



# EVOLVING CRYPTOGRAPHIC APPROACH FOR ENHANCING SECURITY OF RESOURCE CONSTRAINED MOBILE DEVICE OUTSOURCED DATA IN CLOUD COMPUTING

P NAGESWARA RAO, CH.BUCHI REDDY, EEDUNURI MURALIDHAR REDDY

4.G.SAMBA SIVA RAO, 5.MD.ANWAR ALI

Assistant Professor, Department of Computer Science Engineering,

Ellenki college of Engineering and Technology,,

**Abstract:** Mobile cloud computing in the increasing popularity among users of mobile device enables to store their data in cloud. Security is the major concern when the sensitive information is stored and transferred across the internet. It is essential to make sure that the data is secured and protected. In this paper, we discussed the problem of privacy of data with reducing the resources usage. Moreover, mobile cloud computing has limitations in resources such as power energy, processor, Memory and storage. Cryptography ensures the confidentiality, authentication, availability, and integrity of the data. This is done through cryptographic algorithms such as Data Encryption Standard (DES), Blowfish and Advanced Encryption Standard (AES). The experimental results evaluated and compared the performance of the encryption algorithms. The performance. metrics used are encryption and decryption time, CPU and Memory utilization. Evaluation results showed a significant improvement in

reducing the resources, amongst all the techniques, choosing a suitable encryption algorithm based on different parameters that are best fit to the future user requirements is considered.

**Keywords:** group Mobile Cloud Computing, Blowfish, AES, Security, Privacy, Mobile Device.

## I. INTRODUCTION

Mobile cloud computing uses cloud computing to carry out the resource intensive tasks over the internet to provide higher scope of functionality with minimal pressure on mobile resources. Cloud computing is a modern era computing technique that has a greater future and bringing a lot of benefit to the information technology. The major advantage of using cloud is that it offers the cloud services to people by Pay-as-You-Go manner. Cloud computing applies a virtualized platform with elastic resources on demand by provisioning hardware, software, and data sets dynamically.

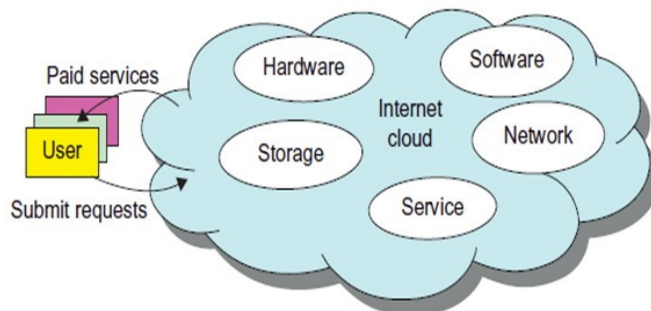


Figure1.1Cloud Environments

There are various layered architectures available for cloud computing to provide the

services as a utility. Cloud's backbone layer consists of physical servers and switches. The cloud service provider is responsible to run, manage, and upgrade cloud hardware resources according to the requirements of users. The backbone layer is also responsible to allocate hardware resources to users in an efficient, quick, and smooth way. The supervisor software layer contains the system software to manage the cloud hardware resources. The system software permits application software to run and utilize underlying resources in an efficient way. In the context of mobile cloud security, cloud providers should ensure reliability and availability by integrating security technologies. MCC satisfies limitations of resource constrained devices by allocating cloud services for the purpose of application executions and data storage. So, whenever we talk about the security in MCC, it is necessary to consider the security and privacy issues.

To secure the mobile cloud environment, several issues need to be considered regarding the data security, data integrity, data confidentiality, authentication, authorization, network security, data violation issues etc. A secure framework is essential to protect sensitive data of mobile users with minimal performance degradation. The proposed scheme uses data encryption to protect sensitive data leakage. When user's data is transmitted to and stored on cloud, it creates many possibilities of unauthorized access of data either during transmission or from storage devices. There are many cryptographic algorithms to deal with security, but the selection must be taken by considering security as well as performance improvement, especially in the case of resource constrained devices.

#### Triple DES

Taking over from the conventional DES mechanism, triple DES was currently implemented in the security approaches. These algorithms permit hackers to ultimately gain the knowledge to overcome in an easy approach. This was the extensively implemented approach by many of the enterprises. Triple DES operates with 3 keys having 56 bits per each key. The entire key length is a maximum of bits, whereas experts

would contend that 112-bits in key intensity is more probable. This algorithm handles to make a reliable hardware encryption answer for banking facilities and also for other industries.

#### Blowfish

To replace the approaches of Triple DES, Blowfish was mainly developed. This encryption algorithm split up messages into clocks having 64 bits and encrypts these clocks separately. The captivating feature that lies in Blowfish is its speed and efficacy. As this is an open algorithm for everyone, many gained the benefits of implementing this. Every scope of the IT domain ranging from software to e-commerce is making use of this algorithm as it shows extensive features for password protection. All these allow this algorithm to be most prominent in the market.

#### RSA

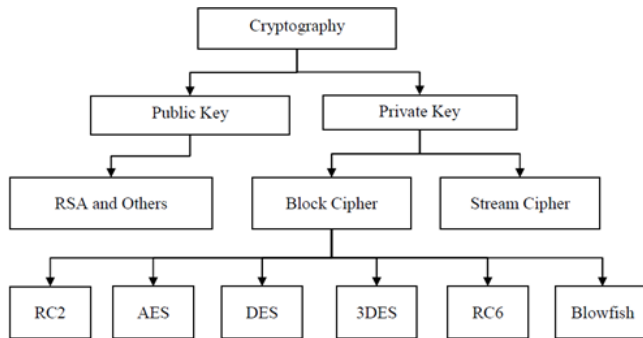
One of the public-key encryption algorithms used to encrypt information transmitted through the internet. It was a widely used algorithm in GPG and PGP methodologies. RSA is classified under symmetric type of algorithms as it performs its operation using a couple of keys. One of the keys is used for encryption and the other for decryption purposes.

#### Twofish

This algorithm implements keys to provide security and as it comes under the symmetric method, only one key is necessary. The keys of this algorithm are with the maximum length of 256 bits. Of the most available algorithms, Twofish is mainly known by its speed and perfect to be implemented both in the hardware and software applications. Also, it is an openly accessible algorithm and has been in execution by many.

**AES (Advanced Encryption Standard)** This is the most trusted algorithm technique by U.S administration and many other enterprises. Even though this works efficiently in 128-bit encryption form, 192 and 256 bits are mainly used for huge encryption activities. Being so invulnerable to all hacking systems, the AES technique receives extensive applause for encrypting information in the private domain.

Figure 2.1 Types of cryptographic algorithms



## SECURITY ISSUES

- **Data Storage:** Cloud storage providers manage the data in multiple copies across many independent locations
- **Confidentiality:** Confidentiality can be defined as the sensitive data not being disclosed to unauthorized process, devices and person. A cloud service provider knows where the user's public or private data is located and who can/cannot access the data. The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of a message.
- **Integrity:** The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender. It is defined as the rightness of data stored in the cloud. The alterations between two updates of a record violate the data integrity.
- **Security:** In the traditional file systems data was stored within boundaries, but cloud data is stored outside the boundaries of an organization, say, and third-party storage using strong encryption techniques.
- **Authentication:** Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.

- **Non- repudiation:** Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.
- **Access Control:** Access Control specifies and controls who can access the process.
- **Availability:** The principle of availability states that resources should be available to authorized parties all the times.

## CRYPTOGRAPHY

Cryptography is a method of protecting information and communications with codes so that only those for whom the information is intended can read and process it. Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher. Security has always been an important term in all the fields. As the paper is discussing on cloud storage systems, the proposed methodology considers the security required to the data that is stored on the cloud. Cryptography has come up as a solution to this security issue. Cryptography is classified into symmetric cryptography, asymmetric cryptography and hashing.

### Types of Cryptography

- **Secret Key Cryptography:** When the same key is used for both encryption and decryption, DES, Triple DES, AES, Blow Fish RC5 etc., may be the examples of

such encryption, then that mechanism is known as secret key cryptography.

- **Public Key Cryptography:** When two different keys are used, that is one key for encryption and another key for decryption, RSA, Elliptic Curve etc., may be the examples of such encryption, then that mechanism is known as public key cryptography.
- **Hash Algorithms** where the input data (message) is recreated from the hash value (message digest/digest) examples include: MD5, SHA, MD2, MD4, MD6.SHA- 256, SHA-512, SHA-1, Whirlpool etc.

**III. PROPOSED METHODOLOGY**

Data Encryption Standard (DES)

DES utilized the one secret key for encryption and decryption process and key length is 56 bits and performs the encryption of message using the 64 bits block size. It includes 64 bits key

that contains 56 bits are directly utilized by the algorithm as key bits and are randomly generated. The DES algorithm processes the 64 bits input with an initial permutation, 16 rounds of the key and the final permutation. The DES was initially considered as a strong algorithm, but today the large amount of data and short key length of DES limits its use.

Advanced Encryption Standard (AES)

The algorithm explains about by AES is a secret-key algorithm which means of the same key is used for both encrypting and decrypting the data. This is one reason why it has a comparably small number of rounds. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices. All the operations in this algorithm involve complete bytes for effective implementation. Three different key lengths such as 128, 192 and 256 block size are supported by AES.

