IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 23-33

An Empirical study on Cryptographic Algorithms implemented in Cloud Computing Environment

P.Porkodi[1], Dr. S. Santhana Megala[2]
[1](Research Scholar, SNMV College of Arts & Science, Coimbatore)
[2](Assistant Professor, SNMV College of Arts & Science, Coimbatore)

Abstract: *Cloud computing is 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 irrespective of the physical position over the internet network. Cloud computing infrastructures allow 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. Technology implemented by Cryptographic algorithms were actualized to defeat the security issues and to guarantee the security of data that stored in cloud computing. Nowadays numerous encryption and decryption procedures have been proposed to keep up security for the data that stored in cloud environment. In this paper, an investigation was made on the distinctive cryptographic algorithms and comparative analysis was done and explained.*

Keywords: *Cloud Computing, Cryptography, Encryption, Decryption, AES, RSA, MD5*

I. Introduction

Cloud computing has developed as an exceptionally understood strategy to encourage broad and voluminous data with the help of shared pool of benefits and tremendous accumulating area. [1] cited that "Cloud computing is another index perspective that is rely upon virtualization, appropriated figuring, utility giving out and organization situated designing". Further it is included that cloud computing has developed as a standout amongst the most critical worldview of the IT business and has pulled in the greater part of the business and the scholarly group of people. [1] have epitomize distributed computing as "Cloud computing is a portrayal for engaging unavoidable, worthwhile, on-ask for sort out access to a typical pool of configurable preparing resources (e.g., frameworks, servers, storing, applications, and organizations) that can be immediately provisioned and released with irrelevant organization effort or expert co-task association".

Cloud computing, without a doubt, is a far reaching term that transmits facilitated benefits over the Internet. These technical advancement induced the Technology industry to utilize the service in three major categories (i.e) [3]: 1. Infrastructure-as-a-Service (IaaS), 2. Platform-as-a-Service (PaaS) and 3. Software-as-a-Service (SaaS). 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 redesigns in each key parts included virtualization passed on enrolling and besides the improved access to fast web office and also weak economy has speeded up the development of distributed computing altogether.

As cloud figuring values handling as ampleness, providers are developing a typical shared assembling of configurable resources, which clients can vivaciously condition and free as shown by their evolving needs. Along these lines, both get-togethers the providers and the customers would easily benefit by the reuse of figuring resources and reducing in expense.

The cloud benefits that are completed will be executed will reliably be joined by a couple of threats. Information about these threats should turn out to be the initial step to avert them. Subsequently security is the main worry of a few customers who want to use cloud administrations. As indicated by [10] there exist a portion of the fundamental security dangers that endeavor the utilization of Cloud Computing. A simple case of this is the activity of botnets to spread spam and malware. 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 organized as follows: Section 2 shows a few works that identified with the field of information security in Cloud computing. Section 3 clarify the administrations given by Cloud computing. Section 4 talks about the security challenges in Cloud computing. Section 5 clarifies the cryptographic

calculations utilized in this exploration. Section 6 outlines the usage of the cryptographic calculations. Section 7 demonstrates the conclusion of our work.

II. Related Works

The most essential objective in [14] is conveying consistent access to control, service, verification and administration arranged engineering administration to end client. It concentrated on gathering the secure and generic design for cloud computing platform without knowing its services and models. In cloud computing, information is safeguard from the unauthorized person, (DOS) Denial of Service and Service Abuse. In [13] 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 [12] difficulties in assessing the cloud approaches, resource performance and application work load is depicted as extremely hard to accomplish, thus it proposed, CloudSim an extensible reenactment toolbox whose empower models and propagation of Cloud computing systems. To achieve anchoring and secure access to control, [16] use astoundingly joining methods of Attributes Based Encryption(ABE), go-between decryption and loosened up decryption. It has depicted cryptographic technique, which give better mystery and security of touchy data outsourced by customer shared on cloud server.

In [11] 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. [9] Have delineated a security of data to secure information in cloud achieved by Third Party Auditor (TPA), which check the dependability of the dynamic data set away in cloud. TPA can play out different analyzing assignments in the meantime. Each task on data is annexed with check tag.

In [2] cloud registering issues were outlined i.e. Unwavering quality, Availability and Security and it gives the accessible answer for cloud issues. It delineate and described well-organized virtualization levels of cloud computing security. The primary cloud security issues were identified in [8] 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 [7] and it presented the design of multi cloud database show and portrays the layers and segments. [4] have analyzed the logical classification for security issues and discuss all the undeniable typical for cloud i.e multi-inhabitance, adaptability and hence forth third party control, by then separate the cloud security necessities i.e. order, respectability and openness finally abbreviate the security issues in cloud handling in light of the cloud security outline.

III. Cloud Services

Cloud processing is conclusively giving diverse facilitated benefits over the web. These facilitated administrations are comprehensively arranged in three diverse administration models, in particular Infrastructure as a Service, Platform as a Service and Software as a Service which have been talked about as beneath.

Cloud preparing gives different encouraged organizations. The distinctive organization models immediately discussed before have furthermore been explained as underneath, to reveal their hugeness with an extent of security perils support in the outline [5]:

• Infrastructure as a Service (IaaS): It is additionally mentioned as Resource Clouds for the most part give assets which are overseen and can without much of a stretch 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 accomplishment rate of data get the opportunity to portray the idea of these cloud servers.As establishment can be dynamically scaled up or down in light of the need of usage resources, it gets ready different tenants meanwhile. Furthermore, the advantages that are used are generally charged by the providers on the preface of the computational use by the customers.

• Platform as a Service (PaaS): It supplies computational assets by means of a stage whereupon 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 each supplier revealed their own specific API as demonstrated by the individual key potential 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 broad programming models with cloud limits.

• 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. Organization mists give an execution of unequivocal business limits and business frames as per the essential. These applications are given with unambiguous cloud limits using a cloud system or stage rather than giving a cloud to them.Over and again, sorts of standard application programming usefulness are realistic inside a cloud. One of the greatest advantages of SaaS, it helps in costing less cash than really purchasing the application. It gives less expensive and dependable applications to the association.

The three cloud organizations depicted above attract some significantly basic proportion of perils. This joins change of data without suitable fortification, provoking data breaks or unapproved access to sensitive data. On the off chance that there ought to emerge an event of authentic data fortification being taken, it is unprotected in case it isn't encoded suitably. Unbound access to resources over the cloud may provoke unapproved use of organization, arrange or even a structure of the provider or diverse customers because of the related preventions of virtualization.

IV. Security Challenges In Cloud Computing

Security is the basic perspective for a few relationships for cloud appointment. Mystery, affirmation, respectability, non-denial, and openness for client's structures are the general guidelines of security. Get the opportunity to control is another fundamental factor for security. There are heaps of security risks to Cloud Service. A lone imperfection in one client application could empower a harmful software engineer to obtain access to in excess of one client's data. This issue is known as data breaks. The data 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. Temperamental APIs and weak interfaces are another ordinary security challenges in cloud preparing. At the point when classified information is put away in it, the outrageous concentration ought to be given to the security of the cloud.

Cryptography is a method of changing over information into unreadable form during storage and transmission that it seems waste to intruder. The unreadable type of information is known as cipher text. At the point when information is gotten by receiver, it will show up in its original form which is known as plain text. Change of plain content to figure content is known as encryption and pivot of this (figure content to plain content) is known as unscrambling. Encryption occurs at sender's end while decoding occurs at beneficiary's end. There are three sorts of cryptography functionality [15]. They are (i) Symmetric Algorithms (ii) Asymmetric Algorithms (iii) Hashing.

In hashing a fixed length signature is made with the assistance of algorithms or hash work for the encryption of information. Each message contains different hash index value, yet the hashing has one disadvantage i.e. when the data is encrypted for security purpose, it can't be decrypted when it is needed. This constringent of hashing was emptied by cryptographic techniques like Symmetric and Asymmetric Algorithms. Symmetric algorithm is otherwise called "Secret Key Encryption Algorithm" in symmetric key calculation, just a single key is utilized for encryption and decryption i.e. private key, where as in asymmetric algorithms both public and private keys are utilized for encryption and decryption, asymmetric algorithms is otherwise called "Public Key Encryption Algorithm".

V. Comparision Of Cryptographic Algorithm

A. Symmetric Algorithms

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 for encrypt and decrypt the user information with good performance. Symmetric algorithms encode plaintexts as Stream ciphers bit by bit at a time or as Block ciphers on a fixed number of 64-bit units.

a. AES

AES cryptographic algorithm is an iterated symmetric block cipher algorithm, which implies that, AES algorithm works by rehashing the same characterized steps again and again. AES algorithm is a secret key encryption algorithm. AES algorithm works on a predetermined number of bytes. AES encryption algorithm and also most of the encryption algorithm is reversible [6]. Such that, nearly similar steps were performed to finish both the encryption and decryption in reverse order. The AES algorithm mainly deals with bytes (i.e) it function with bytes, which makes it easier to employ and clarify. This key is extended into individual sub keys, which mean a sub keys for each and every operation. This procedure is called Key Expansion.

PSEUDO CODE – AES Algorithm

1. *Choose a password (P) and a salt value(S).*
2. *Get the current time as T.*
3. *Compute key K = S + T.*
4. *Encrypting the password P along with Key K which creates the cipher text CT*
   CT =AESencrypt(P,K)
5. *AES encrypt function which does the following process*
   i. *SubBytes*
   ii. *ShiftRows*
   iii. *Mix Columns*
   iv. *AddRoundKey*
6. *Decrypting the cipher text CT to get plane text Password P by reversing the above process.*
7. *Compute K=S-T*
8. *Plain text password P will obtain by repeating the step 4 in reverse order.*
   P=AESdecrypt(CT,K)

b. Blow Fish

Blowfish is a symmetric square figure cryptographic calculation that can be sufficiently used for encryption and decoding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for anchoring data. Bruce Schneier formulated the Blowfish cryptogrphic algorithm in 1993, which gives quick process and easy implementation while comparing with existing encryption calculation.

Blowfish Algorithm draw attention to an essential encryption which works for 16 times. The square size is 64 bits, and the key can be any length up to 448 bits. Each round involves XOR task and a capacity. Each round contains key development and data encryption [20].

PSEUDO CODE – BlowFish Algorithm

1. *Input a 64-bit data element X*
2. *Divide X into two 32-bit halves: xL, xR.*
3. *For Encryption:*
   Compute below step for 16 times starting from P1,P2…..P16
   xL = xL XOR Pi
   xR = F(xL) XOR xR
4. *Swap xL and xR*
5. *After the sixteenth round, swap xL and xR again to undo the last swap.*
6. *Compute*
   xR = xR XOR P17 and xL = xL XOR P18.
7. *Finally, recombine xL and xR to get the ciphertext.*
8. *Decryption is exactly the same as encryption, except that P1, P2, ..., P18 are used in the reverse order.*

B. Asymmetric Algorithms

Public key cryptography, otherwise called asymmetric cryptography, denotes to a cryptographic algorithm which involves two separate 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 is utilized to encode 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 others appeared differently in relation to expected "symmetric" cryptography which depends on a similar key to perform both.

a. Diffie Hellman

In 1976, Whitfield Diffie and Martin Hellman conveyed the Diffie Hellman key exchange methodology. Diffie Hellman key exchange methodology is an perfect technique for exchanging the key used in the cryptographic methodology. This technique grants two client's that have no former data of one another to commonly set up a typical mystery key over a dubious correspondence channel. This key would then have the capacity to be used to encrypt succeeding transaction using a symmetric key cipher. The algorithm is itself restricted to the exchange of keys[17]. The Diffie Hellman key exchange algorithm depends for its feasibility on the difficulty of calculating discrete logarithms.

PSEUDO CODE – Diffie Hellman Algorithm

1. *Firstly, S and R agree on two large prime numbers p1 and p2. These two integers need not be kept secret. S and R can use an insecure channel to agree on them.*
2. *S chooses another large random number x and calculates c such that*
   $c=p2^x \bmod p1$
3. *S sends the number c to R*
4. *R independently chooses another large random integer y and calculate d such that*
   $d=p2^y \bmod p1$
5. *R sends number d to S*
6. *S now compute the secrete key Key_1 as follows*
   $Key_1= d^x \bmod p1$
7. *R now computes the secret key Key_2 as follows.*
   $Key_2=c^y \bmod p1$

b. RSA

RSA is generally used Public-Key cryptography algorithm. It stands for Ron Rivest, Adi Shamir and Len Adleman, who first openly defined it 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 the client and conveys the data. RSA is also called as block cipher, in which each message is mapped to a whole number. RSA comprises of Public-Key and Private-Key[21]. In our Cloud atmosphere, Pubic-Key is known to all, while Private Key is known only to the client who initially possesses the information. Subsequently, encryption is done by the Cloud service provider and decryption is finished 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

1. *Choose two distinct prime numbers p and q.*
2. *Compute n = p*q.*
3. *Select the public key e which is not a factor of (p-1) and (q-1)*
4. *Select the public key d which satisfy.*
   *(d*e) mod (p-1)*(q-1)=1.*
5. *Encrypting the Plain text PT to get cipher text CT*
   CT=PTe mod n
6. *Send Cipher text CT to the receiver.*
7. *Decrypting the cipher text CT to get plane 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 utilization of cryptographic hash functions in various information processing applications to accomplish different security objectives is substantially more far reaching than the utilization of block cipher and 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 returned by a hash function are called message digest or just hash values.

a. SHA-3

The encryption calculation SHA-3 decides a Se-fix Hash Algorithm (SHA3), which can be used to make a dense portrayal of a message called a message Digest. As decided in the Digital Signature Standard (DSS), the SHA3 calculation is required to use alongside the Digital Signature Algorithm (DSA) and at whatever point an ensured hash calculation is required. Both the transmitter and expected receiver of a message in calculating and confirming a digital signature utilize the SHA3. SHA3 is utilized for registering a condensed representation of a message or an information record. At the point when a message of any length < 64 bits is input, the SHA3 produces a 160-bit yield called a message digest. The message digest would then be able to be a contribution to the Digital Signature Algorithm (DSA), which produces or checks the mark for the message. Marking the message process as opposed to the message frequently enhances the effectiveness of the procedure in light of the fact that the message process is normally much smaller in measure than the message. A similar hash algorithm must be utilized by the verifier of an advanced signature as was utilized by the maker of the computerized signature [18]. The SHA3 is called secure on the grounds that it is computationally infeasible to discover 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

1. *Input a Message M, a pointer to the Message s and byte length of M as BL.*
2. *Compute y = 128M + s, 0≤s 128.*
   If s ≤ 111, the number of calls to update is (M+1)
   If s > 111, the number of calls to update is (M+2)
3. *Denote M = floor (x/64) and s = y mod 64, and*
4. *Consider the last block LB as zero*
   LB=Null
5. *Assign the string to the blocks as*
   LB [byte 0] = 0x80 Till LB [byte 15]
6. *Append(M, LB)*
7. *Compute till M(BL)/128*
   Update (hash, M)
   Compute M = M+128
8. *Now hash holds the Digest of the Message.*

b. MD5

The MD5 message-digest algorithm, shortly called as MD5, is a widely used cryptographic hash function, which produces a hash value of length 128-bit (16-byte), which is usually conveyed in text format as a 32 digit hexadecimal number. Cryptographic applications used the MD5 calculation in different ways, what's more all it is by and large used to confirm information uprightness. MD5 hashing calculation forms a variable-length message into a settled length message yield of size 128 bits. The client message is divided into lumps of 512-bit squares (i.e) 16 times of 32-bit words, the message is extended with the goal that its length is distinct by 512. The cushioning demonstrations as indicated by the accompanying advances: at first a solitary piece, 1, is appended to the end or the last position of the message. This is trailed by as a few quantities of zeros, or, in other words get the length of the message up to 64 bits not exactly a numerous of 512. Whatever is left of the bits are topped off with 64 bits speaking to the length of the principal message, or, in other words 264. The crucial MD5 calculation takes a shot at a 128-piece state, apportioned into four 32-bit words, which are indicated as A, B, C, and D. These are set to certain settled constants. The principal calculation at that point hones each 512-bit message square to change the state. The handling of a message block involves four similar stages, as mentioned above, is termed as rounds; each round is made out of 16 similar operations in view of a non-linear function F, modular addition, and left rotation [19].

