International Journal of Computer Science Engineering & Technology
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)- NEW DELHI INDIA .
ISSN :2455-9091

ANALYSIS ON CLOUD COMPUTING SECURITY ALGORITHMS AND ITS SECURITY CHALLENGES

[1] M. Arunadevi, [2] Dr. V. Sathya,
[1, 2] Assistant professor,
[1, 2] Department of computer science,
[1, 2] MGR college, Hosur, Tamil Nadu, India.

ABSTRACT- Cloud computing includes an arrangement of administrations like programming, storing, organize gear assets and these are given to a customer by means of the web. The advantages of cloud computing are adaptability, taken a toll capability and high unwavering quality. Infrastructures of Cloud computing makes the client to access the data anywhere at any time as long as the client's gadget has access with the web. Thus this adaptability creates an impact upon the client and made them to transfer their data to cloud. Be that as it may, it may lay some security issues also. Cryptographic algorithms were executed to conquer the security issues and to guarantee the Cloud computing data security. Nowadays many procedures of this encryption and decoding were proposed to maintain security in cloud data. In this paper we will examine a portion of the cloud computing security challenges and algorithms.

Keywords: [Encryption, Security, Throughput, IDEA, Diffie-Hellman.]

1. INTRODUCTION

Cloud computing has created as an exceptionally comprehended strategy to support broad and voluminous information with the assistance of shared pool of assets and vast amassing an area. States that "Cloud computing is another enlisting perspective that is based on virtualization, disseminated figuring, utility handling and administration situated building". Further it is incorporated that cloud computing has created as extremely most critical perspective of the IT business and has pulled in the greater part of the business and the scholarly network [1]. Cloud computing is the act of using an arrangement of remote servers to interface with a pool of enrolling assets. The guideline favored standpoint is that it discards the enthusiasm for the customer to be in similar area where the storage room is really present. Cloud computing enables an on-demand organize access to a typical pool of preparing assets that can be immediately furnished with fundamental effort or administration provider cooperation.

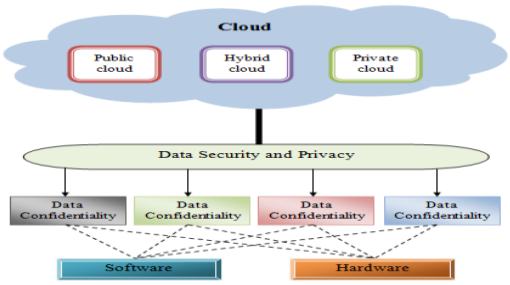

Figure 1: Overview of Cloud Security

Cloud computing is a large gathering of virtual servers organized to allow customers to store, share and access assets virtually. In the adaptable cloud condition, data redistributing became popular among the cloud customers. Secure data accessing is the major task of all cloud providers [2]. Clients can get together with the cloud to get dynamically reliable services, so they can access data from anywhere and at any time. These cloud services are segregated into four sorts, for example, cloud storage service, Software As A Service (SAAS), Platform As A Service (PAAS), and Infrastructure As A Service (IAAS). Among all the above services, the audit handles the data storage and re-appropriating services from the cloud. Regardless of the fact that there are various services available in the cloud, it has several challenging security issues. Data security on cloud incorporates several aspects, for example, secret, reliability and accessibility. In this survey, we will concentrate on various techniques associated with data dependability or reliability. In straightforward terms data trustworthiness can be fathomed as the maintenance of intactness of any data during transactions like storage, sharing and retrieval. In general, the data uprightness is alluded as the way toward maintaining the whole undamaged data. Because of several aspects, re-appropriated data may suffer trustworthiness issues on cloud. Finding and verifying the redistributed data along with the total dependability verification is an active research area. And the tremendous researches issues have a place with this area have been significantly concentrated in the literature.

2. LITERATURE SURVEY

[1] Krishna Keerthi Chennam, Lakshmi Muddana, Rajani Kanth Aluvalu (2017) proposed multi-arrange encryption is broke down utilizing different known encryption systems. In Multistage Encryption, the client is separated into different domains. In every domain, apply distinctive encryption algorithm. Multi-organize encryption algorithm guarantees the security of the data. In this paper, Explored the blend of different encryption algorithms for performing Multistage Encryption. Individual Domain Each data proprietor to deal with the mystery keys and access benefits of clients in his/her faculty domain utilizes encryption strategy. Data Owner is the confided in power of his own domain. The clients are by and by known by Data proprietor; thus he can give access benefits dependent on solicitations. In this paper, RSA algorithm is utilized for encryption of data in client's faculty domain. Public Domain In public domain various quality specialists each administering a disjoint subset of characteristics are kept up. The job of the client is additionally characterized as a quality in public domain. Purchasers get their mystery keys in public domain from trait specialists. They are not required to cooperate with data proprietors. To oblige get to data proprietors to determine fine grain get to approaches. This lessens the key administration overhead connected with an immense number of clients in public domain. In this paper, have utilized DES, AES and IDEA algorithms in public domain and assessed their exhibition. For multistage encryption blend of RSA with AES, at that point Mix of RSA with DES and blend of RSA with IDEA are utilized to encrypt the data. RSA create public-key and private-key with the assistance of two huge prime numbers for the extent of encryption and decryption. Data encryption finished with the public-key and data decryption is utilizing private-key. The RSA utilizes a key of 1024 bit. **[2] Leonardus Irfan Bayu Mahendra, Yehezkiel Khakham Santoso, Guruh Fajar Shidik (2017)** proposed an adjusted AES that changes the first structures by utilizing MAC Address. This adjusted AES could be utilized as an option for symmetric cryptography algorithm. The utilization of MAC Address could expand the randomness of the AES forms as a result of its distinction in every PC. Assailants most likely couldn't break the encrypted message effectively even they know

the essential key. AES has some characterized as of now steps, for example, move columns and the S-box which make AES less random. This exploration proposes an adjusted AES that modifies the first structures by utilizing MAC Address. This extra data is utilized as an extra key to rearrange the S-box and move lines, so the algorithm could be more enthusiastically for wrong people to get the first data which has been encrypted. Macintosh address is chosen due to its uniqueness and not all individuals could recognize the data effectively. By utilizing MAC address, would reinforce the security of AES. S-Box table is one of the most basic components in AES. It is utilized as a non-straight work in the encryption step. Numerous examinations have attempted to adjust S-Box table to build its unpredictability and effectiveness This investigation endeavors to expand the multifaceted nature by doing randomization on the S-Box table. The randomization technique is equivalent to utilized in transposition figure. The plaintext will continue as before, yet the characters are randomized with the goal that they can't be perused effectively. The technique could be connected in this algorithm in light of the fact that needn't bother with the substitution character inside the SBox table to change. A transposition figure is additionally required plaintext in a specific number of characters. For this situation, it doesn't make a difference on the grounds that the S-Box table size is consistently the equivalent. **[3] Dr. D.I. George Amalarethinam, H. M. Leena (2017)** Proposed an Enhanced RSA Algorithm with changing Key Sizes for Data Security in Cloud. The proposed algorithm decreases the time of encryption and decryption forms by partitioning the record into squares and improves the quality of the algorithm by expanding the key size. The proposed Enhanced RSA (ERSA) algorithm utilizes two extra prime numbers in Standard RSA algorithm. This thought had been raised from High Speed and Security RSA algorithm which utilized two random numbers for key age process. The use of prime numbers rather than random numbers in the proposed system improves the speed of encryption and decryption. This speed is as yet enhanced in the proposed algorithm ERSA by isolating the document into a few squares. Aside from expanding the speed, the implementation of ERSA algorithm additionally makes the calculation complex one and builds the quality of security. RSA algorithm which is a lopsided key algorithm utilizing two distinctive keys for encryption and decryption forms. The Key size can be shifted to make the encryption procedure solid. Subsequently it is hard for the aggressors to barged in the data. Expanding key size correspondingly builds the time taken for encryption and decryption process. The Symmetric key algorithms utilize a similar key for encryption and decryption. The other name for Symmetric key is Secret key algorithms. The prominent algorithms like AES, DES, Triple DES, Blowfish and so on., go under Symmetric Group. Two keys, to be specific, public key and private key are utilized in Asymmetric key algorithms. It incorporates the algorithms like RSA, Elgammal crypto system, Elliptic bend crypto system and so on. The Asymmetric key algorithms are otherwise called public key cryptography. In this manner the specialists secure their data by utilizing either Symmetric key or Asymmetric key algorithms. **[4] Ronald S. Cordova, Rolou Lyn R. Maata, Alrence S. Halibas, Rula Al-Azawi (2017)** Proposed the Comparative Analysis on the Performance of Selected Security Algorithms in Cloud Computing.The breaks down and analyzes the exhibition of chose algorithms, in particular: AES (Rijndael), Blowfish and RSA. The three most basic security algorithms utilized in cloud figuring were chosen and looked at. At that point, recreation was done with the goal for us to record the presentation of every algorithm. Two PCs have been used, both having Intel I3 Processors with 4GB and 8GB RAM, separately. NetBeans IDE 8.02 was utilized to run Java programs for the algorithms, every

one of the projects are same in structures. AES, Blowfish and RSA cryptographic algorithms were executed utilizing Java programming language on a similar programming condition. Every algorithm comprises of three stages: key age, encryption and decryption. The Java program for every algorithm took as individual contributions for five diverse content data, the sizes(1.86 kB, 3.73 kB, 7.46 kB, 14.9 kB and 29.8 kB) of content data differs from one another. The plan that was followed in the reproduction is the time and proficiency of every algorithm. The time for every algorithm and for each size of content data for key age, encryption and decryption were recorded. In light of the mimicked outcomes, Blowfish exhibited preferable execution over AES and RSA algorithms. The parts of key age, encryption and decryption were altogether tried and in the majority of the outcomes, Blowfish picked up the least handling time. This makes it as a fantastic candidate for being one of the best security algorithms. Albeit just the speed and effectiveness were shrouded in the reenactment, this makes it an extremely encouraging algorithm that might be used in verifying the cloud and system assets. The exhibitions of thealgorithms were improved once the RAM of the PC was multiplied. The RAM assumed a noteworthy job in improving the speed and proficiency of all the tried algorithms. **[5] Naga Hemanth P, Abhinay Raj N., Nishi Yadav (2017)** Proposed to Secure Message Transfer utilizing RSA algorithm and Improved Playfair figure in Cloud Computing. To give security to the data to send and likewise verifying the key that the encrypting the data. This exploration comprises of three phases, the main stage incorporates encryption of content utilizing playfair figure of 9x6 framework. In the subsequent stage, XOR activity is performed between the encrypted content and the key which it has been encrypted. In the last arrange encryption of key is done utilizing RSA algorithm and proceeded with a XOR activity between the encrypted content and the encrypted key. Starting at now, playfair figure encryption procedure is chipped away at the size 5x5 which has been modified for computing Cipher content (enc1). Along these lines, at long last, this blended algorithm diminishes the bad marks of customary playfair figure and includes an additional layer of security for the message. In this algorithm, 9x6 lattice enables some new characters to embed in free spaces. Lattice development pursues every one of the principles of 5x5. It permits in excess of 26 characters as key. It utilizes lowercase letters, numbers, administrators, sections. It can without much of a stretch encrypt and decrypt mix of letters in order productively.

