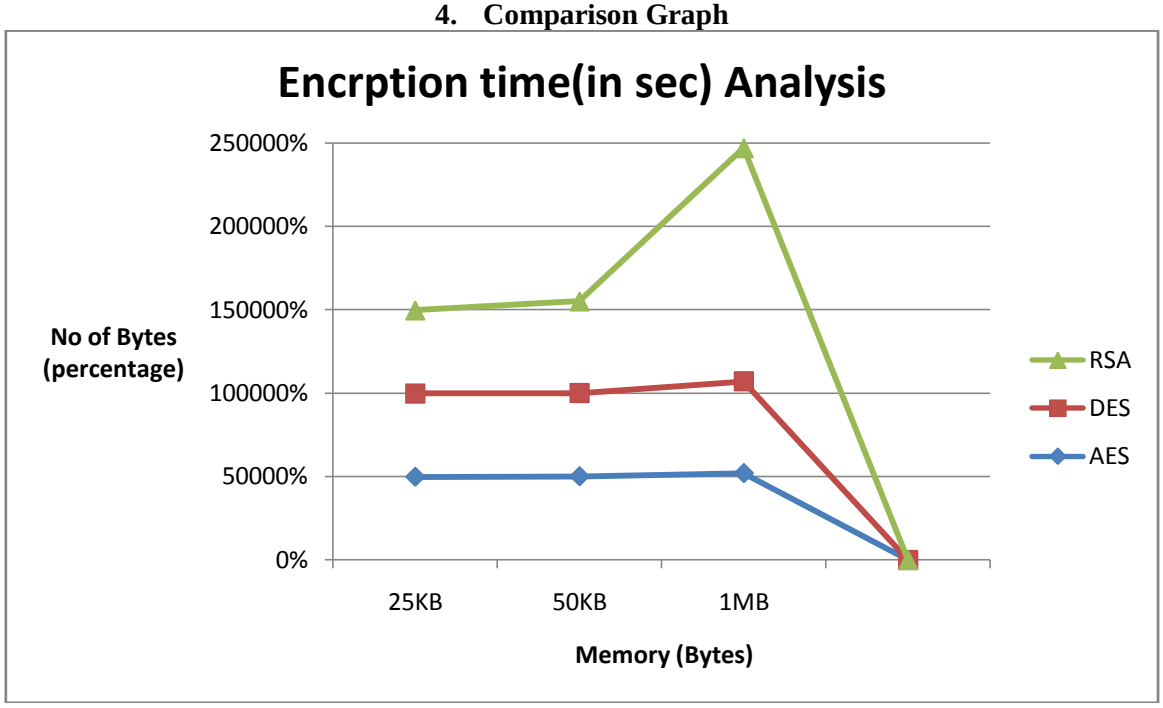


Figure 1: Comparative execution times (in seconds) of Encryption Algorithms in ECB mode on a P-II 266 MHz machine

## 5. Conclusion

In this paper we have made a comparison on various cryptographic algorithms and have found that AES (Advanced Encryption Standards) is more secure and the time of computation, for each algorithm varies according to the size of the file. It also throws a strong emphasize on the importance of security in cloud environment and how to make them more sophisticated for storage purpose. Hence we can conclude that a combination of AES and FHE(Fully Homomorphic Encryption) can be used, as computations on cipher text is eased by using FHE algorithm, providing added safety and stack-pile.

## References

[1] 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.

[2] T .Chou, ***"Security Threats on Cloud Computing Vulnerabilities***", International Journal of Computer Science and Information Technology, Vol 5(3),pp .79-88, 2013.

[3] Dr. A. M. Gonosai and L.M. Raval, ***"Evaluation of Common Encryption Algorithm and Scope of Advanced Algorithm for Simulated Wireless Network",*** International Journal of Computer Trends and Technology, Vol 11(1), pp. 7-12, May 2014.

[4] P.Mell, Grance***," The NIST definition of Cloud Computing***", NIST Special Publication, pp. 800-145, Sep 2011.

[5] Y. Pawar, P. Rewagad and N. Lodha***,"Comparative Analysis of PAVD Security System with Security Mechanism of Differenr Cloud Storage Services",***2014 Fourth International Conference on Communication Systems and Network Technologies, 2014.

[6] Prerna Mahajan,Abhishek Sachdena,***"A study of Encryption Algorithms AES,DES and RSA for Security"***,Global Journal of Computer Science and Technology Network web and Security,vol.13,Issue 15,Vol 1,2013.

[7] R.A.Popa ,C.M.S.Redfield, N.Zeldovich al,H.Balakrishnan, ***"CryptDB: Protecting Confidentiality with Encrypted Query Processing",***pp. 85-100, 2012.

[8] P.Rewagad and Y.Pawar***," Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing"***, 2013 International Conference on Communication Systems and Network Technologies, 2013.

[9] J.Viega***,"Cloud Computing and The Common Man",*** Journal Computer Vol 42(8), pp. 106-108, August 2009.

[10] K.Yang and J.Xiaohva, ***"Security for Cloud Storage Systems",*** Springer Brief in Computer Science, 2014.