PSEUDO CODE – MD5 Algorithm

1. *Input the message block M of size 512 bits.*
2. *Split M into 16 32-bit words as M0, M1, M2,... M15.*
3. *Split the state into four as A,B,C,D*
4. *Save the current state in some variables: A □ A', B □ B', C □ C' and D □ D'*
5. *Compute the below steps for 64 rounds:*
6. *Compute T = B + ((A + fi(B, C, D) + Mk + Xi) <<< si).*
7. *Rotate the state words: D □ A, C □ D, B □ C, T □ B.*
8. *Add the saved state values to the current state variables:*
9. *A + A' □ A, B + B' □ B, C + C' □ C, D + D' □ D.*
10. *Finally the new running state value is the hashed value.*

VI. Experimental Results

The Comparative study of Cryptographic Algorithms was studied and implemented in java environment and experimented the performance of the encryption and decryption algorithms.

Fig. 6.1 - Main Screen of the Research Work

The evaluation is intended to find the performance of the cryptographic algorithms by dividing the algorithms based on their nature as Symmetric Algorithms, Asymmetric Algorithms and Hashing algorithms. The performance calculations for Encryption and Decryption algorithm was done based on the execution time of each algorithm for different file size were done.

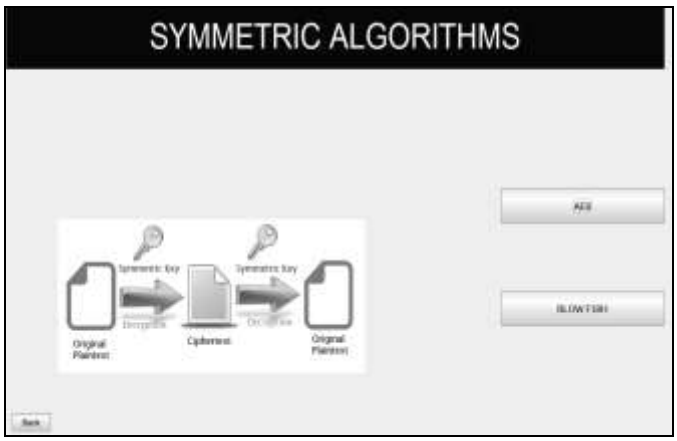

Fig: 6.2 – Symmetric Algorithms taken for study.

