International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

ANALYSIS OF SECURITY ALGORITHMS IN CLOUD

M.Sasikala[1], Dr. V. Anuratha[2]

[1]Research Scholar (PT), Department of Computer Science,
Sree Saraswathi Thyagaraja College, Pollachi
[2] Professor & Head, PG Department of Computer science,
Sree Saraswathi Thyagaraja College, Pollachi

ABSTRACT

With growing awareness and considerations regards to Cloud Computing and knowledge Security, there's growing awareness and usage of Security Algorithms into information systems and processes. This paper presents a short summary and comparison of cryptologic algorithms, with a stress on Asymmetric algorithms that ought to be used for Cloud primarily based applications and services that need information and link encoding. During this paper we have a tendency to review Asymmetric and uneven algorithms with stress on symmetric Algorithms for security thought on that one ought to be used for Cloud primarily based applications and services that need information and link encoding. Here we introduced symmetric and asymmetric encrypt and decrypt algorithm details and comparison.

I. INTRODUCTION

Cloud computing is rising technology that primarily refers to applications delivered as services over the net and also the hardware and computer programme within the datacenters that offer those services. Cloud has left all different distributed computing techniques way behind each in competition and in terms of recognition and success. The first reason is that, any service extended supported customer's desires. [1]. Cloud in science suggests that massive assortment of objects that's visually showing from distance as cloud. Cloud in cloud computing is trope for web. Cloud computing is that the evolution and adoption of existing technologies. The most sanctionative technology of cloud computing is virtualization. Virtualization suggests that separating a physical computing into additional one virtual device which may be simply maintained [2]. There square measure several characteristics of victimization cloud computing over different technologies like gracefulness, less cost, device and placement independence, simply reparable , multitenacy, on demand services broad network access, speedy snap. There square measure 3 varieties of cloud readying models. They're non-public, public, and hybrid. [3] Public clouds: this is often a kind of cloud hosting in that during which the cloud services square measure delivered over a network which is open for public usage. Public cloud suppliers like Amazon AWS, Microsoft and Google which provide services over web. Non-public clouds: it's conjointly called internal cloud; the platform for cloud computing that belongs to the actual company organization. Non-public cloud because it permits solely the au theorized users, offers the organization larger and direct management over their information. Hybrid clouds: this type of cloud may be a mix of the overall public and conjointly the private

cloud and it uses the services that square measure out there in every the overall public and private house. Management of the cloud is completed by every public and private cloud suppliers. Delivery Models: There square measure 3 varieties of cloud delivery models. Package as a Service (SaaS): In SaaS may be outlined as software's deployed over web provided as services to the consumer as per their demand e.g. salesforce.com. Platform as a Service (PaaS): PaaS permits platform access for purchasers so that they can place their own software's and applications on to the cloud. Alternately business produces variety of its custom application used inside the company. Infrastructure as a Service (IaaS): IaaS provides customers with the infrastructure like rent method, storage, network capability, and different basic computing resources. In addition permits shoppers to manage the operative systems, applications, storage, and network property.

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Because of these benefits each and every organizations are moving their data to the cloud. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

Challenges And Issues In Cloud Computing

Security is taken into account collectively of the foremost important aspects in everyday computing and it's not totally different for cloud computing thanks to sensitivity and importance of knowledge keep on the cloud. Cloud Computing infrastructure uses new technologies and services, most of that haven't been absolutely evaluated with regard to the safety. Current cloud atmosphere is related to various challenges as follows;

A. Governance implies management and oversight by the organization over procedures, standards and policies for application development and information technology service ability, additionally as a result of the design, implementation, testing, use, and observance of deployed or engaged services.

B. Malicious Insiders This threat is standard to most organizations. „Malicious insiders‟ impact on the organization is respectable. Malicious insiders ar the threat that has access to the info} or information

concerning the organization being a member of the organization. As cloud shoppers application information is keep on cloud storage provided by cloud supplier that additionally has the access to it information.

C. information Integrity guaranteeing the integrity of the information (transfer, storage, and retrieval) very means it changes solely in response to licensed transactions. Common place typical standard to make sure information integrity doesn't nevertheless exist.

D. Account or service Hijacking this threat happens thanks to phishing, fraud and package vulnerabilities. During this sort assaulter will get access to important areas onto the cloud from wherever he will take allow and steeling vital data resulting in compromise of the supply, integrity, and additionally confidentiality to the services.

