Evolving Cryptographic Approach for Enhancing Security of Resource Constrained Mobile Device Outsourced Data in Cloud Computing.

ABSTRACT

Mobile cloud computing, which is growing in popularity among mobile device users, allows them to store their data in the cloud. When sensitive data is stored and transferred over the internet, security is a major concern. It is important to ensure that the data is safe and secure. We discussed the problem of data privacy while reducing resource usage in this paper. Furthermore, mobile cloud computing has resource constraints in terms of power, processor, memory, and storage. Data confidentiality, authentication, availability, and integrity are all ensured by cryptography. Cryptographic algorithms such as Data Encryption Standard (DES), Blowfish, and Advanced Encryption Standard (AES) are used to implement this (AES). The experimental results evaluated and compared the encryption algorithms' performance. Encryption and decryption times, and also CPU and memory usage, are used as performance metrics. Choosing a suitable encryption algorithm based on different parameters that are best fit to future user requirements is considered among all the techniques, with the evaluation results presenting a significant improvement in reducing resources.

I. INTRODUCTION

Mobile cloud computing makes use of cloud computing to perform resource-intensive tasks over the internet, allowing for a greater range of functionality while putting less strain on mobile resources. Cloud computing is a modern computing technique with a bright future and a lot of benefits for information technology. The main benefit of cloud computing is that it allows people to pay for cloud services as they go. By dynamically provisioning hardware, software, and data sets, cloud computing creates a virtualized platform with elastic resources on demand.

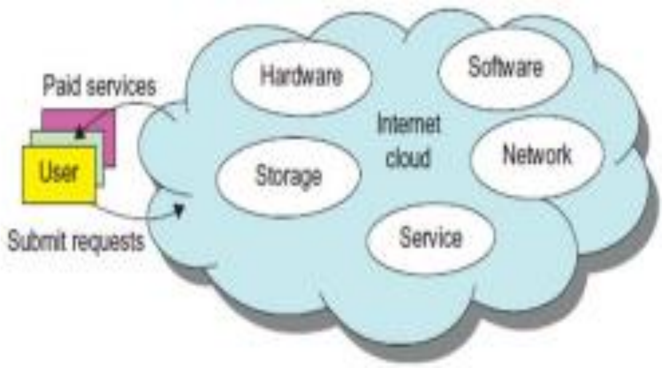

Figure 1.1 Cloud Environments

For cloud computing, there are a variety of layered architectures that can be used to provide services as a utility. Physical servers and switches make up the cloud's backbone layer. The cloud service provider is in charge of running, maintaining, and upgrading cloud hardware resources to meet the needs of users. The backbone layer is also in control of efficiently, quickly, and smoothly allocating hardware resources to users. The system software for managing cloud hardware resources is contained in the supervisor software layer. The system software enables application software to run and efficiently utilize underlying resources. Cloud providers should integrate security technologies to ensure reliability and availability in the context of mobile cloud security. MCC identifies the resource constraints of resource-constrained devices by allocating cloud services for application execution and data storage. As a result, whenever we discuss security in MCC, we must consider both security and privacy issues. Several issues, such as data security, data integrity, data confidentiality, authentication, authorization, network security, data violation issues, and so on, must be considered in order to secure the mobile cloud environment. To protect sensitive data of mobile users while reducing performance degradation, a secure framework is required. To avoid sensitive data leakage, the proposed scheme implements data encryption. When a user's data is sent to and stored on the cloud, it opens up a lot of possibilities for unauthorized data access, both during transmission and from storage devices. There are various cryptographic algorithms for dealing with security, but choosing one must consider both security and performance improvement, especially in the case of resource-constrained devices.

II. SECURITY ISSUES

· Data Storage: Data is stored in multiple copies across many different locations by cloud storage providers.

· Confidentiality: Confidentiality is defined as the protection of sensitive information from unauthorized processes, devices, and persons. A cloud service provider is aware of the location of a user's public or private data, as well as who has access to it. Only the sender and the intended recipient should have access to the contents of a message, according to the principle of confidentiality.

· Integrity: The integrity mechanism ensures that the message's contents are the same when it reaches the intended recipient as they were when it was sent by the sender. It refers to the correctness of data stored in the cloud. Data integrity is violated when changes to a record take place between two updates.

· Security: Data are stored within borders of standard file systems, but cloud data is stored outside of an organization's boundaries, for example, in third-party storage using strong encryption techniques.

· Authentication: Authentication mechanisms aid in the verification of identities. This procedure ensures that the message's origin is correctly identified.

· Non- repudiation: The sender of a message cannot refute the claim that the message was not sent due to non-repudiation.

· Access Control: Who can access the process is specified and controlled by Access Control.

· Availability: The availability principle states that resources should always be available to authorized parties.

III. CRYPTOGRAPHY

Cryptography is a method of using codes to protect information and communications so that only those who are supposed to read and process it can. Cryptography is a term used to describe secure information and communication techniques that use mathematical concepts and a set of rule-based calculations known as algorithms to transform messages in difficult-to-decipher ways. In all fields, the term "security" has always been important. Because the paper is about cloud storage systems, the proposed methodology calculates the security requirements for data stored in the cloud. Cryptography has been identified as a possible solution to this security problem. Symmetric cryptography, asymmetric cryptography, and hashing are the 3 types of cryptography.

Types of Cryptography

· Secret Key Cryptography: When the same key is used for both encryption and decryption, such as in DES, Triple DES, AES, Blow Fish RC5, and other encryptions, the process is called secret key cryptography.

· Public Key Cryptography: When two separate keys are used, one for encryption and the other for decryption, public key cryptography is used. Examples of public key cryptography include RSA, Elliptic Curve, and others.

· Hash Algorithms MD5, SHA, MD2, MD4, MD6, MD6.SHA-256, SHA-512, SHA-1, and Whirlpool are examples of hash algorithms where the input data (message) is recreated from the hash value (message digest/digest).

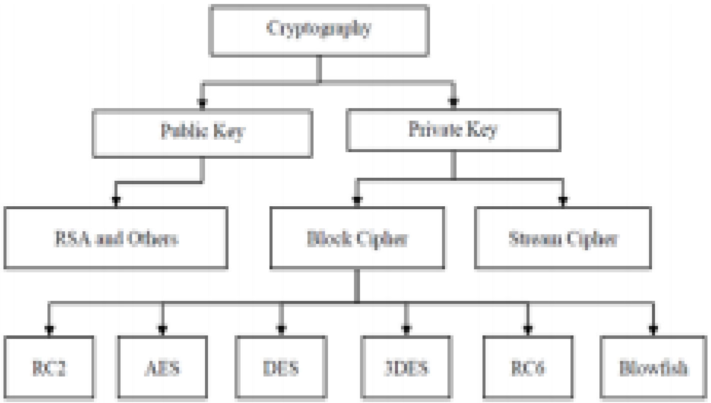

Figure 3.1 Types of cryptographic algorithms

IV. PROPOSED METHODOLOGY

Data Encryption Standard (DES)

DES uses a single secret key for encryption and decryption, with a key length of 56 bits, and performs message encryption using a 64-bit block size. It has a 64-bit key with 56 bits that are directly used as key bits by the algorithm and are provided at random. The DES algorithm uses an initial permutation, 16 rounds of the key, and a final permutation to process the 64-bit input. DES was once thought to be a powerful algorithm, but its use is now limited due to its large amount of data and short key length.

Advanced Encryption Standard (AES)

AES is a secret-key algorithm, which means it uses the same key to encrypt and decrypt data. One of the reasons for the low number of rounds is because of this. The AES encryption algorithm is both quick and flexible. It can be used on a variety of platforms, including smart phones and tablets. For effective implementation, all of the operations in this algorithm require complete bytes. AES supports three different key lengths, including 128, 192, and 256 block sizes.

Table 4.1 Comparison of Symmetric Algorithms

ALGORITHM 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 a fast, license-free, unpatented, open-source encryption algorithm that can be used instead of existing encryption algorithms. It employs a key length range of 32-448 and 64 bits. For the encryption process, the Blowfish algorithm used 16 rounds. A key-dependent permutation and key- and data-dependent substitution are included in each round. The iteration of a simple function 16 times is required for data encryption. A key dependent permutation and data dependent substitution are included in each round. Sub key generation entails converting a key with a length of up to 448 bits to a length of 4168 bits. Because of its high security level and speed, Blowfish is a good algorithm for smart phone devices.

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

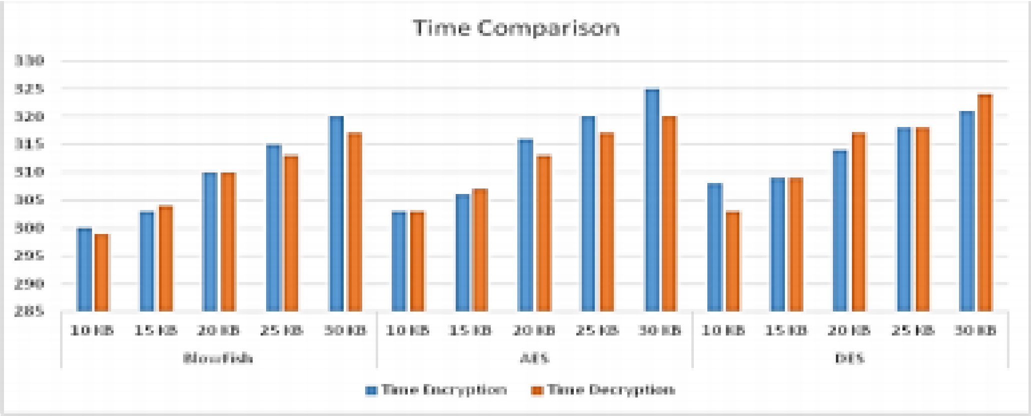

Figure 5.1 Time Comparison for Encryption and Decryption

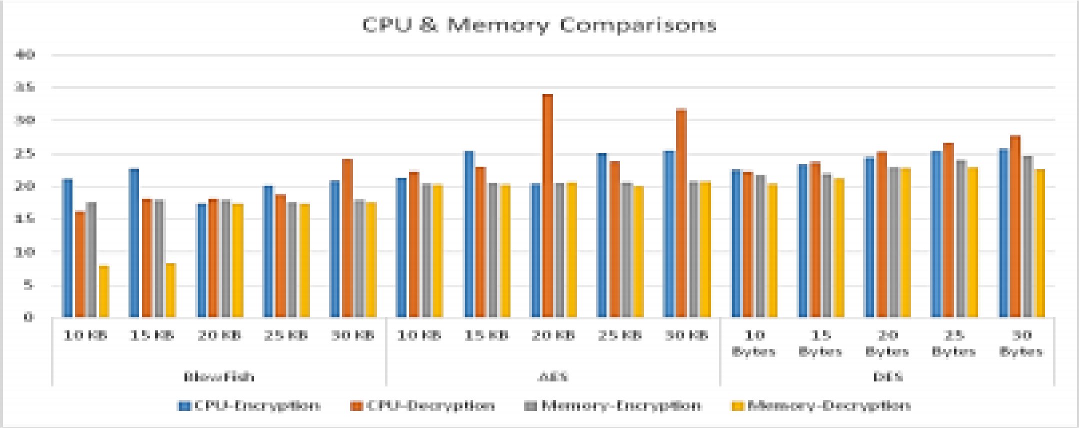

Figure 5.2 CPU and Memory comparisons for Encryption and Decryption

VI. CONCLUSION.

The presentation of results and discussion of these algorithms focuses primarily on evaluation parameters such as encryption and decryption time, memory and CPU usage, which have a greater impact on the protection, confidentiality, integrity, and reliability of secure communication. As mentioned earlier, security is a major concern when storing data in the cloud; however, the proposed system ensures that data stored in the cloud computing model is secure. Blowfish, AES, and DES provide more security based on the resources available, according to the performance evaluation. In the future, we will be able to use encryption techniques to save time and energy.

VII. 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 SathyaNarayanan. 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