Table 4.1 Comparison of Symmetric Algorithms

Algorithms/ Metrics	DES	AES	BLOWFISH
Structure	Feistel	Substitution- Permutation	Feistel
Key Length	56bits	32-448	128,192 or 256
Rounds	16	10,12,14	16
Block Size	64bits	128 bits/192 Or256	64bits
Through put	<AES	<Blowfish	High
Security	Adequate	Excellent	Excellent
Speed	Slow	Fast	Fast

Blowfish is fast, license free, unpatented, freely available and alternative for existing encryption algorithms. It uses the key length range up to 32-448- and 64-bits block. Blowfish algorithm employed 16 rounds for the encryption process. Each round contains a key dependent permutation and key- and data dependent substitution. Data Encryption involves the iteration of a simple function of 16 times. Each round contains a key dependent permutation and data dependent substitution. Sub key

Generation involves converts the key up to 448 bits long to 4168 bits. Blowfish is very suitable algorithm for the platform of smart phones because of its high security level and high speed.

**IV. PERFORMANCE EVALUATION METRICS CPU**

Time Calculation CPU Time = I \* CPI \* T, where I = number of instructions in program, CPI = average cycles per instruction and T =

clock cycle time.  $CPU\ Time = I * CPI / R$ , where  $R = 1/T$  the clock rate,  $T$  or  $R$  are usually published as performance measures for a processor,  $I$  requires special profiling software and  $CPI$  depends on many factors (including memory).

Performance Calculation

$Seconds/Program = (Instructions/Program) \times (Clocks/Instruction) \times (Seconds/Clock)$

Memory Consumption Calculation

$Total\ Memory - (Free + Buffers + Cached) =$  current total memory usage

## V. CONCLUSION

The demonstration of results and discussion about these algorithms are mainly focused on evaluation parameter like encryption and decryption time, memory and CPU utilization which has more impact on the security, confidentiality, integrity, and reliability for secure communication. Security as earlier discussed is the main challenge faced while storing data in the cloud, the proposed system provides security for the data stored in the cloud computing model. Based on the performance evaluation, the results of Blowfish, AES and DES provide more security based on the resources availability. In future we can use encryption techniques in such a way that it can consume less time and minimum energy consumption.

## VI. REFERENCES

- [1]. Gurpreet Kaur and Manish Mahajan (2013), Analyzing Data Security for Cloud Computing Using Cryptography Algorithms, International Journal of Engineering Research and Application, Vol.-3,782-786.
- [2]. Sujithra, M., G. Padmavathi, and Sathya Narayanan. Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile Data to Cloud. In: Procedia Computer Science 47; 2015.p. 480-485.
- [3]. Paresh D.Sharma, Prof. Hitesh Gupta(February 2014) An Implementation for Conserving Privacy based on Encryption

Process to Secured Cloud Computing Environment, IJESRT Sharma, 3(2).

- [4]. D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Evaluating the performance of symmetric encryption algorithms," International Journal of Computer Theory and Engineering, vol. 10, no. 3, pp. 343-351, 2009.
- [5]. M. Sujithra, and G. Padmavathi, "Ensuring Security on mobile device data with two phase RSA algorithms over cloud storage," Journal of Theoretical and Applied Information Technology, Vol.80. No.2 ISSN: 1992-8645, October 2015.
- [6]. HealeyM(2010) Why IT needs to push data sharing efforts. Information Week. Source: <http://www.informationweek.com/services/integration/why-it-needs-to-push-data-sharing-effort/225700544>. Accessed on Oct 2012
- [7]. D. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Performance evaluation of symmetric encryption algorithms," International Journal of Computer Science and Network Security, vol. 8, no. 12, pp. 280-286, 2008.
- [8]. Shanthni KK., Kaviya K and Sujithra M.2018, A Survey on Cloud Computing: Data Security Challenges and Their Defensive Mechanisms. Int J Recent Sci Res. 9(5), pp. 26497-26500. DOI: <http://dx.doi.org/10.24327/ijrsr.2018.0905.2070>
- [9]. D. Salama, A. Minaam, H. M. Abdulkader, and M. M. Hadhoud, "Evaluating the effects of symmetric cryptography algorithms on power consumption for different data types," International Journal of Network Security, vol. 11, no. 2, pp. 78-87, 2010.
- [10]. L. Krithikashree ; S. Manisha ; M. Sujithra, "Audit Cloud: Ensuring Data Integrity for Mobile Devices in Cloud Storage," Published in: 2018 9th International conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, DOI: 10.1109/ICCCNT.2018.8493963