E. Insecure Apis Anonymous access, reusable tokens or word, clear text authentication or transmission of content, inflexible access controls or improper authorizations, restricted observance, and work capabilities etc security threats might occur to organizations if the weak set of interfaces and Apis are used [11].

Privacy and Confidentiality: Once the consumer host knowledge to the cloud there ought to be some guarantee that access thereto knowledge can solely be restricted to the licensed access. Inappropriate access to client sensitive knowledge by cloud personnel is another risk which will create potential threat to cloud knowledge. Assurances ought to be provided to the purchasers and correct practices and privacy policies and procedures ought to be in situ to assure the cloud users of the info safety. The cloud seeker ought to be assured that knowledge hosted on the cloud is going to be confidential. Knowledge integrity: With providing the protection of knowledge, cloud service suppliers ought to implement mechanisms to make sure knowledge integrity and be able to tell what happened to an exact dataset and at what purpose. The cloud supplier ought to create the consumer conscious of what explicit knowledge is hosted on the cloud, the origin and also the integrity mechanisms place in situ.

For compliance functions, it's going to be necessary to own actual records on what knowledge was placed in a very public cloud, once it occurred, what virtual recollections (VMs) and storage it resided on, and wherever it had been processed. Once such knowledge integrity needs exists, that the origin and custody info} or information should be maintained so as to stop meddling or to stop the exposure of knowledge on the far side the in agreement territories (either between completely different completely different servers or different networks). Knowledge location and Relocation: Cloud Computing offers a high degree of knowledge quality. Shoppers don't continuously understand the situation of their knowledge. However, once associate enterprise has some sensitive knowledge that's unbroken on a memory device within the Cloud, they'll wish to grasp the situation of it. They'll conjointly want to specify a most popular location (e.g. knowledge to be unbroken in India). This, then, needs a written agreement, between the Cloud supplier and also the client that knowledge ought to keep in a very explicit location or reside on a given famous server... Also, cloud suppliers ought to take responsibility to make sure the protection of systems (including data) and supply strong authentication to

safeguard customers' info. Another issue is that the movement of knowledge from one location to a different. Knowledge is abilities hold on at associate acceptable location decide by the Cloud supplier. However, it's typically affected from one place to a different. Cloud suppliers have contracts with one another and that they use every others' resources. Knowledge Availability: client knowledge is normally is generally is typically held on in chunk on totally different servers often residing in several locations or in several Clouds. During this case, knowledge accessibility becomes a serious legitimate issue because the accessibility of uninterruptible and seamless provision becomes comparatively tough. Storage, Backup and Recovery: after you arrange to move your knowledge to the cloud the cloud supplier ought to guarantee adequate knowledge resilience storage systems. At a minimum they ought to be able to offer RAID (Redundant Array of freelance Disks) storage systems though most cloud suppliers can store the info in multiple copies across several freelance servers. Additionally thereto, most cloud suppliers ought to be able to offer choices on backup services that are actually vital for those businesses that run cloud primarily based applications in order that within the event of a significant hardware failure they will roll back to associate earlier state.

SECURITY ALGORITHMS

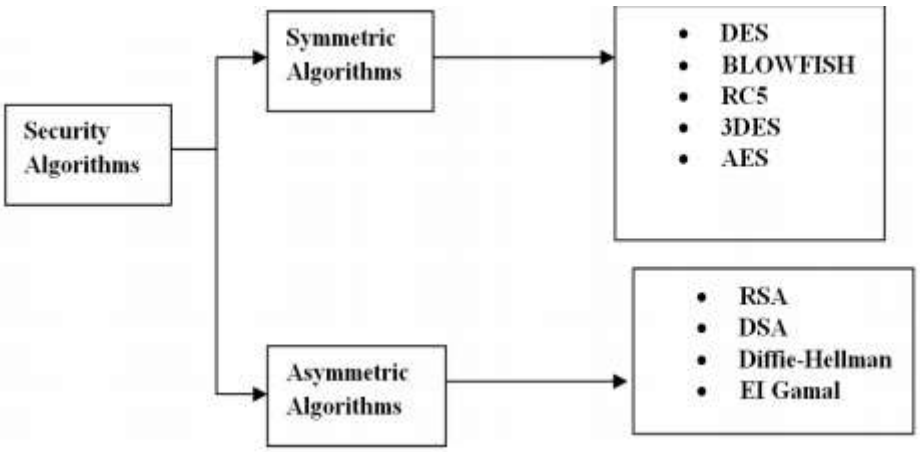

Fig 1. Security algorithms

II. ASYMMETRIC ALGORITHMS

Asymmetric Algorithms [6] a combine of connected key, one key for coding referred to as the general public key and a unique however entomb connected key for decoding referred to as the personal keys once playacting transformation of plain text into cipher text. The most uneven algorithms area unit ECC, Diffie-Hellman and RSA.

2.1 RSA

RSA was fictional by Ranold Fivest, Adi Shamir and Dutch Leonard Adleman in 1977. [6] RSA is additionally associate uneven algorithmic rule. Functioning of RSA is predicated on multiplication of 2 giant numbers. 2 giant prime numbers square measure generated and increased. Once multiplying 2 numbers, modulus is calculated the amount that's generated is employed because the public and personal key [9]. The 2 numbers that square measure used for multiplication-one of them is public alternative is non-public. Steps for RSA algorithm: - a) Divide the massive message into tiny range of blocks wherever every block represents identical vary. b) By raising the eth power to module n write in code the message. c) For the coding of message increase another power d module n.

RSA rule named once its inventers (Rivest, Shamir, and Adelman) is best fitted to knowledge traveling to/from net and Cloud based mostly environments. In operating with Cloud Computing, the top user knowledge is initial encrypted and so hold on the Cloud. Once the information is needed, the top user merely has to place a call for participation to the Cloud Service supplier for accessing the information. For this the Cloud service supplier initial authenticates the user to be the authentic owner and so delivers the information to the requester victimization RSA uneven rule. This rule has support from .NET Security Framework moreover. Here 2 keys concerned – initial the general public Key [7] that known to all or any and also the different personal Key that is thought solely to the top user. conversion from plain text to cipher text is completed victimization Public Key by the Cloud service supplier and also the cipher text to plain text decoding is completed by the top user victimization personal Key because the Cloud service client. Once the user knowledge is encrypted with the general public Key, that cipher knowledge will solely be decrypted with the corresponding personal Key solely. during this rule, prime numbers area unit wont to generate the general public and personal keys supported mathematical formulas and by multiplying the numbers along. This uses the block size knowledge during which plain text or the cipher texts area unit integers between zero and one for a few n values. Here the processed plaintext is additionally encrypted in blocks and also the binary price of every block has to be but the quantity (n). RSA being increasing homomorphy that basically means to search out the merchandise of the plain text, multiply the cipher texts in order that the result of the result's the cipher text of the merchandise.

2.2 DSA (DIGITAL SIGNATURE ALGORITHM)

Digital signatures area unit terribly essential in modern times to verify the sender's identity. Digital signature is AN electronic signature that is employed for verification and authentication of information. A digital signature is pictured as a string of binary digits in system. The signature is employing a set of rules and parameters (algorithm) specified the identity of the person sign language the document also because the originality of the info is verified. The signature is generated with the assistance of a personal key. a personal key's glorious solely to the sender. The signature is verified by receiver by use of a public key that corresponds to the personal key. Digital signature is used with any reasonably knowledge whether or not it's encrypted or not. Digital signatures area unit won't to find unauthorized modifications of information by third party. Also, the recipients of a digitally signed document assure that the document was so signed by the one who it's claimed to be signed by.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

This can be called nonrepudiation, as a result of the one who signed the document cannot repudiate the signature later. Digital signature algorithms is employed in e-mails, electronic funds transfer, software system distribution, knowledge storage that assure the integrity , believability and originality of information. A hash perform is employed within the signature generation method to get a condensed version of information, referred to as a message digest. The message digest is then input to the digital signature rule to get the digital signature.