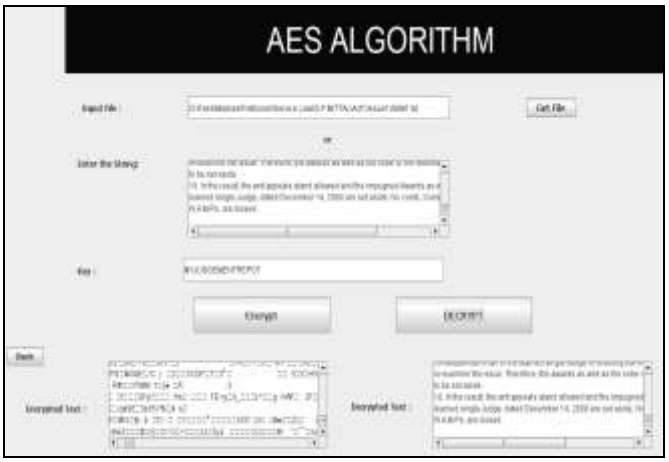

Fig: 6.3 – Encryption and Decryption using AES Algorithm

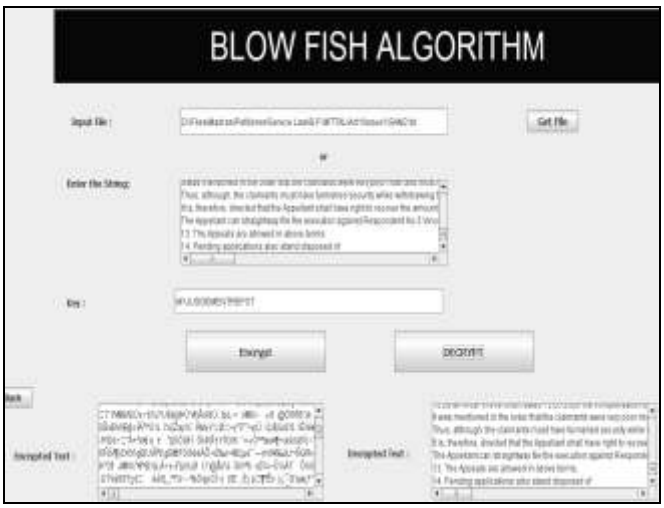

Fig: 6.4 – Encryption and Decryption using Blow Fish Algorithm

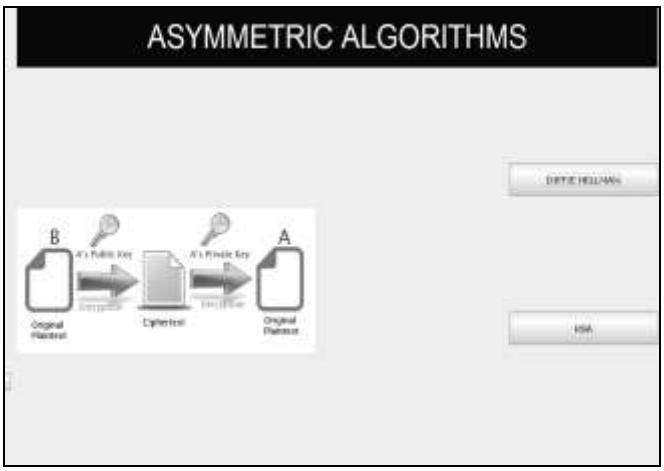

Fig: 6.5 – Asymmetric Algorithms taken for study.

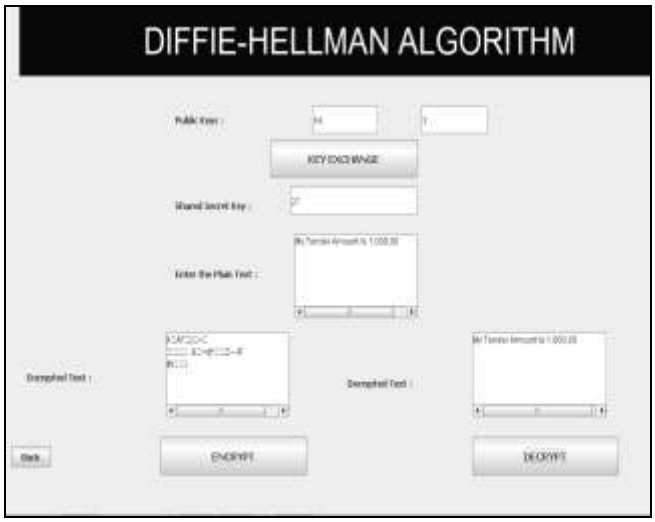

Fig: 6.6 – Encryption and Decryption using Diffie Hellman Algorithm

Fig: 6.7 – Encryption and Decryption using RSA Algorithm

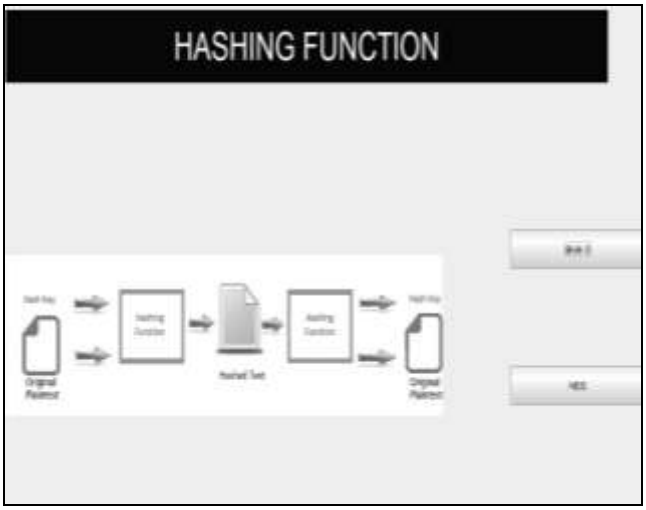

Fig: 6.8 – Hashing Algorithms taken for study.

Fig: 6.9 – Generating Hash Value using SHA-3 Algorithm

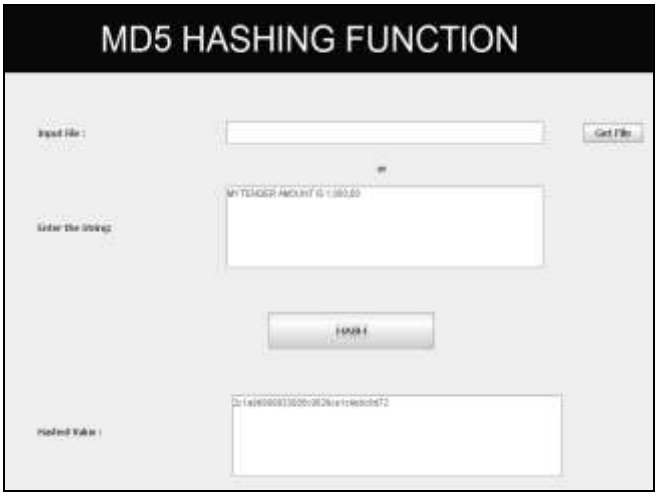

Fig: 6.10 – Generating Hash Value using MD5 Algorithm

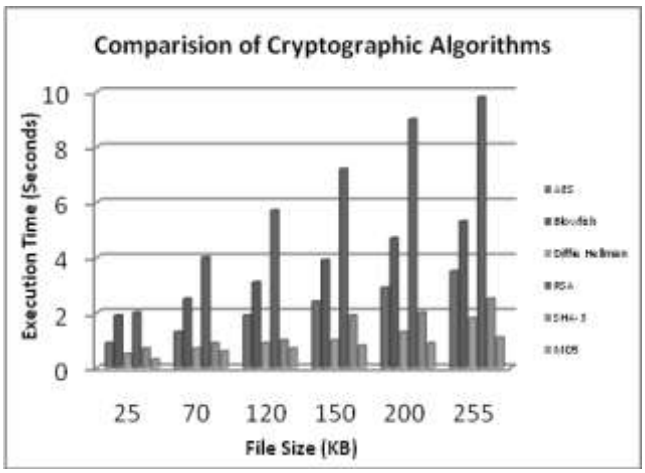

Fig: 6.11 – Comparison of Cryptographic Algorithms

VII. Conclusion

Cryptography is one of the important methodologies 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, that have been 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, which must be utilized as a part of distributed computing for making cloud information secure and not to be hacked by attackers.

Encryption and Decryption algorithms play an important role in data security on cloud; here the comparison of different cryptographic algorithm is done based on Execution Time parameter. It has been revealed that AES calculation utilizes the smallest amount of time to execute cloud information. Blowfish and SHA-3 is slightly high in Execution Time, whereas RSA devours longest encryption and decryption 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 to ensure the security of information.

References

[1]. Alexa Huth and James Cebula "The Basics of Cloud Computing", United States Computer Emergency Readiness Team. 2011.

[2]. Farzad Sabahi, "Virtualization-Level Security in Cloud Computing", Faculty of Computer Engineering Azad University Iran, 978-1-61284-486-2/11, IEEE Transaction, 2011.

[3]. G Devi, Pramod Kumar "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm", IJCTT, 2012.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. Ramgovind S, Elo_ MM, Smith E, "The Management of Security in Cloud Computing", 978-1-4244-5495-2/10, IEEE Transaction, 2010.

[12]. 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.

[13]. 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.

[14]. 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.

[15]. 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.

[16]. 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.

[17]. 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.

[18]. C. Hanser, Performance of the SHA-3 Candidates in Java, Institute for Applied Information Processing and Communications Graz, University of Technology, March 19, 2012.

[19]. A. Kasgar, J. Agrawal 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.

[20]. S.Rajendirakumar, Dr. A. Marimuthu, " A Comparitive study on Cryptographic Algorithms used in Cloud Computing", International Journal For Research In Applied Science & Engineering Technology, Vol:6, I:1, 2018.

[21]. 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.

[22]. 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.