AIJREAS VOLUME 6, ISSUE 2 (2021, FEB) (ISSN-2455-6300)ONLINE
Anveshana's International Journal of Research in Engineering and Applied Sciences

ADVANCED CRYPTOGRAPHIC APPROACH FOR IMPROVING SECURITY OF RESOURCE RESERVED MOBILE DEVICE OUTSOURCED DATA IN CLOUD COMPUTING

Dr. A.NANDA GOPAL REDDY,
HOD, Professor in The Department of Information Technology, Mahaveer Institute of Science and Technology, Bandlaguda, Hyderabad, India,
nandagopalreddy@gmail.com

D.SWATHI
Assistant professor, Department of Information Technology, Mahaveer Institute of Science and Technology, Bandlaguda, Hyderabad, India, swduggi@gmail.com

ABSTRACT

Mobile Cloud Computing in the increasing popularity among users of Mobile Devices to store their information in the cloud. Security is the major concern when the confidential information is stored and transferred across the internet. It is required to make sure that the data is secured and protected. The problem of privacy of data with reducing the resources usage. Moreover, Mobile Cloud Computing has limitations in assets such as power energy, processor, Memory and storage. Cryptography ensures the confidentiality, authentication, availability, and integrity of the information. This is can be achievable through cryptographic algorithms known as Data Encryption Standard, Blowfish and Advanced Encryption Standard. The experimental results evaluated against the performance of the Encryption Algorithm. CPU and Memory utilization are the primary metrics which can be helped while encryption and decryption time. 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 perfect match to the future user requirements is considered.

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

I. INTRODUCTION

Mobile cloud computing uses cloud IaaS to carry out the resource intensive tasks via internet to provide higher scope of functionality with minimal pressure on mobile resources. Cloud computing is a modern era computing technique that has an outstanding future and will become the vital benefit to the information technology. Pay-as-You-Go is the Principle Asset while using cloud computing. Cloud computing provides a virtual platform with flexible resources on demand by facilitating the required infrastructure.

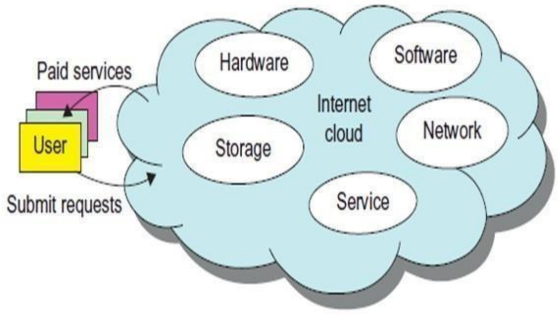

Figure 1.1 Cloud Environments

There are various layered architectures available for cloud computing to provide the services as a utility. Cloud's key layer accommodates physical servers and switches. The cloud service owner is accountable to run, manage, and upgrade cloud hardware resources according to the requirements of cloud customers. The backbone layer is also plays a crucial role while locating hardware resources to users in well-defined manner. The Primary software layer contains the system software to operate the cloud hardware resources. The software of the system permits application to run and utilize underlying resources in a systematic way. In the framework of mobile cloud security, cloud suppliers should make sure the benefit and core usage of reliability and availability by incorporating security technologies. MCC fulfils boundaries of resource constrained devices by facilitating cloud services for the benifit of application readiness and storage of Data. So, whenever we talk about the security in MCC, it is necessary to consider the fundamental benefit of security and privacy concerns.

To protect the mobile cloud environment, numerous topics need to undertake relating to the security of Data, integrity of the Data, confidentiality of data, user validation, user authorization, principle of network security, data violation issues etc. A secure framework should need which plays a vital role to protect confidential data of mobile clients with minimal impact of its performance degradation. The anticipated scheme uses its data encryption to guard the confidential data seepage. When user's data is transferring from source to destination and stored on cloud environment, it generates numerous possibilities of unlicensed access of data either during transmission or from storage devices. We have many cryptographic algorithms which can solve the security concerns, but the choice must be granted by considering security objectives as well as system performance improvement, especially in the case of resource constrained systems.

II. SECURITY ISSUES

- Data Storage: Cloud storage owners operates the data in multiple copies across many independent locations
- Confidentiality: Confidentiality can be demarcated as the sensitive data not being disclosed to unauthorized process, devices and person. A cloud service owner knows where the user's public or private data is located and who Can/cannot access the data. The thumb rule of confidentiality requires that only the source and the target recipient should be able to access the message content.
- Integrity: The integrity mechanism should make sure that the contents of the message will not change when it reaches the target recipient. It is define as the rightness of data stored in the cloud. The modifications between two updates of a record violate the data integrity.
- Security: In the traditional file systems storage of the data was within limitations, but cloud data is resides outside the boundaries of the company, say, and third-party storage using robust encryption techniques.
- Authentication: The Main characteristics of Authentication helps the project to create proof of user identities. This process ensures that the origin of the message is correctly identified.
- Non- repudiation: Objective of Non-repudiation should not allow the sender of a message to refute the claim of not sending the message.
- Access Control: Access Controls authenticate and authorize individuals to access the information they are allowed to see and use.
- Availability: The prototype of availability states that resources should be ready to authorized parties all the times.

III. CRYPTOGRAPHY

Cryptography is a way of protecting information and communications through the use of codes so that only those for whom the information is projected can read and process it. Cryptography refers to confident information and communication techniques derived from mathematical conceptions and a set of rule-based calculations called algorithms to convert messages in such a way that are tough to decipher. As the paper is deliberating on cloud storage systems, the planned methodology reflects the security is mandatory to the data that is stored on the cloud. Cryptography has derived a possible solution to eradicate this security issue as following. Cryptography is categorized as Symmetric cryptography Asymmetric cryptography Hashing Types of cryptography

- Secret Key Cryptography: is also called the symmetric cryptography because the same key is used for both encrypt and decrypt the data. Well known secret key cryptographic algorithms include Data Encryption Standard (DES), triple-strength DES (3DES), Rivest Cipher 2 (RC2), and Rivest Cipher 4 (RC4).
- Public Key Cryptography: When two non-identical keys are used, that is one key for encrypt 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 regenerated from the hash value (message digest/digest) examples as: MD5, SHA, MD2, MD4, MD6.SHA-256, SHA-512, SHA-1, Whirlpool etc.

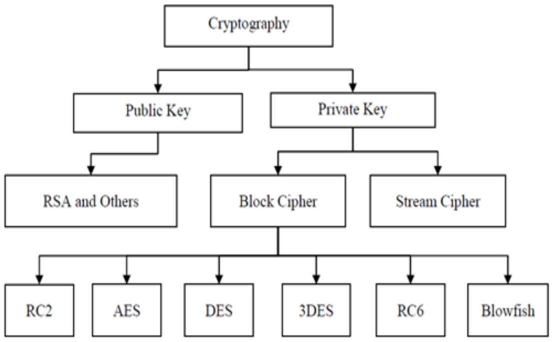

Figure 3.1 Types of cryptographic algorithms

IV. PROPOSED METHODOLOGY

Data Encryption Standard (DES)

DES utilized the one secret key for encryption and decryption procedure and length of the key is 56 bits and performs the encryption of message using the 64 bits Block size. It includes 64 bits key that comprises 56 bits are directly operated 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 describes about by AES is a secret- key algorithm which represents of the same key is used for both encrypting and decrypting the data. This is one root reason why it has a small number of rounds. AES encryption is fast and flexible. It can be applied smoothly on various platforms especially in small devices. All the operations in this algorithm involve complete bytes for effective implementation. Following are the Three different key lengths of block size are supported by AES.

128, 192 and 256

Table 4.1 Comparison of Symmetric Algorithms

Algorithms/ Metrics	**DES**	**AES**	**BLOWFISH**
Structure	Feistel	Substitution - Permutation	Feistel
Key Length	56 bits	32-448	128,192 or 256
Rounds	16	10, 12, 14	16
Block Size	64 bits	128 bits/192 0r 256	64 bits
Throughput	< AES	< Blowfish	High
Security	Adequate	Excellent	Excellent
Speed	Slow	Fast	Fast

Blowfish

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.

V. 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) x (Clocks/Instruction) x (Seconds/Clock)

Memory Consumption Calculation

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

Table 5.1. Experimental Results: Time Comparison

Algorithm	**File Size**	**Time Encryption (milliseconds)**	**Time Decryption (milliseconds)**
Blowfish	10 KB	300	299
	15 KB	303	304
	20 KB	310	310
	25 KB	315	313
	30 KB	320	317

AES	10 KB	303	303
	15 KB	306	307
	20 KB	316	313
	25 KB	320	317
	30 KB	325	320
DES	10 KB	308	303
	15 KB	309	309
	20 KB	314	317
	25 KB	318	318
	30 KB	321	324