3. SECURITY CHALLENGES IN CLOUD COMPUTING

Security is the imperative perspective for certain associations for cloud appropriation. Mystery, confirmation, respectability, nonrevocation, and accessibility for client's frameworks are the general standards of security. Get the chance to control is another vital factor for security. There are loads of security dangers to Cloud Service. A solitary deformity in one client application could enable a malignant programmer to get access for more than one client's information. This issue is known as information breaks. The information adversity is another issue that happens when the unapproved customer may erase or change the entire records in the cloud if there is the helplessness in cloud provider side. Unreliable APIs and weak interfaces are another normal security challenges in cloud handling. Cryptography is also a strategy for changing over information into unreadable structure during storage and transmission that it appears to be waste to gatecrasher. The unreadable information called as figure content. At the moment that information is gotten by recipient, it will appear as original called as plain content. Changing over to figure content from plain content called encryption and turnaround of this (figure content to plain content) is known as

decoding. Encryption happens at sender's end while decoding happens at recipient's end. There are three kinds of cryptography calculations. Classified as Symmetric, Asymmetric and Hashing.

4. CLOUD COMPUTING SECURITY ALGORITHMS

4.1 Triple DES Algorithm

The compelling security 3DES gives is just 112 bits because of compromise attacks. Triple DES runs multiple times more slow than DES, yet is substantially more secure whenever utilized appropriately. The methodology for unscrambling something is the same as the strategy for encryption, with the exception of it is executed backward. In DES, data is scrambled and unscrambled in 64 - bit lumps. The information key for DES is 64 bits in length; the actual key utilized by DES is just 56 bits long. The least significant (right-most) bit in each byte is a parity bit, and ought to be set so that there are always an odd number of 1s in each byte [2]. These parity bits are disregarded, so just the seven most significant bits of each byte are utilized, bringing about a key length of 56 bits. This means that the viable key quality for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not utilized during the encryption procedure. Triple Data Encryption Standard (DES) is a sort of automated cryptography where square figure algorithms are applied multiple times to each data square. The key size is increased in Triple DES to guarantee additional security through encryption capabilities. Each square contains 64 bits of data. Three keys are alluded to as group keys with 56 bits for every key. There are three keying choices in data encryption standards:

- All keys being independent
- Key 1 and key 2 being independent keys
- All three keys being identical

Triple DES algorithm utilizes three iterations of basic DES figure. It gets a mystery 168-bit key, which is partitioned into three 56-bit keys.

- Encryption using the first secret key
- Decryption using the second secret key
- Encryption using the third secret key.

Triple DES is advantageous because it has a significantly estimated key length, which is longer than most key lengths affiliated with other encryption modes. DES algorithm was replaced by the Advanced Encryption Standard and Triple DES is currently viewed as out of date. It gets from single DES yet the strategy is utilized in triplicate and includes three sub keys and key padding when necessary. Keys must be increased to 64 bits long Known for its compatibility and adaptability can easily be changed over for Triple DES consideration.

4.2 IDEA algorithm

IDEA scrambles a 64-bit square of plaintext to 64-bit square of figure content. It utilizes a 128-bit key. The algorithm comprises of eight identical rounds and a "half" round final transformation. because of 128-bit cryptosystems like AES, IDEA is old, yet its algorithm can be a valuable teaching instrument to enable understudies to cross over any barrier between DES, which uses XOR however no algebraic operations, and AES, which requires understanding of algebraic operations on limited fields. IDEA utilizes algebraic operations; however it is just necessary to understand modular addition and modular multiplication to understand the IDEA algorithm [1]. The algebraic idea behind IDEA is the blending of three incompatible algebraic operations on 16-bit squares: bitwise XOR, addition modulo 216, and multiplication modulo 216 + 1.

The square figure IDEA encodes a 64-bit square of plain content and a 64-bit of figure content, and a 128-bit key controls it. The algorithm comprises of eight identical rounds in addition to a half round for yield transformation. The fundamental plan in IDEA is the utilization of the blending of three incompatible algebraic gatherings: bit-by-bit

XOR, addition modulo 216, and multiplication modulo 216+1. The plain content is a fixed size (64-bit hinder) that is separated into four 16-bit squares (X1|| X2|| X3|| X4). The key is a 128-bit square. It is partitioned into eight 16-bit sub keys. The division into 16 bits is because all of the algebraic operations utilized in the encryption and unscrambling procedure operate at 16-bit numbers. The last yield round is four 16-bit sub keys. Each round utilizations six 16-bit sub keys and the remaining two sub keys are utilized in the following round by actualizing left moving by 25 positions. The total sub keys is 52 {52=8 rounds*6 sub keys + (4 sub keys "yield transformation")}

The IDEA encryption algorithm has a few features which claim for use:

High level security not staying quiet about the algorithm, yet endless supply of the mystery key.

- Easily comprehended.
- Available on the web.

Widely utilized range of application and productively, for example, distance learning.

4.3 Diffie- Hellman Key Exchange

In Diffie Hellman Key Exchange, a shared mystery key established, that is utilized that is utilized for communication over the open system. In Diffie Hellman Key Exchange Algorithm Sender and Receiver picks two mystery numbers and these numbers are known to both sender and collector. Diffie-Hellman key exchange, also called exponential key exchange, is a technique for digital encryption that utilizations numbers raised to explicit forces to deliver unscrambling keys on the basis of parts that are rarely straightforwardly transmitted, making the task of an eventual code breaker mathematically overpowering [12]. The Diffie-Hellman algorithm is being utilized to establish a shared mystery that can be utilized for mystery communications while exchanging data over an open system utilizing the elliptic bend to generate focuses and get the mystery key utilizing the parameters.

For the sake of straightforwardness and practical implementation of the algorithm, we will think about just 4 variables one prime P and G (a crude base of P) and two private values an and b.

P and G are both freely available numbers. Clients (say Alice and Bob) pick private values an and b and they generate a key and exchange it freely, the contrary individual got the key and from that generates a mystery key after which they have the same mystery key to scramble.

Its advantages are The security factors regarding the fact that understanding the discrete logarithm is challenging, and That the shared key (for example the mystery) is never itself transmitted over the channel.

5. EXPERIMENTAL RESULTS PACKET DELIVERY RATIO

Triple Data Encryption Standard	International Data Encryption Algorithm	Diffie Hellman Key Exchange Algorithm
0.02	0.09	0.04
0.05	0.14	0.08
0.09	0.19	0.13
0.14	0.25	0.19
0.19	0.3	0.22

Table 1: Comparison table of Packet Delivery Ratio

The comparison table of Packet Delivery Ratio shows the different values of Triple Data Encryption Standard (Triple DES), International Data Encryption Algorithm (IDEA) and Diffie Hellman Key Exchange Algorithm. When comparing theses three algorithms the packet delivery ratio of IDEA is high. The Triple DES value starts from 0.02 to 0.19, IDEA algorithm values starts from 0.09 to 0.3 and Diffie Hellman Key Exchange Algorithm values starts from 0.04 to 0.22. The IDEA algorithm provides the better results of compare than the other two algorithms.

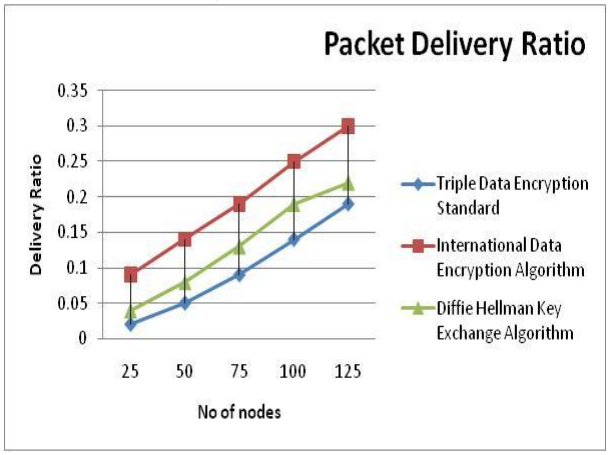

Figure 2: Comparison Chart of Packet Delivery Ratio

The comparison chart of Packet Delivery Ratio demonstrates the different values of Triple Data Encryption Standard (Triple DES), International Data Encryption Algorithm (IDEA) and Diffie Hellman Key Exchange Algorithm. No of node in X axis and Packet delivery ratio in Y axis. The Triple DES value starts from 0.02 to 0.19, IDEA algorithm values starts from 0.09 to 0.3 and Diffie Hellman Key Exchange Algorithm values starts from 0.04 to 0.22. The IDEA algorithm provides the better results than the other two algorithms.

Traffic Ratio

Triple Data Encryption Standard	International Data Encryption Algorithm	Diffie Hellman Key Exchange Algorithm
31.9	26.77	39
37.7	31.98	45
42.6	34.56	49
50.4	38.92	55
55.23	44.56	58

Table 2: Comparison table of Traffic Ratio

The comparison table of Traffic Ratio shows the different values of Triple Data Encryption Standard (Triple DES), International Data Encryption Algorithm (IDEA) and Diffie Hellman Key Exchange Algorithm. When comparing theses three algorithms the traffic ratio of IDEA is low. The Triple DES value starts from 31.9 to 55.23, IDEA algorithm values starts from 26.77 to 44.56 and Diffie Hellman Key Exchange Algorithm values starts from 39 to 58. The IDEA Algorithm provides the better results than the other two algorithms.

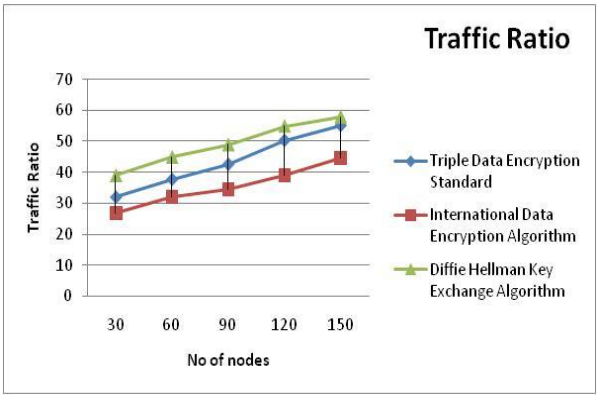

Figure 3: Comparison Chart of Traffic Ratio

The comparison chart of Traffic Ratio demonstrates the different values of Triple Data Encryption Standard (Triple DES), International Data Encryption Algorithm (IDEA) and Diffie Hellman Key Exchange Algorithm. No of node in X axis and Traffic ratio in Y axis. The Triple DES value starts from 31.9 to 55.23, IDEA algorithm values starts from 26.77 to 44.56 and Diffie Hellman Key Exchange Algorithm values starts from 39 to 58. The IDEA algorithm provides the better results than the other two algorithms.

Throughput Level

Triple Data Encryption Standard	International Data Encryption Algorithm	Diffie Hellman Key Exchange Algorithm
67.2	57	69.5
69.7	59	69.9
70.8	62	69.5
72.6	66	70.9
75	69	72

Table 3: Comparison table of Throughput Level

The comparison table of Throughput Level shows the different values of Triple Data Encryption Standard (Triple DES), International Data Encryption Algorithm (IDEA) and Diffie Hellman Key Exchange

Algorithm. When comparing theses three algorithms the throughput level of Triple DES is high. The Triple DES value starts from 67.2 to 75, IDEA algorithm values starts from 57 to 69 and Diffie Hellman Key Exchange Algorithm values starts from 69.5 to 72. The Triple DES algorithm provides the better results than the other two algorithms.

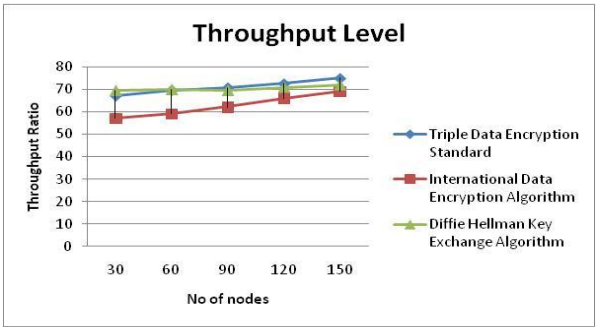

Figure 4: Comparison Chart of Throughput Level

The comparison chart of Throughput Level demonstrates the different values of Triple Data Encryption Standard (Triple DES), International Data Encryption Algorithm (IDEA) and Diffie Hellman Key Exchange Algorithm. No of node in X axis and Throughput Level in Y axis. The Triple DES value starts from 67.2 to 75, IDEA algorithm values starts from 57 to 69 and Diffie Hellman Key Exchange Algorithm values starts from 69.5 to 72. The Triple DES algorithm provides the better results than the other two algorithms.

CONCLUSION

Cloud computing demonstrate a fruitful application for organizations. Because organizations have large amount of data to store and cloud gives that space to its client and also allows its client to access their data from anywhere anytime easily. In cloud computing innovation there are a lot of important arrangement issue, which incorporates issue of privacy, security, anonymity, telecommunications capacity, and reliability among others. Yet, the most important between them is security and how cloud supplier assures it. In this paper analyses the importance of security to cloud. We compared the symmetric algorithm and asymmetric algorithm for data security in cloud to give the better security.

REFERENCES

[1]. Krishna Keerthi Chennam, Lakshmi Muddana, Rajani Kanth Aluvalu, "Performance Analysis of various Encryption Algorithms for usage in Multistage Encryption for Securing Data in Cloud", © 2017 IEEE.

[2]. Leonardus Irfan Bayu Mahendra, Yehezkiel Khakham Santoso, Guruh Fajar Shidik, "Enhanced AES using MAC Address for Cloud Services", © 2017 IEEE.

[3]. Dr. D.I. George Amalarethinam, H. M. Leena," Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud", World Congress on Computing and Communication Technologies (WCCCT) @2017IEEE.

[4]. Ronald S. Cordova, Rolou Lyn R. Maata, Alrence S. Halibas, Rula Al-Azawi," Comparative Analysis on the Performance of Selected Security Algorithms in Cloud Computing", 2017 IEEE International Conference on Electrical and Computing Technologies and Applications (ICECTA).

[5]. Naga Hemanth P, Abhinay Raj N., Nishi Yadav," Secure Message Transfer using RSA algorithm and Improved Playfair cipher in Cloud Computing", 2017 IEEE 2nd International Conference for Convergence in Technology (I2CT)

[6]. Shubhi Mittal, Shivika Arora, Rachna Jain," PData Security using RSA Encryption Combined with Image Steganography", © 2016 IEEE

[7]. Priyanka Ora, Dr.P.R.Pal," Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography", IEEE International Conference on Computer, Communication and Control (IC4-2015).

[8]. Sattar B. Sadkhan, Farqad H. Abdulraheem," A Proposed ANFIS Evaluator

for RSA Cryptosystem used in Cloud Networking", ©2017 IEEE
[9]. Viney Pal Bansal, Sandeep Singh," A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs", ©2015 IEEE.
[10]. Chin-Tan Lee, Yi-Chin Chung, Tung-Chun Shen and Ko-Wei Weng," Development of Electronic Locks Using Gesture Password of Smartphone Base on RSA Algorithm", Proceedings of the 2017 IEEE International Conference on Applied System Innovation IEEE-ICASI 2017 - Meen, Prior & Lam (Eds).
[11]. Debasis Das," Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi-Party Computation", ©2018 IEEE.
[12]. Samjot Kaur, Vikas Wasson," Enhancement in Homomorphic Encryption Scheme for Cloud Data Security", 2015 IEEE 9th International Conference on Next Generation Mobile Applications, Services and Technologies.
[13]. R.Nivedhaa and J.Jean Justus," A Secure Erasure Cloud Storage system using Advanced Encryption Standard algorithm and Proxy Re-encryption", ©2018 IEEE.
[14]. Nivedita Shimbre, Prof. Priya Deshpande," Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm", 2015 IEEE International Conference on Computing Communication Control and Automation.