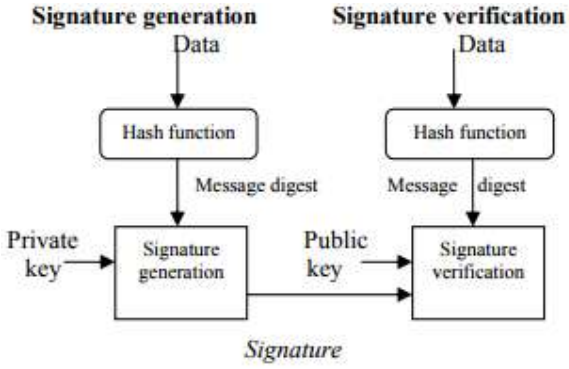

Fig 2.Dsa Algorithm

2.3 DIFFIE-HELLMAN KEY EXCHANGE (D-H):

This is a technique for exchanging cryptologic keys [8] by initial establishing a shared secret key to use for the repose communication and not for secret writing or decoding. This key exchange method ensures the 2 parties that haven't any previous information of every different to put together establish a shared secret key over unsecure web. Transformations of keys area unit interchanged and each find you with identical session key that appears sort of a secret key. Then every will then calculate a 3rd session key that can't simply be derived by Associate in nursing aggressor WHO is aware of each changed values. This key encrypts the next communications employing a symmetric key cipher however is liable to the Man-in-the Middle (MITM) attack. This key exchange isn't used for exchanging real giant knowledge not like RSA.

III. SYMMETRIC ALGORITHMS

Symmetric algorithms involve one shared secret key [9] to code in addition as decode knowledge and area unit capable of process great amount of information and from computing position aren't terribly power intensive, thus has lower overhead on the systems and have high speed for playacting secret writing and decoding. Symmetric algorithms code plaintexts as Stream ciphers bit by bit at a time [10] or as Block ciphers on mounted range of 64-bit units.

Exchanging Shared Secret Key over unsecure web. Symmetric-key algorithms share secret keys needed by the sender and receiver throughout secret writing or decoding method. Just in case a 3rd person gains access to the secure secret key, cipher text messages will simply be decrypted. The actual fact of getting one single secret key algorithmic rule is that the most important issue baby-faced by Cloud service suppliers once coping with finish

users WHO communicate over unsecure web. The sole possibility is to possess that secret key be modified typically or unbroken as secure as potential throughout the distribution part.

3.1 DATA ENCRYPTION COMMONPLACE (DES)

DES is incredibly unremarkably used bilateral key rule. It had been developed by IBM in 1974, however currently days several strategies area unit found that had established this rule unsecured [1]. In DES algorithms block cipher is of sixty four bits [2] and key used is of fifty six bits out of sixty four bits of key's used remainder of eight bits area unit soft. In block cipher we have a tendency to code block of information that include plain text by combination of confusion and diffusion to create cipher block then this cipher block should pass sixteen rounds, before passing through these sixteen rounds the sixty four bits of information is split into thirty two bits. Once dividing the info into thirty two bits, F-function (Feistel function) is applied. F-function consists of substitution, permutation, key mixing. The output of operate is combined with partner of the info victimization XOR circuit alternate crossing of information is completed; then crossing of information is done.

After doing sixteen such rounds cipher text is created or encoding of information is completed. To decipher the info reverse operation is completed. The downside of DES is that key employed in DES is incredibly tiny and its security will be broken simply and DES works quickly on hardware solely and woks slowly on software package. As shown in Fig three information bits area unit divided into 2 elements low frequency and Rf than F operate and XOR operation is applied on Rf , and output is combined with low frequency.

3.2 ADVANCE ENCODING RULE (AES)

Advanced encoding commonplace (AES), additionally referred to as Rijindael is employed for securing data. AES could be a bilateral block cipher that has been analyzed extensively and is employed wide now-a-days. However AES works in cloud environment? AES, bilateral key encoding rule is employed with key length of 128-bits for this purpose. As AES is employed wide now-a-days for security of cloud. Implementation proposal states that initial, User decides to use cloud services and can migrate his information on cloud. Then User submits his services necessities with Cloud Service supplier (CSP) and chooses best nominative services offered by supplier. Once migration of information of knowledge of information to the chosen CSP happens associate degreed in future whenever an application uploads any data on cloud, the info can initial encrypted victimization AES rule so sent to supplier. Once encrypted, information is uploaded on the cloud, any request to scan the information can occur once it's decrypted on the users finish so plain text data will be scan by user. The plain text information isn't written anyplace on cloud. This includes every kind of information. This encoding resolution is clear to the appliance and may be integrated quickly and simply with none changes to application. The key's ne'er hold on next to the encrypted information, since it's going to compromise the key additionally. To store the keys, a physical key management server will be put in within the user's premises. This encoding protects information and keys and guarantees that they continue to be underneath user's management and can ne'er be exposed in storage or in transit. AES has replaced the DES as approved commonplace for a good vary of applications.

Advance encoding rule AES is additionally referred to as Rijndael. AES is proclaimed as U.S FIPS by government agency in 2001. In AES, totally different size of key's used i.e. 128, 192 or 256 bits,

Depends on what percentage cycle it uses [3]. For ten cycle's 128-bit key, twelve cycle's 192 bit key and for fourteen cycles 256 bit key's used. All rounds of AES area unit similar accept the last one. AES works on 4x4 matrixes. AES consists of key growth, initial and final spherical. Initial spherical include Add spherical Key, Sub Bytes, Shift Rows, combine Columns, Add spherical Key and final spherical additionally consists of comparable operate as initial spherical except combine columns. AES works quickly on each software package and hardware.

3.3 TRIPLE- DES (TDES)

TDES is increased version of DES in TDES the key size is accrued to extend i.e. 168 bits the safety of information. In TDES solely size of key's accrued remainder of the operating is analogous to DES. In TDES 3 totally different keys area unit applied on cipher block.

3.4 BLOWFISH ALGORITHM

Blowfish rule could be a symmetrical key rule that was developed in 1993 by Bruce Schneider. Its operating is nearly like DES however in DES key size is little will be decrypted simply however in Blowfish rule the dimensions of secret is massive [4] and it can vary from thirty two to 448 bits. Blowfish additionally consists of sixteen rounds like DES [11]. Blowfish rule will inscribe knowledge having size multiple of eight and if the dimensions of the message isn't multiple of eight than bits square measure cushioned. In Blowfish rule additionally sixty four bits of plain text is split into 2 components of size thirty two bits. One half taken because the left a {part of} message and different is correct part of message. The left half is XOR with the weather of P-array that creates some worth, then that worth is undergone transformation operate F. the worth originated from the transformation operate is once more XOR with the opposite 1/2 the message i.e. with right bits, then F| operate is termed that replace the left 1/2 the message and P| replace the correct facet message.

3.4 IDEA INTERNATIONAL ENCRYPTION RULE

IDEA was projected by James Massey and Xuejia Lai in 1991.It is thought-about as best symmetrical key rule. It accepts sixty four bits plain text and key size is 128 bits. IDEA consists of 8.5 rounds. All rounds square measure similar except the one. In plan the sixty four bits of knowledge is split into four blocks every having size sixteen bits. Currently basic operations standard, addition, multiplication, and bitwise exclusive OR (XOR) square measure applied on sub blocks. There square measure eight and 0.5 spherical in plan every round encompass completely different sub keys. Total range of keys used for playing completely different rounds is fifty two. In spherical one the K1 to K6 sub keys square measure generated, the sub key K1 has the primary sixteen bits of the first key and Godwin Austen has following sixteen bits equally for K3, K4, K5 and K6. Thus

for spherical one (16*6=96) ninety six bits of original cipher secret is used. What's the sequence of operations performed in every round? Let I1, I2 …I6 be the inputs to [5] spherical one, functions in spherical one are: - (i) Multiply I1 and K1. (ii) Add I2 and Godwin Austen. (iii) Add I3 and K3. (iv) Multiply I4 and K4. (v) Now, step one is EXOR with step three. (vi) Step two EXOR with step four. (vii) Multiply step five with K5. Similar operations square measure performed in different rounds.

3.5 HOMOMORPHIC ALGORITHM

Homomorphic secret writing uses uneven key rule within which 2 completely different keys square measure used for secret writing and decipherment i.e. public key and personal key [10]. In arithmetic homomorphic suggests that conversion of 1 knowledge set to a different, while not losing its relation between them. In homomorpic complicated arithmetic functions square measure applied to inscribe the information and similar however reverse operation is applied to rewrite the information.

RC5 could be a symmetrical secret writing rule developed by Bokkos Rivest in 1994. RC stands for "Ron's Code" or "Rivest Cipher". It's appropriate for hardware and computer code implementation. The RC5 secret writing rule could be a w is word block cipher that converts plaintext knowledge blocks of sixteen, thirty two and sixty four bits into the cipher text blocks of a similar length. RC5 uses a key selectable length b (0, 1, 2, ...,, 255) byte. The rule is organized as a collection of iteration known as rounds r that takes values within the vary (0, 1, 2,...,, 255) as demonstrate in Fig. 5. The operation performed on the blocks embrace bitwise XOR of words, data-dependent rotations by suggests that of circular left and right rotations and Two's complement addition/subtraction of words, that is moduloaddition/subtraction. RC5 could be a totally parameterized family of secret writing algorithm; it's additional accurately nominal as RC5- w/r/b wherever the word size is w bits, secret writing consists of a plus range of rounds r and b denotes the length of the secret writing key in bytes. The first instructed alternative of parameter were w=32bits, r=12 and b=16 bytes. For all variants, RC5-w/r/b operates on 2 w-bit words exploitation the subsequent operations. The fundamental operation in RC5 is outlined as follows:

A+B number addition modulo-

- A+B number subtraction modulo-
- A⊕B bitwise exclusive-or of w-bit words

A<<< B rotation of the w-bit word A to the correct by the number given by the smallest amount important lg w bits of B

A>>>>B rotation of the w-bit word A to the correct by the number given by the smallest amount important lg w bits of B

There square measure 3 routines in RC5: key enlargement, secret writing and decipherment. During this section discuss the key - enlargement rule is employed to get the spherical sub keys which will be utilized in each secret writing and decipherment rule. RC5 features a completely different rule for secret writing and decipherment, within the secret writing it uses number addition modulo- however in decipherment it uses number subtraction modulo- . RC5 could be a symmetrical key secret writing thus secret writing and decipherment rule uses a similar key [13]

IV. CONCLUSION & FUTURE WORK

Cloud computing is dynamical the manner IT departments pass. Businesses have a variety of methods to the cloud, as well as infrastructure, platforms and applications that ar accessible from cloud suppliers as on-line services. Many folks is also confused by the vary of offerings and also the word wont to describe them and can be unsure of the danger and edges. Security may be a major demand in cloud computing whereas we tend to refer information storage. There are variety of existing techniques won't to implement security in cloud. During this paper, we tend to mentioned variety of rhombohedral and uneven algorithms. Our future are considering some issues associated with existing security algorithms and implement a higher version of DES, 3DES, AES, RSA, IDES, Blowfish

REFERENCES

[1.] [1]. P.Kalpana, "Cloud Computing –Wave of the Future", International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 3, ISSN 2249–071X, June 2012.

[2.] [2]. Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.

[3.] [3]. Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011.

[4.] [4] Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance Cryptography algorithm for improving data security", International Journal of Advanced Research in Computer

[5.] [5] V. Sandhya, "A Study on Various Security Methods in Cloud Computing", International Journal of Advanced Research in Computer Science, Volume 2,No.6, Nov-Dec 2011.

[6.] [6]. Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science and Information Technology, Vol.2(3), 242-249, 2012.

[7.] [7] Birendra Goswani, Dr.S.N.Singh, "Enhancing Security in Cloud computing using Public Key Cryptography with Matrices", International Journal of Engineering Research and Applications, Vol 2, Issue 4, 339-344, July-Aug 2012.

[8.] [8]. G. Jai Arul Jose, C.Sanjeev, Dr. C.Suyambulingom, "Implementation of Data Security in Cloud Computing", International Journal of P2P Network Trends and Technology, Vol 1, Issue 1, 2011.

[9.] [9].William Stallings, "Network Security Essentials Applications and Standards", Third Edition, Pearson Education, 2007.

[10.] 10. G. Devi , M. Pramod Kumar, "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803, pp. 592-596,2012.

[11.] 11. Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.

[12.] 12. Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication,NIST SP - 800- 144 ,80 pp., 2011.

[13.] 13. G. Lin, D. Fu, J. Zhu, and G. Dasmalchi, "Cloud Computing: IT asa Service," IT Professional, vol. 11, pp. 10-13, Mar./Apr.2009.

[14.] 14. Mandeep Kaur and Manish Mahajan, "Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology, Vol. 2, pp.831-835, October 2012.

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

[16.] 16. Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , "Cloud Computing System Based on Trusted Computing Platform", International Conference on Intelligent Computation Technology and Automation, Volume 1, pp.942-945, 2010.

[17.] 17. Pearson, S., Benameur, A., Privacy, "Security and Trust Issues Arises from Cloud Computing", Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference, pp.693-702, 2010.

[18.] 18. Lizhe Wang, Gregor von Laszewski, Marcel Kunze, Jie Tao, Cheng Fu, Xi He, Andrew Younge, "Cloud Computing: A Perspective Study", New Generation Computing- Advances of Distributed Information Processing, Volume 28, pp.137-146, 2010.

[19.] 19. Puneet Jai Kaur, Sakshi Kaushal, "Security Concerns in Cloud Computing", Communication in Computer and Information Science Volume 169, pp.103-112, 2011.

[20.] 20. