EFFICIENT ENCRYPTION ALGORITHM PREDICTION IN CLOUD COMPUTING

[1]Gummadi Divya, [2]S.K.A. Manoj, [3]D.Lalitha Bhaskari

[1]Student, [2]Research Scholar, [3]Professor
[1] Department of Computer Science and Systems Engineering
[1]Andhra University College of Engineering(A), Andhra University, Visakhapatnam, India

ABSTRACT: Cloud is one of the most beneficial innovations for businesses providing low-cost, virtual services, and local hardware. It is a global platform that permits digital information to be shared and distributed at very low cost at very fast pace to access. Cloud data security and performance are essential elements, as you will want to be sure that your data is safe while stored in the cloud. The main goal of cloud computing is to provide easily scalable access to computing resources to improve performance. One way to deal with performance aspect is using encryption mechanism to construct reliable and secure cloud environment. Implementing encryption sometimes may degrade the performance due to the data type and algorithm type. There are many cryptographic encryption algorithms and in this AES, DES, SHA1, MD5 and blowfish algorithms are used to improve the security and performance of cloud data. In this project, a model is being implemented which analyses the type of data and suggest the suitable algorithm for encryption to improve the performance of the cloud.

Index terms: cloud stored data, performance, encryption, decryption, hashing, AES, DES, SHA1, MD5, **Blow fish.**

I.INTRODUCTION

Cloud is the group of servers and data centers that are placed at different locations and these severs and data centers are responsible for providing on demand service to its users with help of internet. The service provided by cloud is not available on user's computer. User has to access these services with help of internet connection through accepting them.

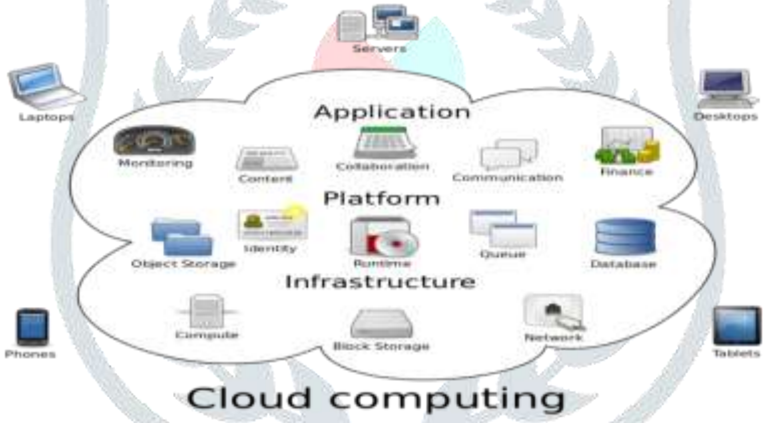

Figure 1: Server consolidation in the cloud [14]

The main advantage of Cloud computing is that it abolishes the need for user to be in same location where hardware software and storage space is physically present. Cloud creates it possible to store and access your data from anywhere anytime without worrying about maintenance of hardware software and storage space. All these services are makes available to user at low cost. User has to pay charges according to storage space he is using. Due to this flexibility everyone is transferring his data on cloud environment.

Benefits of Cloud Computing are Reduced Cost, scalability and flexibility, backup and recovery, broad network access, multi sharing etc.

Security is considered as one of the most critical aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven't been fully evaluated with respect to the security. Cloud Computing has several major issues and troubles, such as data security, trust, expectations, regulations, and performances issues.

Encryption is the process of transforming information in such a way that an unauthorized person cannot read it; a trusted person can decrypt data and access it in its original form though. There are a lot of popular encryption and decryption algorithms, but the key to security is not a proprietary algorithm. The most important thing is keeping the encryption key secret so only trusted person know it. Encryption can protect data in motion as well as at rest.

Symmetric key algorithms: This is the simplest kind of encryption that includes only one secret key to cipher and decipher information. Symmetrical encryption is an old and well-known technique. It utilizes a secret key that can either be a number, a word or a string of random letters. It is a combined with the plain text of a message to change the content in a particular way. The sender and the recipient should know the secret key that is utilized to encrypt and decrypt all the messages. Blowfish, AES, RC4, DES, RC5, and RC6 are symmetric encryption algorithms. The most commonly used symmetric algorithms are AES-128, AES-192, and AES-256.

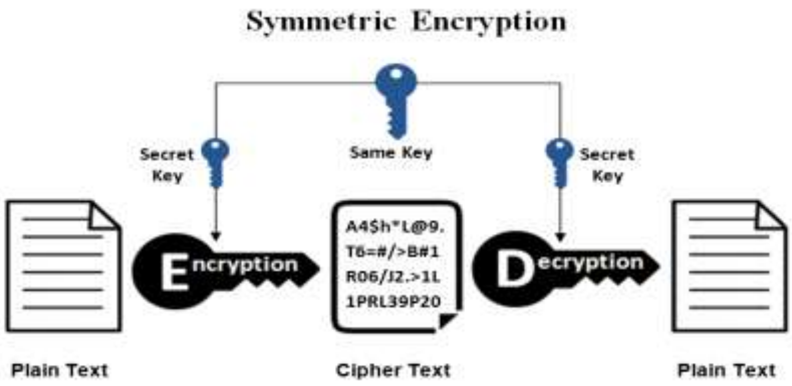

Figure 2: symmetric encryption process [15]

Asymmetric algorithms: Asymmetric Encryption is a relatively new and complex mode of Encryption. Complex because it consists of two cryptographic keys to implement data security. That keys are one is Public Key and another one is Private Key. The Public key, as the name suggests, is accessible to everyone who wishes to send a message. On the other hand, the private key is kept at a secure location by the owner of the public key.

The public key encrypts the information to be sent and it uses a specific algorithm in doing so. Whereas, the private key, which is in possession of the receiver, decrypts that encrypted data. The Same algorithm works behind both these processes.

The involvement of two keys results asymmetric encryption a complex technique. Thus, it demonstrates to be a massively beneficial in terms of data security. Diffie-Hellman and RSA algorithm are the most commonly used algorithms for Asymmetric Encryption.

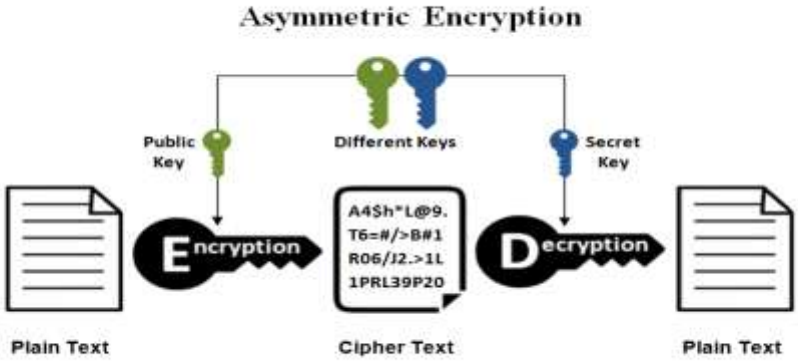

Figure 3: asymmetric encryption process [16]

Hash algorithm: Hashing is generating a value or values from a string of text using a mathematical function and it is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to preserve the security of the transmission against tampering.

Hashing is also a method of sorting key values in a database table in an effective manner. Examples of hashing algorithms are SHA, MD5, HMAC, VMAC etc.

II. LITERATURE REVIEW

Cryptography in the cloud makes use of encryption techniques to secure data that will be used or stored in the cloud. Cryptography allows users to conveniently and securely access shared cloud services, as any data that is hosted by cloud providers is protected with encryption. Cryptography in the cloud environment protects sensitive data without delaying information exchange. Below are some cryptographic algorithms which will perform encryption on cloud data.

AES: AES also known as Advanced Encryption Standard is a very popularly used encryption algorithm. AES was first approved by United States National Institute of Standards and Technology (NIST) in 2001. This algorithm was originally named as 'Rijndael' and consists of different key and block sizes. By design, AES is a block cipher technique consisting of 128 bits or 192 bits or 256 bits. A block cipher technique is the one in which encrypts one data block at a time. Though 128 bits are strong and efficient, 256 bits are used for high grade encryption algorithms. This algorithm is used by a number of organizations across the globe. It is a symmetric algorithm it uses a single private key for encryption and decryption process [17].

Blowfish: Blowfish is a symmetric key algorithm and developed in 1993. It is the most common public algorithm provided by Bruce Schneier. It is a variable length key and 64-bit block cipher. No attack is recognized to be successful compared to this. Several experiments and research exploration proved the dominance of Blowfish algorithm over the other algorithms in relations of the processing time. Blowfish is the improved than any other algorithms in data and power consumption. Fast- Blowfish encryption speed on 32-bit is 26 clock cycles per byte. Simple-Blowfish uses simple operation such as addition, XOR and table consult, making its policy and application simple [18].

DES: It is also known as Data Encryption Standard encryption algorithm was first used and endorsed by US Government in 1977. This encryption algorithm forms the basis for ATM PIN authentication and also utilized in UNIX encryption password. It is a block cipher with 64-bit block size and uses 56-bit keys. Triple DES or 3DES was designed as a more secure and stronger encryption algorithm to replace the original version of DES algorithm. Triple DES encrypts the data three times with three different individual keys of 56-bits each, that makes the total cumulative key length up to 112-168 bits long [20].

Secure Hashing Algorithms: SHA are a family of cryptographic functions designed to keep data secured. It works by transforming the information using a hash function an algorithm that consists of bitwise_operations, modular_additions, and compression_functions. The hash function then produces a fixed size string and it looks nothing like the original. These algorithms are designed to be one way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data [19].

Message Digest (MD): MD5 was most popular and mostly used hash function for quite some years. The MD family consists of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321and is a 128-bit hash function. MD5 digests have been mostly used in the software world to provide assurance about integrity of transferred file. Consider an example, file servers often provide a pre-computed MD5 checksum for the files, so that a user can compare the checksum of the downloaded file to it [19].

Most commonly used algorithms for all types of files

s.no	Mostly used Algorithms
1	Advanced Encryption Standard Algorithm
2	Data Encryption Standard Algorithm
3	Blow fish algorithm
4	Message Digest Algorithm
5	Secure Hash Algorithm

III.PROPOSED METHODOLOGY

Encryption algorithms are employed to create cloud data more secure and efficient. Cryptographic algorithms are used to store the data securely in the cloud environment. By using those algorithms we will encrypt the data securely and calculate the encryption time for given data in the cloud. Based on that calculated encryption time performance of the encryption algorithm is analyzed. But depends on the file size and type encryption time differs for each algorithm. In this paper total of nine types of data like MP4, PDF, JPG, PNG, SVG, FLV,GIF and 3GP(mobile acceptable) have been considered and the comparison has been made by running existing encryption algorithms like AES, DES, Blowfish and hashing algorithms like SHA1 and MD5 to process different types of data with different sizes to evaluate the algorithms encryption speed in milliseconds. By comparing those results we concluded that particular algorithm is suitable for given file based on their type and size with that encryption speed.

To achieve this in this project we have developed a methodology. In this the process is done in three stages.

Stage 1: In the first stage user data which they want to encrypt needs to upload. In this project we have taken nine types of data with n number of sizes. When the user uploaded the file it displays the file name and size. We have two types of data one is sensitive data and another one is non sensitive data.

Stage 2: In second stage it will display the sensitive and non sensitive data algorithms based on prior results. Depends on the conditions it will display the appropriate algorithms by considering file size and type. For sensitive data AES, DES and Blowfish algorithms works best and for non sensitive data MD5 AND SHA1 algorithms works best.

Stage 3: In the third phase by using those existing encryption algorithms the user will select the relevant algorithm to encrypt and decrypt the data. That encrypted and decrypted data will store at particular location. This methodology will improve the performance of the cloud stored data with the encryption algorithms.

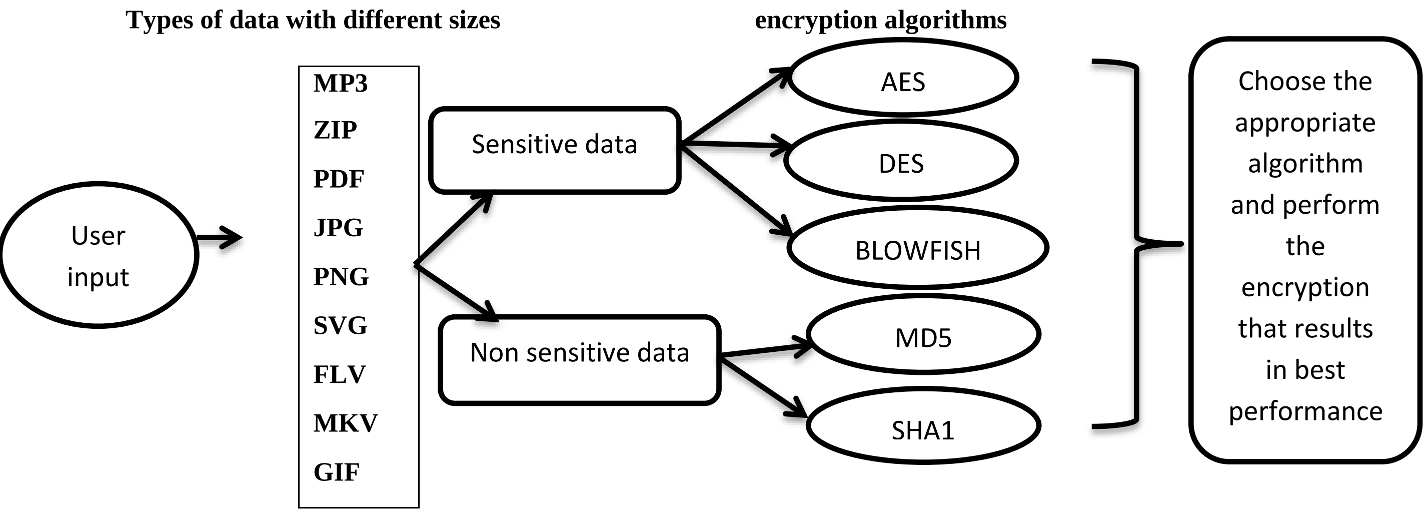
Types of data with different sizes
encryption algorithms
User input
MP3
ZIP
PDF
JPG
PNG
SVG
FLV
MKV
GIF
Sensitive data
Non sensitive data
AES
DES
BLOWFISH
MD5
SHA1
Choose the appropriate algorithm and perform the encryption that results in best performance

Figure 4: Proposed System Architecture

IV.RESULTS AND ANALYSIS

We performed encryption and hashing algorithms for different types of data with n number of sizes. Below are experimental results that show Encryption and hashing algorithms with best performance for different types of files with different sizes based on encryption decryption and hash time in milliseconds.

Efficient encryption algorithms which will work better for jpg, zip, gif, 3gp, png files

TYPE/SIZE	ANY SIZE
JPG	MD5 AES BLOWFISH
ZIP	MD5 AES BLOWFISH
GIF	MD5 BLOWFISH DES
3GP	MD5 AES BLOWFISH
PNG	AES SHA1 BLOWFISH

For mp4 file with <5mb sha1, des, blowfish are efficient and for >=5mb sha1, blowfish and aes are efficient

TYPE/SIZE	<5MB	>=5MB
MP4	SHA1 BLOW FISH 3DES	SHA1 BLOWFISH AES

For excel file with <28kb aes, des, md5 are efficient and for >=28kb md5, blowfish and aes are efficient

TYPE/SIZE	<28KB	>=28KB
EXCEL	AES MD5 DES	AES MD5 BLOWFISH

For flv file with <30mb md5, aes, blowfish are efficient and for >=30mb md5, des and aes are efficient

TYPE/SIZE	<30MB	>=30MB
FLV	MD5 AES BLOWFISH	MD5 AES DES

For mkv file with <10mb sha1, des, blowfish are efficient and for >=10mb sha1, blowfish and aes are efficient

TYPE/SIZE	<10MB	>=10MB
MKV	AES MD5 DES	AES MD5 BLOWFISH

For svg file with <5mb md5, blowfish are efficient and for >=5mb md5 and aes are efficient

TYPE/SIZE	<5MB	>=5MB
SVG	MD5 BLOWFISH	MD5 AES

For pdf file with <1mb aes, sha1, des, are efficient and for >=1mb aes, sha1, blowfish are efficient

TYPE/SIZE	<1MB	>=1MB
PDF	AES SHA1 DES	AES SHA1 BLOWFISH

V.CONCLUSION

Cloud services have geared up for being the most suitable option for storing personal and important data online digitally and data is remotely maintained, managed and backed up. Performance and security are extremely high priority for all cloud storage services. To achieve this in this paper encryption algorithms have been offered to make cloud data efficient and also evaluations have been made among AES, DES, SHA1, MD5, Blow fish to find the efficient algorithm by taking different files with different sizes. Based on appeared results we concluded that particular algorithm is suitable for particular file based on their type and size which will assist the performance and security of cloud stored data.

VI.REFERRENCES

[1] Murtala Aminu Baba, Abdulrahman Yusuf, Aminu Ahmad,” Performance Analysis Of The Encryption Algorithms As Solution To Cloud Database Security”, International Journal Of Computer Applications (0975 – 8887) Volume 99 – No.14, August 2014.

[2] Nabeel Zanoon, “Toward Cloud Computing: Security And Performance” International Journal On Cloud Computing: Services And Architecture (Ijccsa) ,Vol. 5,No. 5/6, December 2015.

[3] Tara Salman, Tara (Dot) Salman (At) Wustl.Edu, “Performance Analysis Of Traditional Cryptosystems In Multi-Cloud Management Platform”.

[4] Sangeet Mishra , Asis Kumar Tripathy , Pallavi Joshi, “Making A Cloud Data Secure And Effective For Better Performance Of Services”, Indonesian Journal Of Electrical Engineering And Computer Science Vol. 2, No. 3, June 2016, Pp. 695 ~ 702 Doi: 10.11591/Ijeecs.V2.I3.Pp695-702.

[5] Monjur Ahmed And Mohammad Ashraf Hossain, “Cloud Computing And Security Issues In The Cloud”, International Journal Of Network Security & Its Applications (Ijnsa), Vol.6, No.1, January 2014.

[6] Shakeeba S. Khan1 , Prof.R.R. Tuteja, “Security In Cloud Computing Using Cryptographic Algorithms”, International Journal Of Innovative Research In Computer And Communication Engineering (An Iso 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015.

[7] Pradnya B. Godhankar, Deepak Gupta, “Review Of Cloud Storage Security And Cloud Computing Challenges”, (Ijcsit) International Journal Of Computer Science And Information Technologies, Vol. 5 (1) , 2014, 528-533.

[8] V. Spoorthy, M. Mamatha, B. Santhosh Kumar” A Survey On Data Storage And Security In Cloud Computing”, International Journal Of Computer Science And Mobile Computing, Vol.3 Issue.6, June- 2014, Pg. 306-313.

[9] Heru Susanto & Mohammad Nabil Almunawar And Chen Chain Kang, (2012) “Toward Cloud Computing Evolution: Efficiency Vs Trendy Vs Security”, Computer Science Journal.

[10] Niloofar Khanghahi & Reza Ravanmehr, (2013)” Cloud Computing Performance Evaluation: Issues And Challenges”, International Journal On Cloud Computing: Services And Architecture (Ijccsa), Vol.3, No.5.

[11] Shailesh Paliwal, (2014) “Performance Challenges In Cloud Computing”, Https://Www.Cmg.Org

[12] Geeta C Ma , Raghavendra Sb , Rajkumar Buyyac , Venugopal K Rd , S S Iyengare , L M Patnaikf,” Data Auditing And Security In Cloud Computing: Issues, Challenges And Future Directions”, International Journal Of Computer (Ijc) Issn 2307-4523.

[13] Suresh, K.S. And Prasad, K.V. (2012). Security Issues And Security Algorithms In Cloud Computing. International Journal Of Advanced Research In Computer Science And Software Engineering, 2(10), 110-114.

[14] https://www.google.co.in/search?q=cloud+computing+images&rlz=1C1RLNS_enIN804IN804&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiM-JCKodbeAhVbinAKHUKYAQQQ_AUIDigB&biw=1526&bih=692#imgrc=24YjXXMD5Qdv3M.

[15] https://www.google.co.in/search?q=asymmetric+encryption+images+images&rlz=1C1RLNS_enIN804IN804&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjL7M7LodbeAhUMqo8KHcchBXIQ_AUIDigB#imgrc=epu6guPybkFMqM:

[16] https://www.google.co.in/search?q=Asymmetric+encryption+images&rlz=1C1RLNS_enIN804IN804&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiCsPq7otbeAhWeiHAKHTm0CNQQ_AUIDigB&biw=1526&bih=692&dpr=1.25#imgrc=5ca2hxKev9b_CM:

[17] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[18] Ms NehaKhatri, Valmik, Prof. V. K Kshirsagar , “Blowfish Algorithm” *IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83www.iosrjournals.org*

[19] https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

[20] https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm