iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1373

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal For Research In Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available AT www.Ijraset.com

Cryptographic Algorithms used in Cloud Computing – an Analysis and Comparison

S. Rajendirakumar[1], Dr. A.Marimuthu[2]
[1]*Assistant Professor of Computer Science, Govt. College for Women, Kolar, Karnataka*
[2]*Associate Professor of Computer Science, Govt. Arts College, Coimbatore, Tamilnadu*

Abstract: ***Cloud Computing- A technology which provides the on-demand Information Technology services for the customer through the internet. Cloud computing facilitates the user by providing the resources of third party in the name of infrastructure, hardware and software over the network. Infrastructures of Cloud computing makes the user to access the data anywhere at any time as long as the user's device has access with the internet. Such activity improves the use of internet application which provides "pay as you go" facility. Hence this flexibility creates an impact upon the user and made them to transfer their data to cloud. But it may lay some security issues also. Cryptographic algorithms were implemented to overcome the security issues and to ensure the Cloud computing data security. Nowadays many techniques of this encryption and decryption were proposed to maintain security in cloud data. Here a study was made on this cryptograpic algorithms and a comparative analysis was presented.***

Index Terms: Cloud Computing, Cryptography, Encryption, Decryption, AES, RSA, MD5.

I. INTRODUCTION

Cloud computing has developed as an exceptionally understood strategy to help extensive and voluminous information with the assistance of shared pool of assets and vast stockpiling territory. [1] States that "Cloud computing is another registering worldview that is based on virtualization, disseminated figuring, utility processing and administration situated engineering". Further it is included that cloud computing has developed as very most critical worldview of the IT business and has pulled in the greater part of the business and the scholarly community.

[2] have characterized about cloud computing. Cloud computing, without a doubt, is a far reaching term that gives more internet benefits. These are isolated into three general classes [3]: Infrastructure-as-a-Service , Platform-as-a-Service and Software-as-a-Service. The web is generally spoken to as the "Cloud". The most part a cloud service is utilized by the customers as and when required, regularly on the hourly premise. This "on-request" or "pay as you go" approach influences the cloud to benefit adaptable, where end client can have an incredible arrangement or unassuming of an administration the way they want at any point of time and the administration is completely regulated by the supplier. Vital upgrades in each key parts included virtualization conveyed registering and furthermore the enhanced access to rapid web office and in addition feeble economy has speeded up the expansion of cloud computing thoroughly.

As cloud figuring appreciates processing as an adequacy, suppliers are building up a common shared gathering of configurable assets, which customers can energetically condition and free as indicated by their changing needs. In this way, both gathering the suppliers and the clients would effortlessly profit by the reuse of figuring assets and diminishing in cost.

The cloud benefits that are actualized will be executed and dependable with few threats. Initial steps needed to avert these threats. Subsequently security is the main worry those who want to use cloud administrations. As indicated by [4] there exist a portion of the fundamental security dangers that endeavor the Cloud computing utilization that spreading spam and malware activity of botnets. The other case is the application interfaces that are required to associate with cloud benefits particularly that are produced by outsiders. These interfaces must furnish the client with much secured verification, approval, encryption and development observing systems

This paper designed as follows: Section 2 is the works that related to cloud computing data security. Section 3 is related to the cloud computing services. Section 4 discusses cloud computing security challenges. Section 5 explains the cryptographic algorithms used in this research. Section 6 illustrates the cryptographic algorithms implementation. Section 7 shows the conclusion of our work.

II. RELATED WORKS

The most essential objective in [5] is conveying consistent access to control, service, verification and administration arranged engi-

©IJRASET (UGC Approved Journal): All Rights are Reserved

neering administration to end client. It concentrated on gathering the secure and generic design for that cloud computing platform without knowing its services and models. In cloud computing, information is shield from the unapproved individual, denial of service and service abuse. In [6] the features of cloud security strategies, protection issues have concentrated on service provider side security and proposed the extensible validation convention for confirmation with RSA calculation.

