IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Improvisation Of Security For Outsourcing Data In Cloud Computing Through Mobile Device With The Help Of Evolving Encryption Method

Saurabh Singh, Assistant Professor
Computer Applications Department
Veer Bahadur Singh Purvanchal University, Jaunpur

Abstract:

The increasing popularity of mobile cloud computing among mobile device users has allowed their data to be stored in cloud. When sensitive information is stored and transmitted on the Internet, security is the main issue. So user must have to ensure that the data is secure and protected. This article include the discussion of Data privacy to reduce data usage. In addition, mobile cloud computing has limitations in the following aspects resources, such as energy, processors, memory, and storage. Cryptography can ensure confidentiality, authentication, availability and data integrity. This is done through encryption algorithms, such as Data Encryption Standard (DES), Blowfish and Advanced Encryption Standard (AES). Experimental results and the performance of encryption algorithms is evaluated and compared. The performance indicators used are Encryption and Decryption time, CPU and memory utilization. The evaluation result shows to choose a suitable encryption algorithm among all technologies to reduce resources and consider the different parameters that are most suitable for future user requirements.

Keywords: DES, Blowfish, AES, Cryptography, Cloud Computing, RSA.

Introduction:

Mobile cloud computing uses cloud computing to carry out resource-intensive tasks over an internet to provide a higher range of functions with the least pressure on mobile resources. Cloud Computing is a modern computing technology, Have a bigger future and bring many benefits for the improvement of Information Technology. The main advantage to use the cloud platform is that it provides cloud services for people to pay on demand. Cloud computing virtualization platform with flexible resources provide hardware, software and dynamic data set. There are multiple layered architectures available for Cloud computing which provides services in the form of utility programs. The backbone layer of the cloud consists of physical servers and switch. The cloud service provider is responsible for running, managing and upgrading the cloud hardware resources as required user. The backbone is also responsible for efficiently allocate hardware resources to users and provide fast and smooth way. Supervisor software layer contains management of cloud hardware resources. System software allow application software to run and use effective basic resources. The context of mobile cloud security, cloud provider reliability and availability should be ensured by integrate the safety technology satisfied by MCC Limitations of resource-constrained devices to allocate cloud services for the following purposes application execution and data storage. So whenever user mention security in "My Client Centre", it's necessary to consider security and privacy issues. In order to protect the mobile cloud environment, focused is to consider about data Security, data integrity, data confidentiality, authentication, authorization, network security, data Violation issues, etc. Security framework is essential to Maximum protection of sensitive data of mobile user's performance drops. Proposed program use Data encryption protects sensitive data from leakage.

When user data is transferred to and stored in Cloud, it creates many unauthorized possibilities Access data during or from transmission Storage device. There are many passwords Algorithms that deal with security, but selection is focused on to consider security and Performance improvement, especially in Resource-constrained equipment.

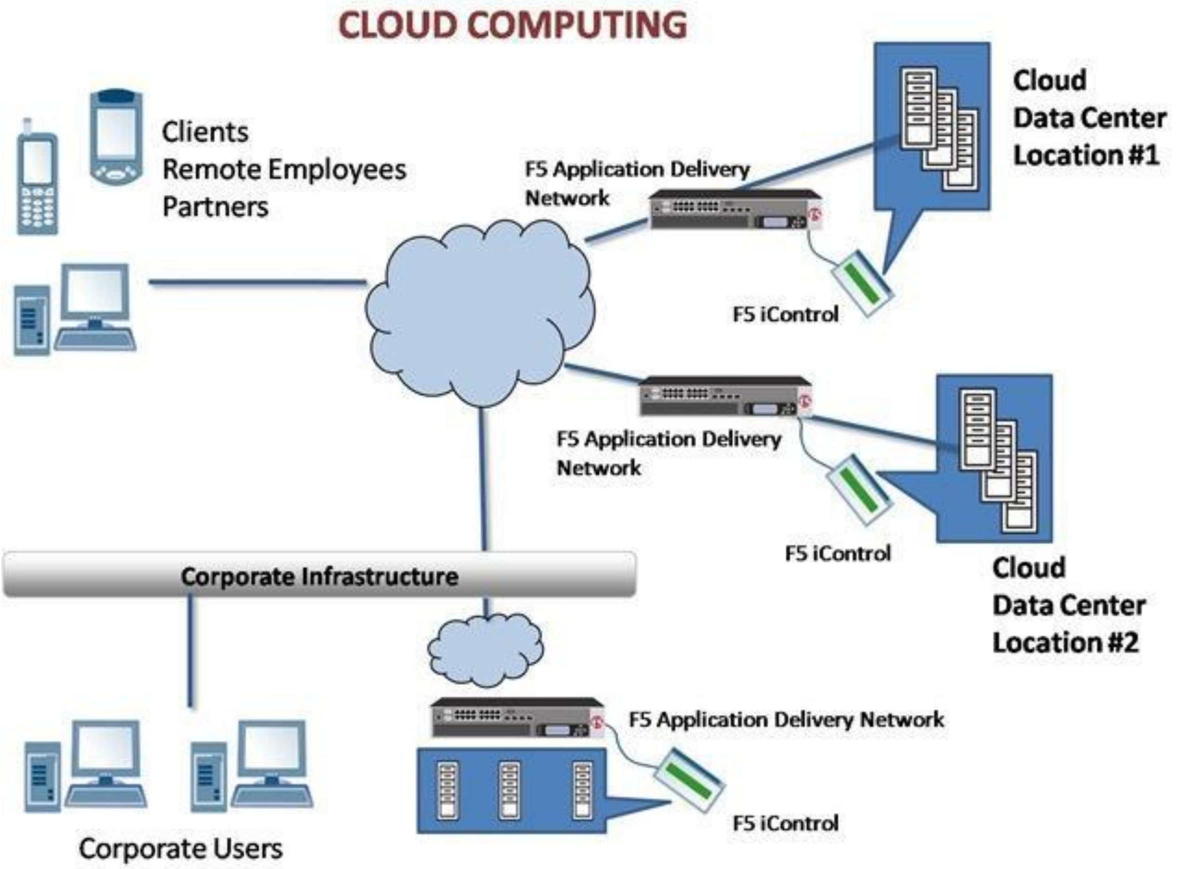

CLOUD COMPUTING
Clients
Remote Employees
Partners
F5 Application Delivery Network
Cloud Data Center Location #1
F5 iControl
F5 Application Delivery Network
F5 iControl
Cloud Data Center Location #2
Corporate Infrastructure
F5 Application Delivery Network
F5 iControl
Corporate Users

Fig. 1. Cloud computing architecture (www.researchget.net)

Security Problems:

Data storage: Cloud storage provider can manage the data in multiple copies over a multiple location.
Confidentiality: Confidentiality can be defined as non-disclosure of sensitive data unauthorized process, equipment and personnel. The cloud service provider knows where the user is find public or private data, and who can/cannot access the data. Principle The confidentiality requirement is only the sender and the intended recipient should be able to access the content of the message.
Integrity: The integrity mechanism ensures the content of the message remains unchanged When it reaches the intended recipient sent by sender. Defined as the correctness of the data Stored in the cloud. Changes between the two the update of the record violates data integrity.
Security: In traditional file systems, data is stored within the boundary, but cloud data is stored outside the organizational boundaries, for example, and third-party storage using strong encryption technology.
Identity verification: Identity verification mechanism can help create proof of identity. This process make sure the source of the message is correct and determine.
Non-repudiation: Non-repudiation allow email senders to reject claims of do not send messages.
Access control: Access control designation and control who can access the process.
Usability: Usability principle resources should be available for authorization among attending parties.

Cryptography:

It is an information protecting method which communicate with the code, so due to this only those particular person can see these information who are entitled as a receiver can be read and Deal with it. Cryptography consist secure technology which originates from Mathematical concepts for information and communication and a set of rule-based Calculations are called algorithms to transform messages it is always secure in an incomprehensible way It is an important term in all fields. As paper Discussing cloud storage system, suggest

Methodology considered Data stored in the cloud. Cryptography has Solve this security problem. Symmetry Cryptography, asymmetric cryptography and hashing.

Types of cryptography:

Key encryption: When the same key is used to encrypt and decrypt DES, Triple DES, AES, Blow Fish RC5, etc. Examples of such encryption this mechanism is called secret key encryption.

Public key cryptography: two different times Use key, the key used for encryption and encryption another key for decryption, RSA, elliptic curve etc. An example of such encryption, the mechanism is called public key Cryptography.

Hash algorithm, where the input data (message) recreate from hash (message) Abstract/Abstract) Examples include: MD5, SHA, MD2, MD4, MD6. SHA-256, SHA-512, SHA-1, Whirlpool etc.

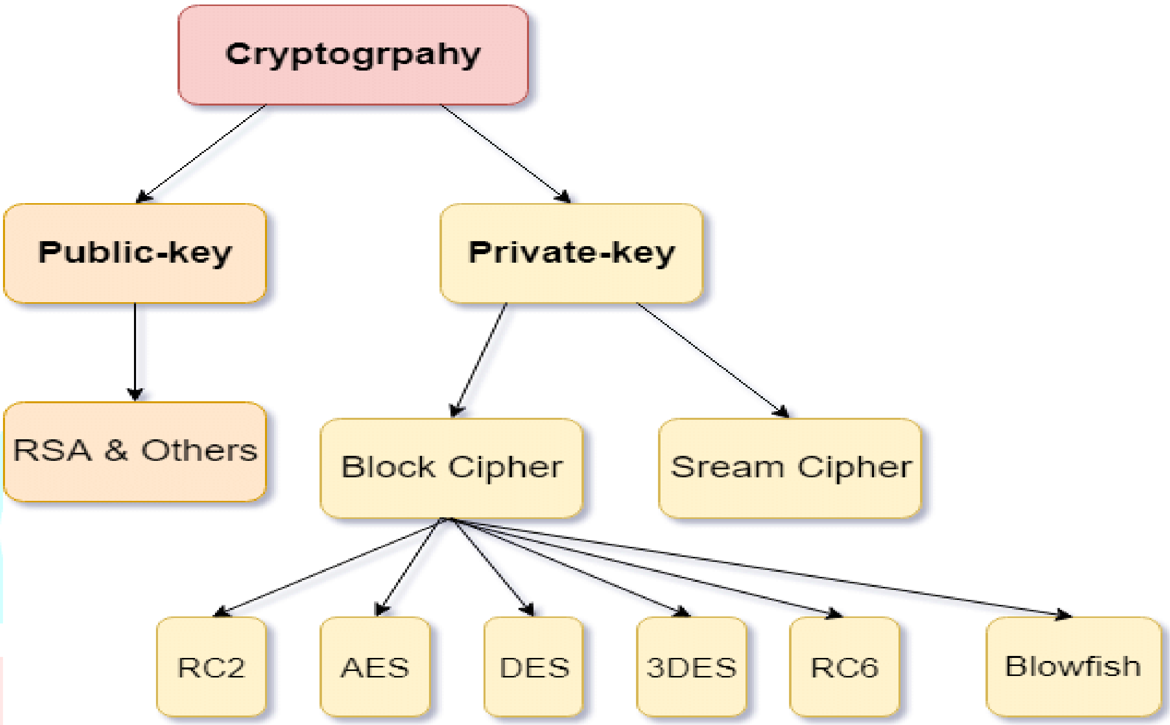


Fig. 2. Types of cryptographic algorithms (www.researchget.net)

IJCRT

Proposed Method:

Data Encryption Standard (DES)-

DES uses a secret key for encryption and decryption, the key length is 56 bits, and 64 bits block size are used to perform message encryption. It contains a 64-bit key, which contains 56 bits. The algorithm directly uses the key as a key bit and generates it randomly. The DES algorithm uses initial permutation, 16 rounds of the key, and final permutation to process 64-bit input. DES was originally considered a powerful algorithm, but nowadays the large amount of data and short key length of DES restrict its use.

Advanced Encryption Standard (AES)-

The algorithm explained by AES is a secret key algorithm that uses the same key to encrypt and decrypt data. This is one of the reasons why it has relatively few rounds. AES encryption is fast and flexible. It are often implemented on various platforms, especially in small devices. All operations in this algorithm involve complete bytes for effective implementation. AES supports three different key lengths, such as 128, 192, and 256 block sizes.

Blowfish-

Blowfish is fast, free, patent-free, freely available, and can replace existing encryption algorithms. The key length range it uses is up to 32-448 bits and 64-bit blocks. The Blowfish algorithm uses 16 rounds of encryption. Each round contains a permutation related to the key and substitutions related to the key and data. Data encryption involves 16 iterations of simple functions. Each round contains permutations related to keys and substitutions related to data. Sub-key generation involves converting a key with a maximum length of 448 bits into 4168 bits. Blowfish has high security and fast speed, and is an algorithm very suitable for smartphone platforms.

Table 1. Comparison of Symmetric Algorithms

Algorithms	DES	AES	Blowfish
Key Size (Bits)	64	128,192,256	32-448
Block Size (Bits)	64	128	64
Round	16	10,12,14	16
Structure	Feistel	Substitution Permutation	Feistel
Flexibility	No	Yes	Yes
Features	Not Structure Enough	Excellent Security	Secure Enough
Speed	Slow	Fast	Fast

Performance Evaluation Index:

Time Calculation of CPU –

CPU time = **I * CPI * T**, where **I** = the number of instructions in the program, **CPI** = the average cycle of each instruction, and **T** = clock cycle time. CPU time = **I * CPI / R**, where **R** = 1 / T clock rate, **T** or **R** is usually released as a performance indicator of the processor, **I** need special performance analysis software, and **CPI** depends on many factors (including memory).

Performance calculation-

Seconds/program = (instruction/program) x (clock/instruction) x (second/clock)

Memory consumption- calculation total memory-(free + buffer + cache) = current total memory usage.

Table 2. Experimental Results: Time Comparison

Algorithms	File Size	Time Encryption(m.s.)	Time Encryption(m.s.)
DES	20 KB	408	403
	25 KB	409	409
	30 KB	414	417
	35 KB	418	418
	40 KB	421	424
AES	20 KB	403	403
	25 KB	406	407
	30 KB	416	413
	35 KB	420	417
	40 KB	425	420
Blowfish	20 KB	400	399
	25 KB	403	404
	30 KB	410	410
	35 KB	415	413
	40 KB	420	417

Table 3. Experimental Results: CPU and Memory Consumption

Algorithms	**File Size**	**E-CPU (%)**	**D-CPU (%)**	**E-Memory (KB)**	**D-Memory (KB)**
DES	20 KB	32.4	32.2	31.7	30.4
	25 KB	32.3	33.6	31.9	31.3
	30 KB	34.4	35.2	32.9	32.8
	35 KB	35.3	36.7	33.9	32.9
	40 KB	35.7	37.7	34.6	32.5
AES	20 KB	31.4	32.2	30.4	30.3
	25 KB	35.3	33	30.5	30.3
	30 KB	30.4	44	30.5	30.6
	35 KB	35	33.7	30.6	30.1
	40 KB	35.5	41.7	30.7	30.7
Blowfish	20 KB	31.1	26.2	27.6	18
	25 KB	32.7	28.1	27.9	18.3
	30 KB	27.4	28.1	27.9	27.4
	35 KB	30.2	28.8	27.6	27.4
	40 KB	30.8	34.2	27.9	27.6

Fig. 3. Types of cryptographic algorithms Time Comparison for Encryption and Decryption

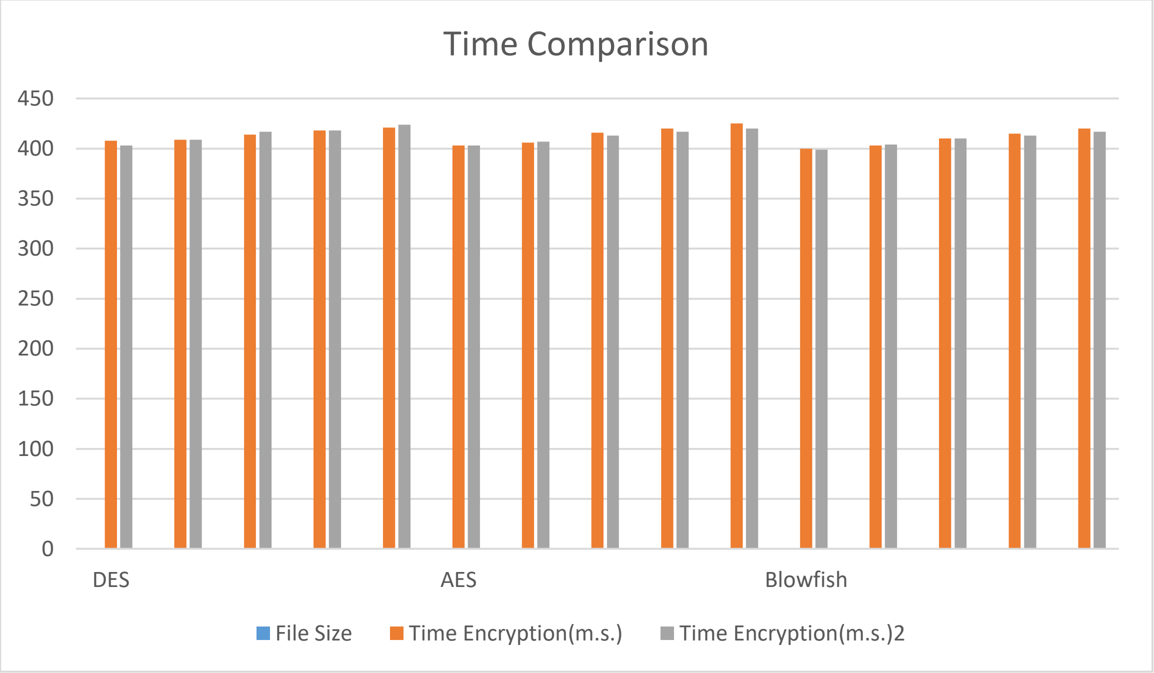
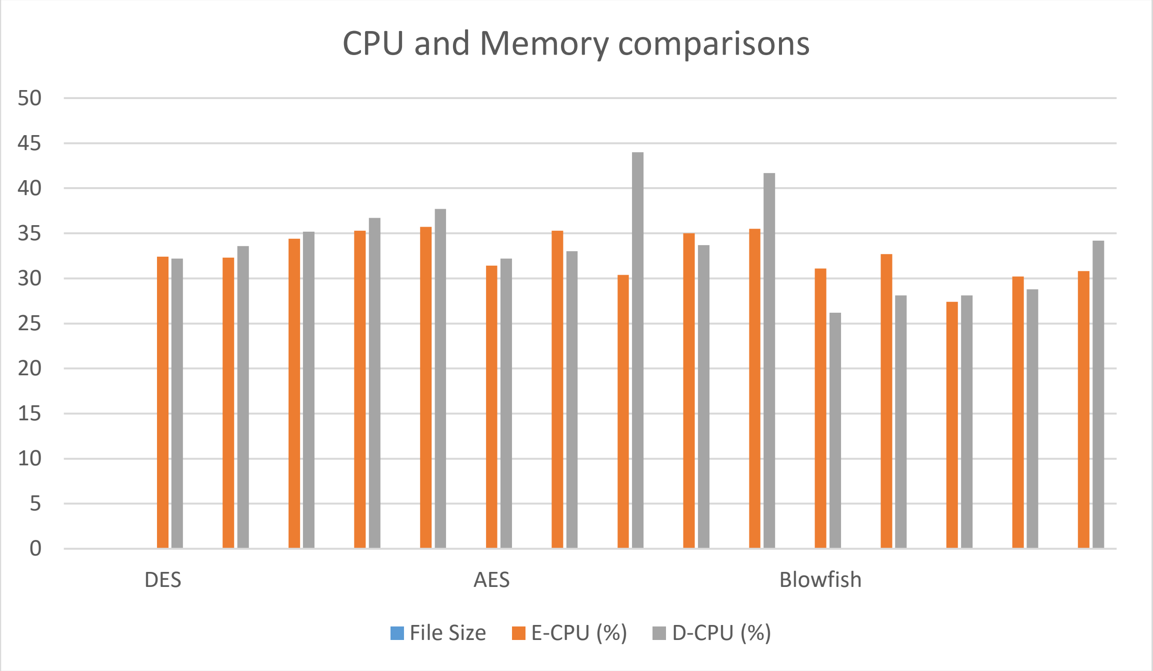


Fig. 4. CPU and Memory comparisons for Encryption and Decryption



Conclusion:

The demonstration of the results and the discussion of these algorithms mainly focus on evaluating parameters, such as encryption and decryption time, memory and CPU utilization, these parameters have a greater impact on the security, confidentiality, integrity and reliability of secure communications . As mentioned earlier, security is the main challenge faced when storing data in the cloud, and the proposed system provides security for the data stored in the cloud computing model. Based on performance evaluation, the results of Blowfish, AES and DES provide higher security based on resource availability. In the future, we can use encryption technology to make it consume less time and the lowest energy consumption.

References:

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 480-485.

Paresh D. Sharma, Professor Hitesh Gupta (February 2014), An Implementation for Conserving Privacy based on Encryption Process to Secured Cloud Computing Environment IJESRT Sharma, 3(2).

DSA Elminaam, H. MA Kader and MM Hadhoud, "Evaluating the performance of symmetric encryption algorithms," International Journal of Computer Theory and Engineering, Volume. 10, no.3 pp. 343-351, 2009.

HealeyM (2010) Why IT needs to promote data sharing. Information week. Source: http://www.informationweek.com/services/integration/why-it-needs-to-push-data-sharingeffort/225700544. Visited in October 2012.

Shanthni KK. , Kaviya K and Sujithra M.2018, "Cloud Computing Survey: Data Security Challenges and Their Defence Mechanisms." International J recent science. 9(5), pp. 26497-26500. DOI: http://dx.doi.org/10.24327/ijrsr.2018.0905.2070 [10].

L Krithikashree; S. Manisha; M Sujithra, "Audit Cloud: Ensuring the Data Integrity of Mobile Devices in Cloud Storage", published in: 2018 9th International Conference on Computing, Communication and Network Technology (ICCCNT), IEEE, DOI: 10.1109/ ICCCNT.2018.8493963