Implementation of Cryptographic Algorithms for Performance Measurement in Cloud Computing

[1]Amit R Gadekar1, [2]Dr M V Sarode, [3]Dr V M Thakare
[1]Assistant Professor, [2]Professor, [3]Professor
1Department of Computer Engineering
[1]SF's, SITRC, Nashik, SPPU Pune(MH), India

Abstract : Cloud Computing-An innovation which gives the on-request Information Technology administrations for the client through the web. Cloud computing encourages the client by giving the assets of outsider for the sake of framework, equipment and programming over the system. Foundations of Cloud processing makes the client to get to the information anyplace whenever as long as the client's gadget approaches with the web. Such movement enhances the utilization of web application which gives "pay as you go" office. Henceforth this adaptability makes an effect upon the client and made them to exchange their information to cloud. In any case, it might lay some security issues too. Cryptographic algorithms were actualized to conquer the security issues and to guarantee the Cloud figuring information security. These days numerous procedures of this encryption and decryption were proposed to keep up security in cloud information. Here an examination was made on this cryptographic algorithms and a similar investigation was introduced.

Index Terms **- Cloud Computing, Cryptography, Decryption, Distributed computing, Encryption.**

I. INTRODUCTION

Cloud computing has created as an incredibly comprehended methodology to encourage broad and voluminous data with the help of shared pool of benefits and tremendous storing an area. [1] States that "cloud computing is another enrolling perspective that depends on virtualization, dispersed figuring, utility preparing and organization arranged designing". Facilitate it is included that distributed computing has created as most basic perspective of the IT business and has pulled in most of the business and the insightful network. [2] have portrayed about distributed computing. Distributed computing, point of fact, is an extensive term that gives more web benefits. These are secluded into three general classes [3] Infrastructure-as-a-Service , Platform-as-a-Service and Software-as-a-Service. The web is by and large addressed as the "Cloud". The most section a cloud benefit is used by the clients as and when re-quired, frequently on the hourly introduce. This "on-demand" or "pay as you go" approach impacts the cloud to profit versatile, where end customer can have an amazing game plan or unassuming of an organization the way they need any point of time and the organization is totally directed by the provider. Indispensable redesigns in each key parts included virtualization passed on registering and moreover the upgraded access to fast web office and also weak economy has speeded up the development of distributed computing altogether. As cloud figuring values handling as a sufficiency, providers are developing a typical shared assembling of configurable assets, which clients can enthusiastically condition and free as showed by their evolving needs. Along these lines, both gathering the service providers and the customers would easily benefit by the reuse of figuring resources and lessening in cost. The cloud benefits that are completed will be executed and reliable with couple of threats. Beginning advances expected to deflect these threats. In this way security is the fundamental stress the individuals who need to utilize cloud organizations. As demonstrated by [4] there exist a bit of the essential security risks that undertaking the Cloud figuring use that spreading spam and malware movement of botnets. The other case is the application interfaces that are necessary to connect with cloud benefits especially that are created by outsiders. These interfaces must outfit the customer with much anchored check, endorsement, encryption and advancement observing systems.

II. LITERATURE REVIEW

The most fundamental goal in [5] is passing on reliable access to control, administration, check and organization masterminded designing organization to end customer. It focused on get-together the safe and bland outline for that distributed computing stage without knowing its administrations and models. In distributed computing, data is shield from the unapproved singular, denial of service and administration manhandle. In [6] the highlights of cloud security techniques, insurance issues have focused on specialist co-op side security and proposed the extensible approval tradition for affirmation with RSA calculation.

In [7] troubles in surveying the cloud approaches, asset execution and application work stack is portrayed as to a great degree difficult to achieve, along these lines it proposed, To achieve anchoring and secure access to control, [8] use astoundingly joining systems of Attributes Based Encryption(ABE), go-between decoding and loose unscrambling. It has depicted cryptographic technique, which give better mystery and security of important data outsourced by customer shared on cloud server. In [9] include every one of security requirements of distributed computing were featured and advising about how to manage the cloud computing security. It have depicted and include the general security concern whose made sense of how to comprehend the whole cloud handling and inspect about the cloud security issues. [10] Have delineated a security of data to secure information in cloud achieved by Third Party Auditor (TPA), which check the reliability of the dynamic data set away in cloud and play out different inspecting assignments in the meantime. Each activity on data is added with check tag. In [11] cloud enlisting issues were sketched out i.e.

Steadfast quality, Availability and Security and it gives the open response for cloud issues. It laid out and portrayed all around requested virtualization levels of cloud figuring security. The essential cloud security issues were distinguished in [12] and it gives the course of action in cloud handling. It proposes the logical scientific classification design of security in cloud handling by disengaged the security issue and security course of action with assembled control. A multi cloud database display has proposed in [13] and it exhibited the outline of multi cloud database appear and depicts the layers and portions. [14] have inspected the security issues and discuss all the undeniable typical for cloud i.e multi-inhabitance, versatility and outsider control, by then separate the cloud security necessities i.e. grouping, respectability and openness ultimately shorten the issues in security while cloud preparing and cloud plan.

III. CLOUD SERVICES

In the Web, Cloud preparing is definitively giving advantages. The Service models are Infrastructure, Platform and Software is discussed as underneath. Cloud handling gives different encouraged organizations. The diverse organization models immediately discussed before have moreover been explained as underneath, to reveal their tremendousness with an extent of security risks en-strength in the review

A. Infrastructure as-a-Service (IaaS): It is furthermore said as Resource Clouds generally give resources and can be scaled up, as organizations to a group of customers. They fundamentally supply transcendent virtualization capacities. Along these lines, diverse resources may be offered by methods for an organization line: Data and limit mists convey to the table a dependable access to data of a possibly colossal size. The accomplishment rate of data gets the opportunity to describe the idea of these cloud servers. As establishment can be continuously scaled up or down for the need of usage resources, it gets ready different tenants meanwhile. Furthermore, the benefits that are used are generally charged by the providers.

B. Platform as-a-Service (PaaS): It supplies computational resources by methods for a phase where upon applications and organizations can be urbanized and encouraged. In other way, it supplies all the expected resources for amass an application and organization through the web, without downloading or presenting it. PaaS generally makes usage of over the best APIs to mastermind the execution of a server encouraging engine which completes and rehashes the execution as showed by buyer requests. As each supplier revealed their own specific API as showed by the individual key conceivable outcomes, applications delivered for one correct cloud provider can't be enthused to an additional cloud have; there is anyway attempts to make more prominent sweeping programming models with cloud limits.

C. Software as-a-Service (SaaS): It is also implied as Application or a Service Clouds. SaaS is the model which has the application as a help of its different cloud customers by methods for web. The customer utilizes the item out of the case with no compromise or setting up with any edge work. Organization mists give an execution of unequivocal business limits and business frames as indicated by the essential.

IV. CLOUD COMPUTING SECURITY CHALLENGES

Security is the basic perspective for a few relationship for cloud allotment. Mystery, affirmation, respectability, non-denial, and availability for client's systems are the general benchmarks of security. Get the chance to control is another fundamental factor for security. There are heaps of security threats to Cloud Service. A singular imperfection in one client application could empower a malignant developer to get access for in excess of one client's data. This issue is known as data cracks. The in-arrangement setback is another issue that happens when the unapproved customer may eradicate or change the entire records in the cloud if there is the lack of protection in cloud provider side. Questionable APIs and weak interfaces are another typical security challenges in cloud handling.

Cryptography is additionally a strategy for changing over data into indistinguishable frame amid capacity and transmission that it appears to be waste to interloper. The indistinguishable data called as cipher text. Exactly when data is gotten by recipient, it will appear as unique called as plain text. Changing over to cipher text from plain content called encryption and turnaround of this (cipher content to plain content) is known as decryption. Encryption occurs at sender's end while unscrambling occurs at collector's end. There are three sorts of cryptography calculations. Delegated Symmetric, Asymmetric and Hashing. In hashing a signature with fixed length is made with the help hash work or algorithms for the encryption of information. Each message comprises of various hash value, but the hashing has one drawback i.e. once the information is encrypted, it can't be decrypted.

This confinement of hashing was evacuated by the algorithm of symmetric and asymmetric. "Secret Key Encryption Algorithm" in symmetric key calculation and single key is utilized. i.e. private key, where as in asymmetric algorithms both the keys(Public and Private) are utilized, asymmetric algorithms is otherwise called "Public Key Encryption Algorithm".

V. CRYPTOGRAPHIC ALGORITHMS - COMPARISON

A. SYMMETRIC ALGORITHMS: Here Symmetric algorithms include a single shared secret key to encode as well as decode the information and are proficient of pre- paring a large amount of data and from processing outlook are not extremely power intensive, so has bring down overhead on the frameworks. It has high speed to encrypt and decrypt the user information with good performance. Symmetric algorithms encode the plaintexts as either Stream ciphers or Block ciphers with the fixed number of 64-bit units.

1) AES: This Cryptographic algorithm is symmetric block cipher with iterative, which implies that, AES algorithm works by re- hashing the same characterized steps again and again. AES algorithm consists with a Secret key. AES algorithm works on a

predetermined number of bytes. AES encryption algorithm and also most of the encryption algorithm is reversible. Such that, nearly similar steps were performed to finish both the encrypt and decrypt in reversible order. The algorithm mainly deals with bytes (i.e) it function with bytes, easy to employ and clarify. This key is extended into individual sub keys, which mean a sub keys for all operations. This procedure is called Key Expansion.

PSEUDO CODE – AES Algorithm

a) Choose a password (P) and a salt value(S).
b) Get the current time as T.
c) Compute key K = S + T.
d) Encrypting the password P along with Key K which creates the CT(Cipher Text) CT =AESencrypt(P,K)
e) AES encrypt function which does the following process Sub Bytes(SB)-Shift Rows(SR)-Mix Columns(MC) Add Round Key(ARK)
f) Decrypt the CT to get plane text Password P by reversing the above process.
g) Compute K=S-T
h) Plain text password P will obtain by repeating the step 4 in reverse order. P=AESdecrypt(CT,K)

2) BLOW FISH: Blowfish is one of the Symmetric Cryptographic Algorithm of Block Cipher(BCSCA) and utilized for encrypt and decrypt the texts. It uses a Variable length key and composed as a quick and free option compare with existing encryption algorithm. Blowfish Algorithm works 16 times. The square size is initially 64 bits then it can be extended till 448 bits. Each round comprises of XOR with expansion of keys and information encryption.

PSEUDO CODE – BlowFish Algorithm

a) Input a 64-bit data to Y
b) Divide Y into two halves: yL, yR(each 32 bit).
c) Compute below step for 16 times starting from P1,P2…..P16 yL = yL XOR Pi yR = F(yL) XOR yR
d) Swap yL and yR
e) After the 16th round, swapping yL and yR again with undo the last swap.
f) Compute yR = yR XOR P17 and yL = yL XOR P18.
g) Finally, recombine yL and yR to get the cipher text.
h) Then getting Decryption same as encryption, but P1 Upto P18 are in the order (reverse).

B. ASYMMETRIC ALGORITHMS: Public key cryptography, otherwise called asymmetric cryptography, denotes to a cryptographic algorithm which involves two different keys, one of which is secret key or private key and other one is public key. Even though dissimilar, the two sections of this key combination are scientifically connected. The Public key for encoding plain content or to confirm a digital signature, likewise the private key is utilized to decode the cipher text or to make an advanced digital signature. The term "Asymmetric" stems from the utilization of various keys to play out these inverse capacities each being the inverse of the other as appeared differently in relation to expected "symmetric" cryptography which depends on a similar key to perform both.

1) DIFFIE HELLMAN: Diffie Hellman key exchange is a definite technique for exchanging cryptographic keys. This strategy permits two user's that have no preceding information of each other to mutually set up a common secret key over an uncertain communication channel. This key would then be able to be utilized to encode succeeding correspondences utilizing a symmetric key cipher. The algorithm is itself restricted to the exchange of keys. This algorithm depends for its viability on the trouble of computing discrete logarithms.

PSEUDO CODE – Diffie Hellman Algorithm

a) Firstly, S and R are large prime numbers as p1 and p2. These integers kept as secret. S and R can use an insecure channel.
b) S chooses another random number as large i.e (x) and calculates c such that c=p2x mod p1
c) S sends the number c to R
d) R selects another random integer i.e
(y) as independent and find d (i.e) $d=p2^y \bmod p1$
e) R sends number d to S
f) S now compute the secrete key Key1 as follows $Key1= d^x \bmod p1$
g) R now computes the secret key Key2 as follows. $Key_2=c^y \bmod p1$

2) RSA: RSA is generally used as Public-Key cryptography algorithm defined in 1977. RSA algorithm is employed to encrypt the user information to offer security with the objective that the concerned client can only get the information. First user information is encoded and after that it is deposited in the Cloud. Whenever required, client puts a demand for the information from the Cloud service provider; Cloud supplier verifies and conveys the client data.

RSA is also called as block cipher because each message is mapped to a whole number. RSA comprises of Public-Key and Private-Key. In our Cloud atmosphere, all known with public key, while private key known who initially possesses the information. Subsequently, Cloud service provider does the encryption and decryption is handled by the Cloud client or user. Once the information is encoded with the Public-Key, it can be decoded with the equivalent Private-Key only.

PSEUDO CODE – RSA Algorithm

a) Choose the prime numbers p and q with distinct

b) Calculate the n = p*q.
c) Select the e as public key that not a factor of which is (p-1) and (q-1)
d) Select the public key d which satisfies the (d*e) mod (p-1)*(q-1)=1.
e) Encrypting the PT to get CT(Cipher Text) CT=PT e mod n
f) Sending Cipher text CT to the receiver.
g) Decrypting the CT to get plain text PT CT d mod n

C. HASHING ALGORITHMS: Cryptographic Hash functions are the most essential tools in the field of cryptography and are utilized to accomplish various security objectives like genuineness, Digital Time Stamping, Digital signature, Digital Steganography, pseudo number generation and so forth. The hash functions utilized in various information processing applications to accomplish different security objectives is substantially more far reaching than the utilization of the block cipher and the stream cipher. Hash capacities are to a great degree of valuable and appear in all data security applications. A hash work is a scientific methodology that changes over numerical information into compacted numerical information. The input to the hash work is of self-assertive length but the yield is dependably of fixed length. Qualities derived in the hash function also called as message digest or just hash values.

1) SHA-3: The Secure Hash Algorithm can be utilized to create a message known as Message Digest. As determined in that Digital Signature Standard (DSS), the SHA3 algorithm combined along with that Digital Signature Algorithm and at whatever point a protected hash algorithm is required. The transmitter and expected message of receiver in calculate and confirm a digital signature utilize the SHA3. SHA3 is utilized for registering an information record. At the point when a message length less than 64 bits of two is input, the SHA3 produces a 160-bit yield known as Message Digest. The message digest would then be able to be a contribution to the DSA, which produces or checks the mark for the message. Marking the message process as opposed to the message frequently enhancing the effectiveness of the procedure in that the message process is normally much smaller in measure than the message. A similar algorithm must be utilized by an advanced signature as was utilized by the maker of the computerized signature .
The SHA3 is called secure on the grounds that to invent a message which relates to a given message digest or to discover two unique messages which create a similar message digest. Any change to a message in travel will, with high likelihood, result in an alternate message process, and the mark will neglect to check.
PSEUDO CODE – SHA-3 Algorithm
a) Input a Message M, a pointer to the Message p and byte length of M as BL.
b) Compute z = 128M + p, 0 ≤ s 128
If p ≤ 111, the numberof calls to update is (M+1)
If p > 111, the number of calls to update is (M+2)
c) Denote M = floor (x/64) and s = z mod 64, and
d) Consider the last block LB as zero LB=Null
e) Assign the string to the blocks as
LB[byte 0] = 0x80 Till LB [byte 15]
f) Append(M, LB)
g) Compute till M(BL)/128
Update (hash, M)
Compute M = M+128
h) Now hash will be the Message digest.

2) MD5: The MD5 algorithm produces a 16 byte hash value of length 128-bit , which is usually conveyed in text format as 32 hexadecimal number digits. Cryptographic applications uses MD5 algorithm in various ways, and generally used for verifying data integrity. MD5 algorithm processes a variable length to fixed length. The message output will be 128 bits size. The user message then fragmented into 512 bit blocks chunks (i.e) the message expanding like 16 times of 32-bit words) so the length can be divisible by 512 bit blocks. Padding acts according to the following steps: initially a bit single as 1, and attached to the end or the last position of the message. This is trailed by as several numbers of zeros, which is required to get the message length up to 64 bits which is less than a multiple of 512. The rest of the bits with 64 bits and the length of first message, which is modulo of 264. The fundamental MD5 algorithm works on a 128 bit, partitioned into 32 bit words of four. These are set to certain A to D fixed constants. The fundamental algorithm then practices each Message block of 512 bit to modify the state. It involves four similar stages, as mentioned above, is termed as rounds; each round with 16 operations to view.
PSEUDO CODE – MD5 Algorithm
a) Input the message block M of size 512 bits.
b) Split M into 16 32-bit words as M0, M1, M2,... M15.
c) Split the state into four as A,B,C,D
d) Store the state in some variables: A->A', B->B', C->C' and D->D'
e) Compute the below steps for 64 rounds:
i. Compute T = B + ((A + fi(B, C, D) + Mk + Xi) <<< si).
ii. Rotate the state words: D -> A, C ->D, B ->C, T ->B.
f) Add the stored state values to the state variables: A + A' ->A, B + B' ->B, C + C' ->C, D + D' ->D

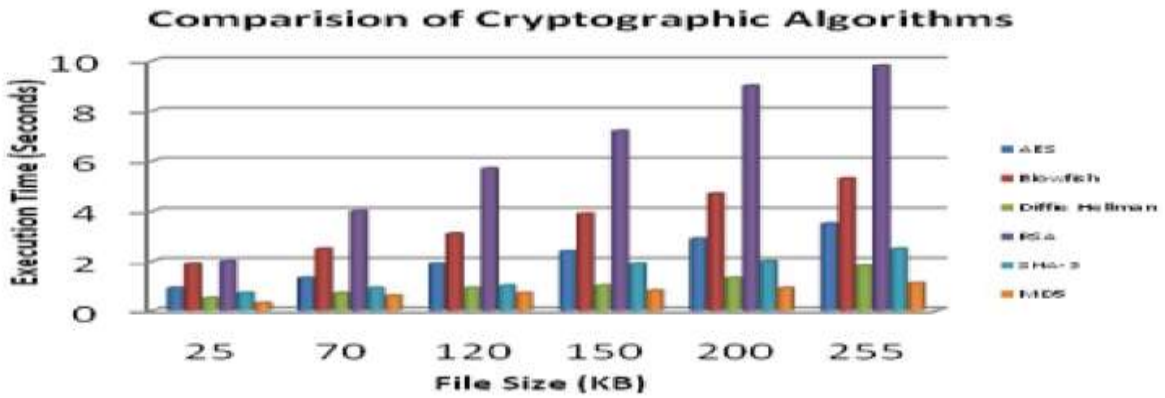
g) Finally that new running state value is the hashed value.

VI. RESULTS AND DISCUSSION

The comparative study of this Cryptographic algorithm was studied, implemented and experimented the Performance of algorithms(Encryption and Decryption). The evaluation is intended to find the performance of the cryptographic algorithms by dividing the algorithms by their nature as Symmetric Algorithms, Asymmetric Algorithms and Hashing algorithms. The performance calculation for Encryption and Decryption of algorithm was done based on the execution time of each algorithm for different file size. Cryptography is the important methodology of the modern network security innovations that enable us to send secure information over an unreliable channel and to ensure the significant information on the web, extranet, and the intranets. This paper analyzed various techniques for information security in the cloud. Different encryption techniques were proposed by the researchers to make cloud information secure, defenseless were discussed. In continuation with that security issues, challenges and furthermore techniques of Encryption Decryption algorithms have been made between Symmetric, Asymmetric and Hashing algorithms (i.e) AES, Blowfish, Diffie Hellman, RSA, SHA-3 and MD5 calculations to find the best security algorithm for our further process as a part of distributed computing for making cloud information secure and not to be hacked by attackers. The algorithms of Encryption and Decryption are very important in data security on cloud; here the cryptographic algorithms comparison is done based on values of Execution Time. It has been noted that AES calculation takes the smallest time to execute cloud information. Blowfish and SHA-3 is slightly high in Execution Time, whereas RSA devours longest time.The future extent of this work is to discover a capable algorithm to influence the information to secure by consolidating Diffie Hellman and MD5 calculation and utilize some compression algorithm for the security of information.

Table 6.1: Comparison of Cryptographic algorithms

File Size(KB)	AES	Blowfish	Diffie Hellman	RSA	SHA-3	MD5
25	1.0	1.8	0.4	1.9	0.4	0.2
70	1.3	2.3	0.5	3.9	0.6	0.4
120	1.9	3.0	0.6	5.8	0.8	0.4
150	2.2	3.9	0.7	7.1	1.5	0.6
200	3.0	4.4	0.8	9.0	1.9	0.7
255	3.8	4.7	0.9	9.8	2.4	1.0



REFERENCES

[1] Nelson Gonzalez, Fernando Redigolo, "A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing", IEEE Third International Conference on Cloud Computing Technology and Science 2011.

[2] Ms.Anupma Sehrawat , Ms.Neha Bishnoi, "Survey Paper on Basics of Cloud Computing and Data Security", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014.

[3] Rajiv R Bhandari, Nitin Mishra "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish-algo.",International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321-8169,Volume: 1 Issue: 4 217- 223,April 2013.

[4] Rachna Arora, Anshu Parashar "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 ,Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926

[5] V. Krishna Reddy, Dr. L.S.S.Reddy, "Security Architecture for Cloud Computing Platform", International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462 Vol. 3 No. 9 September 2011

[6] Sadia Marium, Qamar Nazir, Aftab Ahmed, Saira hthasham Mirza Aamir Mehmood, "Implementation of Eap with RSA for Enhancing The Security of Cloud Computing",International Journal of Basic and Applied Sciences, 2012,177-183.

[7] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, Cesar A. F. De Rose and Rajkumar Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms". Wiley Online Library, DOI: 10.1002/spe.995, 2011.
[8] Nagi Reddy, B. Ravi Prasad, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013.
[9] Ramgovind S, Smith E, "The Management of Security in Cloud Computing", 978-1-4244-5495-2/10, IEEE Transaction, 2010.
[10] Cong Wang, Kui Ren, Wenjing Lou, and JinLi, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, no. 5, May 2011.
[11] Farzad Sabahi, "Virtualization-Level Security in Cloud Computing", Faculty of Computer Engineering Azad University Iran, 978-1-61284-486-2/11, IEEE Transaction, 2011.
[12] Mats Naslund and Makan Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing", 978-0-7695-4622-3/11, IEEE Transaction, 2011.
[13] Ben Soh , Eric Pardede, "MCDB: Using Multi- Clouds to Ensure Security in Cloud Computing", 978-0-7695-4612-4/11, IEEE Transaction, 2011.
[14] Huaglory Tian_eld, "Security Issues In Cloud Computing", School of Engineering and Built Environment Glasgow Caledonian University, United Kingdom, 978-1- 4673-1714-6/12, IEEE Transaction, 2012.