Table 2. Experimental Results: CPU and Memory Consumption

Algorithm	**File Size**	**E- CPU (%)**	**D- CPU (%)**	**E-Memory (KB)**	**D-Memory (KB)**
BlowFish	10 KB	21.1	16.2	17.6	8
	15 KB	22.7	18.1	17.9	8.3
	20 KB	17.4	18.1	17.9	17.4
	25 KB	20.2	18.8	17.6	17.4
	30 KB	20.8	24.2	17.9	17.6
AES	10 KB	21.4	22.2	20.4	20.3
	15 KB	25.3	23	20.5	20.3
	20 KB	20.4	34	20.5	20.6
	25 KB	25	23.7	20.6	20.1
	30 KB	25.5	31.7	20.7	20.7
DES	10 KB	22.4	22.2	21.7	20.4
	15 KB	23.3	23.6	21.9	21.3
	20 KB	24.4	25.2	22.9	22.8
	25 KB	25.3	26.7	23.9	22.9
	30 KB	25.7	27.7	24.6	22.5

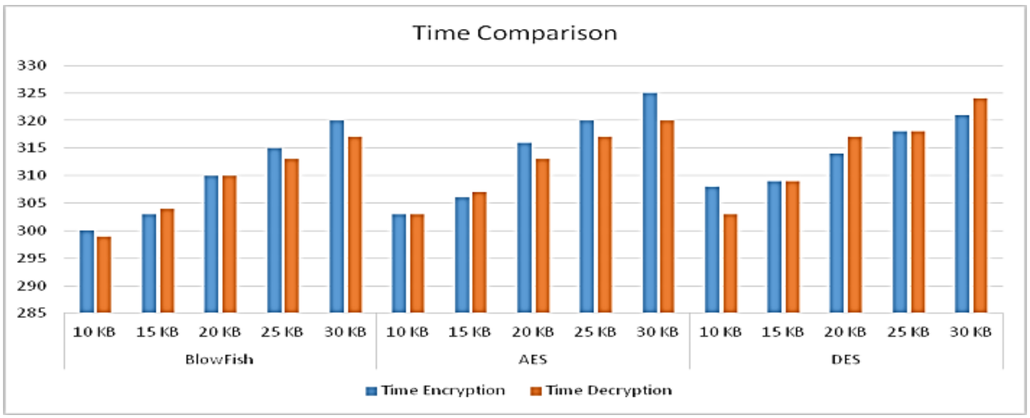

Figure 5.1 Time Comparison for Encryption and Decryption

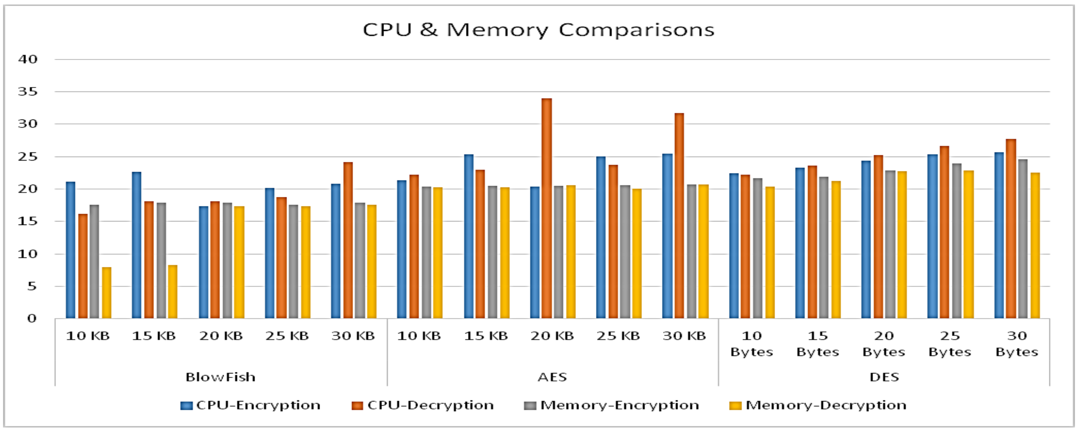

Figure 5.2 CPU and Memory comparisons for Encryption and Decryption

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 encryptionalgorithms," 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 DefensiveMechanisms. 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. Abdual-kader, 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

K. Kaviya, K. K. Shanthini, Dr. M. Sujithra, "Evolving Cryptographic Approach for Enhancing Security of Resource Constrained Mobile Device Outsourced Data in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 101-106, January-February 2019. Available at doi : https://doi.org/10.32628/CSEIT195111