In [7] difficulties in assessing the cloud approaches, resource performance and application work load is depicted as extremely hard to accomplish, thus it proposed, To accomplish securing and secure access to control, [8] utilize exceptionally joining procedures of Attributes Based Encryption(ABE), intermediary decryption and relaxed decryption. It has portrayed cryptographic strategy, which give better secrecy and security of sensitive information outsourced by client shared on cloud server.

In [9] feature each of security prerequisites of cloud computing were highlighted and telling about how to deal with the cloud computing security. It have portrayed and feature the general security concern whose figured out how to understand the entire cloud processing and examine about the the cloud security issues. [10] Have depicted a security of information to put away data in cloud accomplished by Third Party Auditor (TPA), which check the trustworthiness of the dynamic information put away in cloud and play out various examining assignments at the same time. Every operation on information is appended with verification tag.

In [11] cloud registering issues were outlined i.e. Unwavering quality, Availability and Security and it gives the accessible answer for cloud issues. It outlined and described well-ordered virtualization levels of cloud figuring security. The primary cloud security issues were identified in [12] and it gives the arrangement in cloud processing. It proposes the scientific taxonomy architecture of security and protection in cloud processing by isolated the security issue and security arrangement with gathered guide. A multi clouds database model has proposed in [13] and it presented the design of multi cloud database show and portrays the layers and segments. [14] have examined the security issues and talk about all the unmistakable normal for cloud i.e multi-occupancy, versatility and so forth and outsider control, at that point break down the cloud security requirements i.e. classification, respectability and accessibility lastly abridge the issues in security while cloud processing and cloud design.

III. CLOUD SERVICES

In the Web, Cloud processing is conclusively giving benefits. The Service models are Infrastructure, Platform and Software is talked about as beneath. Cloud processing gives various facilitated administrations. The different administration models quickly talked about before have additionally been expounded as beneath, to uncover their hugeness with a scope of security dangers encourage in the overview [15]:

A. Infrastructure-as-a-Service (IaaS)

It is additionally mentioned as Resource Clouds for the most part give assets and can be scaled up, as administrations to an assortment of clients. They basically supply predominant virtualization abilities. Thus, different assets might be offered by means of an administration line: Data and capacity clouds bring to the table a tried and true access to information of a conceivably huge size. The achievement rate of information gets to characterize the nature of these cloud servers. As foundation can be progressively scaled up or down for the need of utilization assets, it prepares various occupants in the meantime. Additionally, the assets that are utilized are for the most part charged by the suppliers.

B. Platform-as-a-Service (PaaS)

It supplies computational assets by means of a stage where upon applications and administrations can be urbanized and facilitated. In other way, it supplies all the required assets to assemble an application and administration through the web, without downloading or introducing it. PaaS traditionally makes utilization of over the top APIs to arrange the execution of a server facilitating motor which finishes and repeats the execution as indicated by purchaser demands. As every provider uncovered their own particular API as indicated by the individual key possibilities, applications produced for one exact cloud supplier can't be enthused to an extra cloud have; there is however endeavors to make greater expansive programming models with cloud capacities.

C. Software-as-a-Service (SaaS)

It is additionally alluded to as Application or a Service Clouds. SaaS is the model which has the application as a support of its different cloud clients by means of web. The client uses the product out of the case with no reconciliation or fixing up with any framework. Administration clouds give an execution of unequivocal business capacities and business forms according to the prerequisite. These applications are given with unambiguous cloud capacities utilizing a cloud framework or stage as opposed to giving a cloud

©IJRASET (UGC Approved Journal): All Rights are Reserved

to them. Over and again, sorts of standard application programming usefulness are realistic inside a cloud. One most advantage of SaaS is that it helps in costing less cash than really purchasing the application. It gives less expensive and dependable applications to the association.

The three cloud administrations portrayed above draw in some profoundly critical measure of dangers. This incorporates alteration of information without appropriate reinforcement, prompting information ruptures or unapproved access to touchy information. If there should arise an occurrence of legitimate information reinforcement being taken, it is defenseless that not encoded appropriately. Unsecured access to assets over the cloud may prompt unapproved utilization of administration, stage or even a framework of the supplier or different clients due to the related hindrances of virtualization.

IV. SECURITY CHALLENGES IN CLOUD COMPUTING

Security is the imperative viewpoint for some associations for cloud appropriation. Secrecy, confirmation, respectability, non-revocation, and accessibility for customer's frameworks are the general standards of security. Get to control is another vital factor for security. There are loads of security dangers to Cloud Service. A solitary defect in one customer application could enable a malignant programmer to procure access for more than one customer's information. This issue is known as information ruptures. The information misfortune is another issue that happens when the unapproved client may erase or change the whole records in the cloud if there is the defenselessness in cloud supplier side. Unreliable APIs and feeble interfaces are another normal security challenges in cloud processing.

Cryptography is also a method of changing over information into unreadable form during storage and transmission that it seems waste to intruder. The unreadable information called as cipher text. At the point when information is gotten by receiver, it will show up in the form of original called as plain text. Converting to cipher text from plain text called encryption and turnaround of this (cipher text to plain text) is known as decryption. Encryption happens at sender's end while decryption happens at receiver's end. There are three types of cryptography calculations[16]. Classified as 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 decodethe information and are proficient of preparing 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 rehashing 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[17]. 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)

©IJRASET (UGC Approved Journal): All Rights are Reserved

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[18].

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[19]. 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

$c=p2^x \bmod p1$

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 Key_1 as follows

$Key_1= d^x \bmod p1$

g) R now computes the secret key Key_2 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 informa-

©IJRASET (UGC Approved Journal): All Rights are Reserved

tion 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 [20]. 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
CTd 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 [21]. 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 number of 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]

©IJRASET (UGC Approved Journal): All Rights are Reserved

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.

a) *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.[22].

PSEUDO CODE – MD5 Algorithm

b) Input the message block M of size 512 bits.
c) Split M into 16 32-bit words as M0, M1, M2,... M15.
d) Split the state into four as A,B,C,D
e) Store the state in some variables: A → A', B → B', C → C' and D → D'

f) 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.
g) Add the stored state values to the state variables:
A + A' → A, B + B' → B, C + C' → C, D + D' → D.
h) Finally that new running state value is the hashed value.

VI. EXPERIMENTAL RESULTS

The comparative study of this Cryptographic algorithm was studied and implemented in java environment 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.



FIGURE 6.1 - MAIN SCREEN OF THE RESEARCH WORK

©IJRASET (UGC Approved Journal): All Rights are Reserved

International Journal For Research In Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available AT www.Ijraset.com

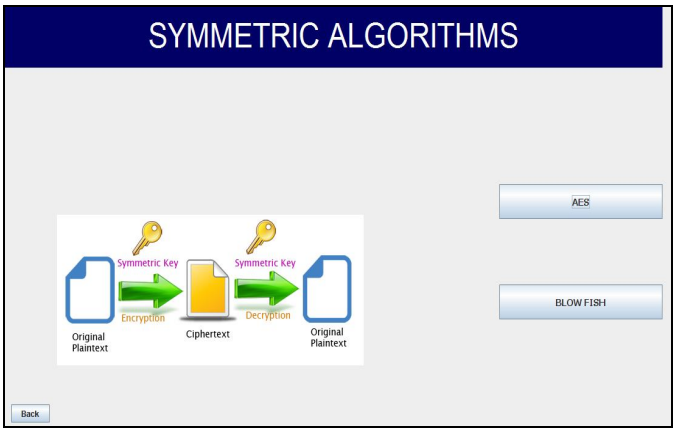


FIGURE 6.2 – SYMMETRIC ALGORITHMS TAKEN FOR STUDY.

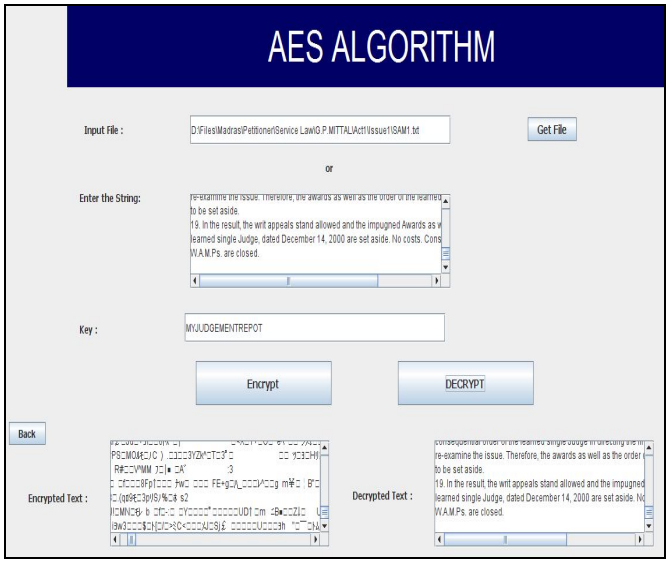


FIGURE 6.3 – ENCRYPTION AND DECRYPTION USING THE AES ALGORITHM

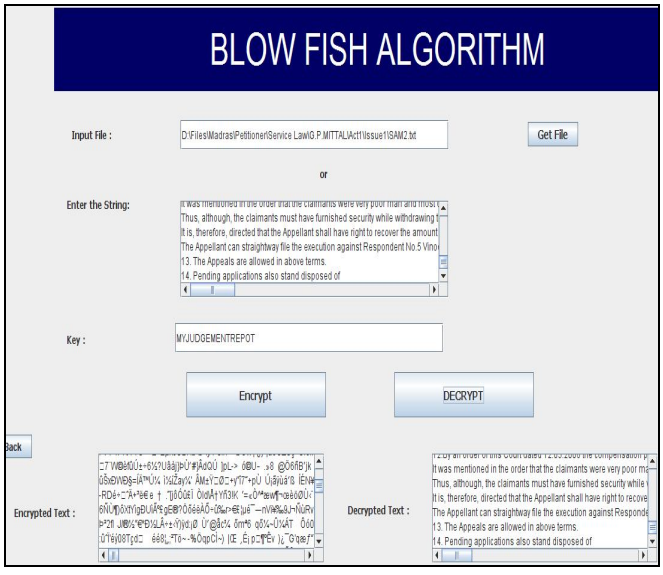


FIGURE 6.4 – ENCRYPTION AND DECRYPTION USING THE BLOWFISH ALGORITHM

©IJRASET (UGC Approved Journal): All Rights are Reserved

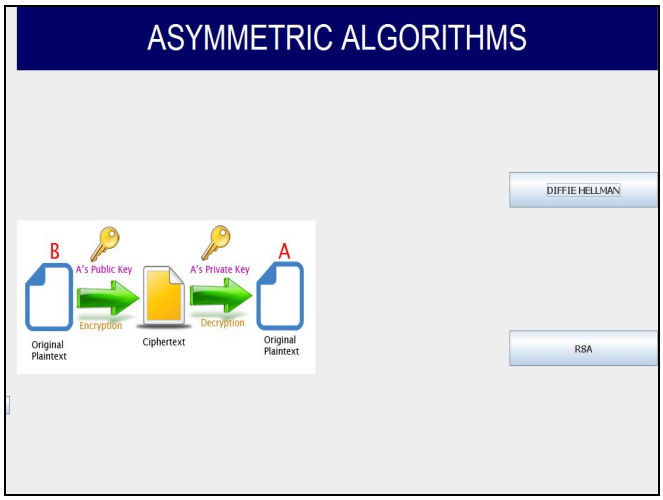


FIGURE 6.5 – ASYMMETRIC ALGORITHMS TAKEN FOR STUDY.

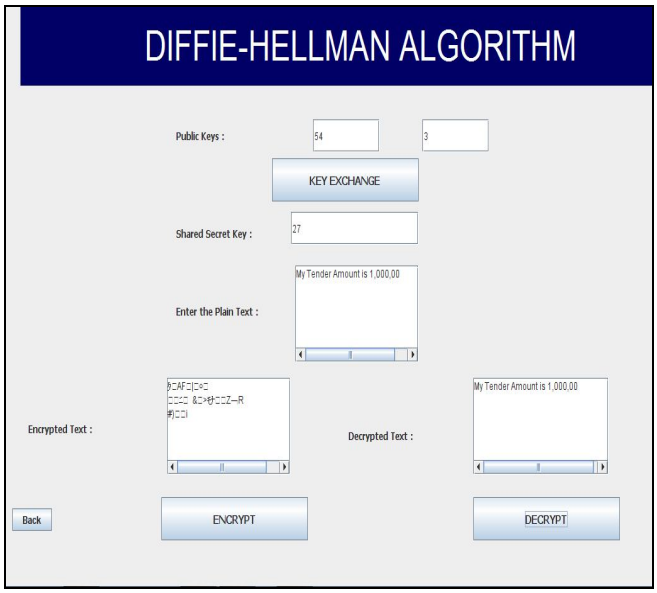


FIGURE 6.6 – ENCRYPTION AND DECRYPTION USING THE DIFFIE HELLMAN ALGORITHM

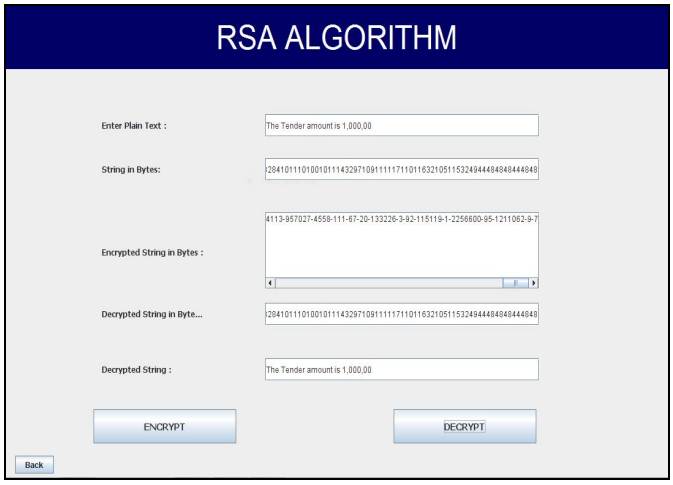


FIGURE 6.7 – ENCRYPTION AND DECRYPTION USING THE RSA ALGORITHM

©IJRASET (UGC Approved Journal): All Rights are Reserved

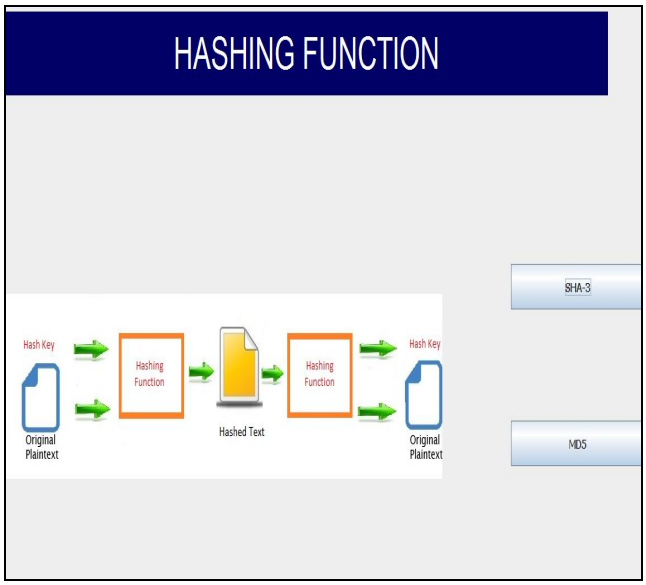


FIGURE 6.8 – HASHING ALGORITHMS TAKEN FOR STUDY.

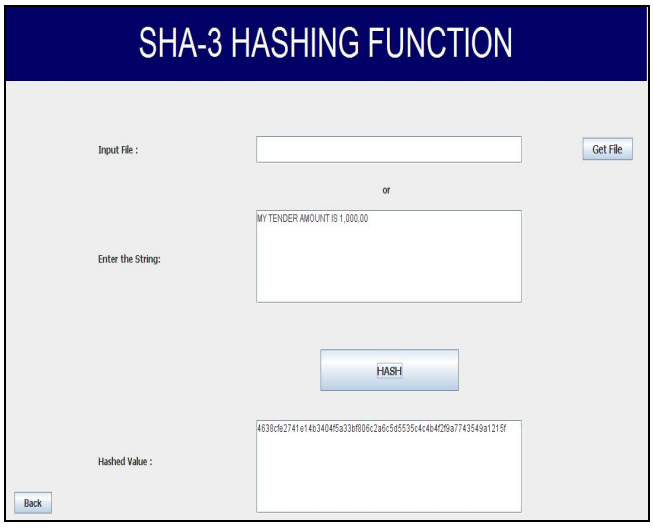


FIGURE 6.9 – GENERATING HASH VALUE USING THE SHA-3 ALGORITHM

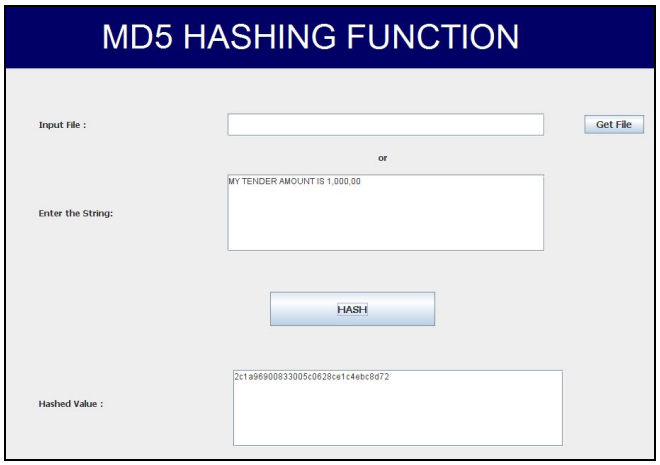


FIGURE 6.10 – GENERATING HASH VALUE USING MD5 ALGORITHM

©IJRASET (UGC Approved Journal): All Rights are Reserved

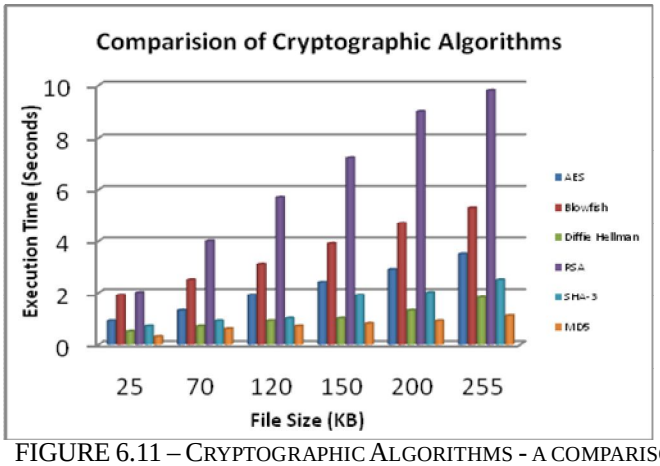


FIGURE 6.11 – CRYPTOGRAPHIC ALGORITHMS - A COMPARISON

VII. CONCLUSION

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.

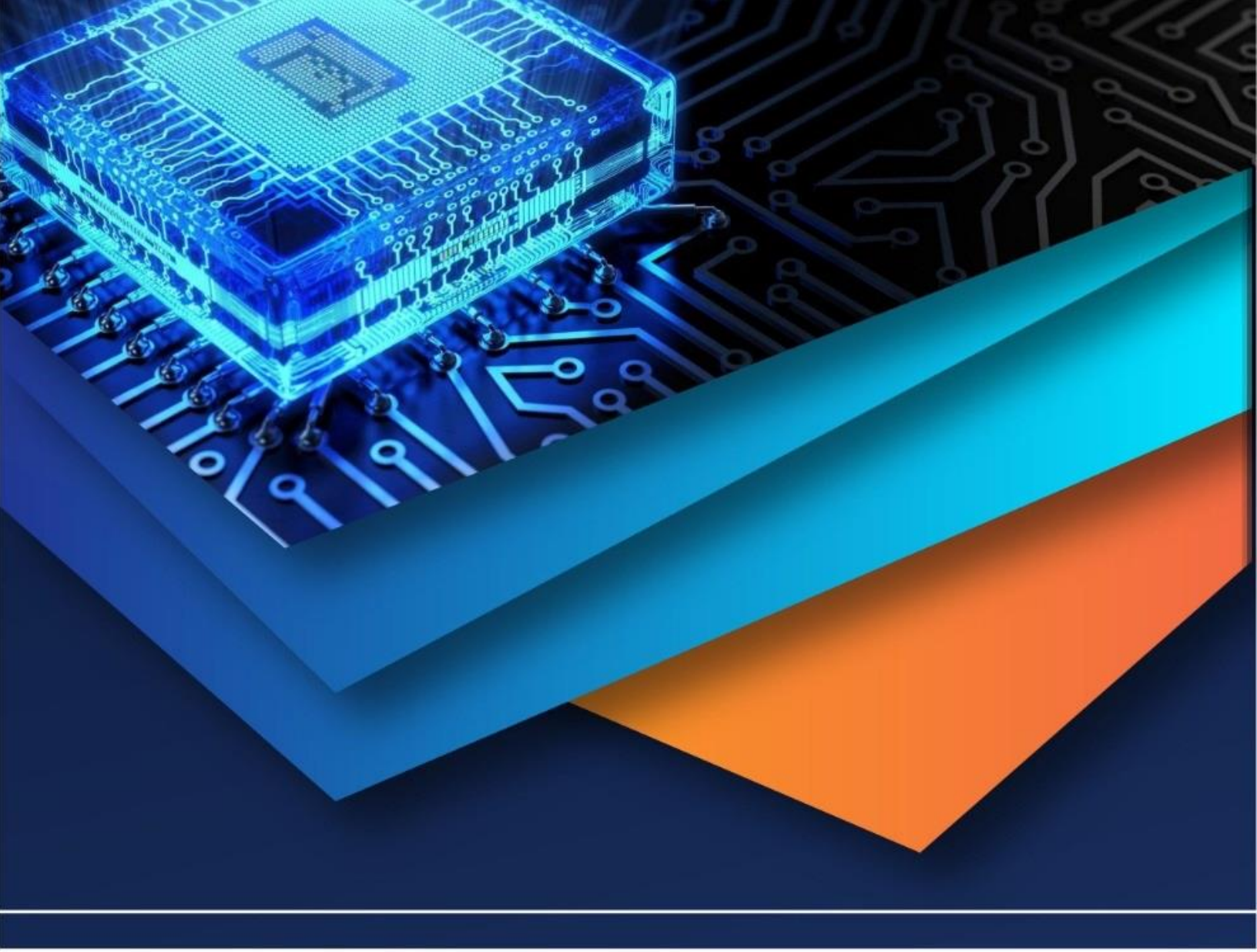
REFERENCES

[1] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund, Makan Pourzandi "A quantitative analysis of current security concerns and solutions for cloud computing", Springer 2012.
[2] Alexa Huth and James Cebula, "The Basics of Cloud Computing", United States Computer Emergency Readiness Team. 2011.
[3] G Devi, Pramod Kumar "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm", IJCTT, 2012.
[4] Rachna Jain and Ankur Aggarwal "Cloud Computing Security Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 1, 2014.
[5] Sanjana Dahal, "Security Architecture for Cloud Computing Platform", Master of Science Thesis Stockholm, KTH Industrial Engineering and Management, TRITA-ICT-EX-2012:291, Sweden, 2012.
[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, 177-183, 2012.
[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] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", 978-1-4244-5837-0/10, IEEE Transaction, 2010.
[9] Ramgovind S, Elo_ M M, Smith E, "The Management of Security in Cloud Computing", 978-1-4244-5495-2/10, IEEE Transaction, 2010.
[10] Qian Wang, 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] Nelson Gonzalez, Charles Miers, Fernando Redgolo, Tereza Carvalho, Marcos Simplicio, 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] Mohammed A. AlZain, Ben Soh and Eric Pardede, "MCDB: Using Multi- Clouds to Ensure Security in Cloud Computing", 978-0-7695-4612-4/11, IEEE Transaction, 2011.

©IJRASET (UGC Approved Journal): All Rights are Reserved

[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.
[15] A. Iosup, S. Ostermann, N. Yigitbasi, R. Prodan, T. Fahringer, D. Epema, Performance analysis of cloud computing services for many-tasks scientific computing, IEEE Transactions on Parallel and Distributed Systems 22 (6), P.no: 931–945, 2011.
[16] Shakeeba S. Khan and Prof. R.R. Tuteja, 'Security in Cloud Computin Using Cryptographic Algorithms', International Journal of Innovative Research in Computer and Communication Engineering. ISSN (online): 2320-9801, (Print): 2320-9798 Vol. 3, Issue, 2015.
[17] Jawahar Thakur, Nagesh Kumar,"DES,AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," in International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, pp.6-12, 2011.
[18] Meyers, R.K.; Desoky, A.H. "An Implementation of the Blowfish Cryptosystem" Signal Processing and Information Technology, ISSPIT 2008, IEEE International Symposium.pp 346 – 351, 2008.
[19] S. Anahita Mortazavi, Alireza Nemaney Pour, Toshihiko Kato,"An Efficient Distributed Group Key Management using Hierarchical Approach with Diffie-Hellman and Symmetric Algorithm: DHSA", CNDS Feb 2011.
[20] B.Persis Urbana Ivy, Purshotam Mandiwa and Mukesh Kumar, 'A Modified RSA Cryptosystem Based on 'n' Prime Number', International Journal of Engineering and Computer Science. ISSN: 2319-7242 Volume 1 Issue 2, 2012.
[21] C. Hanser, Performance of the SHA-3 Candidates in Java, Institute for Applied Information Processing and Communications Graz, University of Technology, March 19, 2012.
[22] A. Kasgar, J. Agarwal and S. Sahu "New Modified 256-bit MD5 Algorithm with SHA Compression Function", International Journal of Computer Applications (0975 – 8887) ,Vol.42,No.12, March 2012.
[23] Nandita Sengupta, Jeffrey Holmes, "Designing of Cryptography based Security system for Cloud Computing. 2013 Internatioal Conference on Cloud & Ubiquitous Computing & Emerging Technologies
[24] I. Sriram, & A. Khajesh-hosseini, "Research agenda in cloud tecnologies", in 1st ACM Symposium on cloud computing, SOCC 2010.
[25] B. Grobauer, T.Walloschek, E.Stocker, "Understanding Cloud Computing Velnerabilities", Security & Privacy, IEEE, vol.9,no.2,pp.50,57, March-April 2011 doi:10.1109/MSP.2010.115.
[26] S.Pearson, A.Benameur, "Privacy, Security and Truset Issues Arising from Cloud Computing", 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom),2010.
[27] M.A. Alzain, E.Pardede, B.Soh, J.A.Thom, "Cloud Computing Security; From single to Multi-clouds", 45th Hawaii International Conference on system Science (HICSSS), 2012.
[28] K.Wood. M. Anderson, "Understanding the complexity surrounding multitenancy in cloud computing", 2011 8th IEEE International Conference on e-business engineering. Vol.1,no.,119-124,2011.
[29] A.abdulrahaman, M.Sarfaz, et al, "A Distributed Access Control Architecture for Cloud Computing," IEEE Software, vol.12.no., 36-44, 2012.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)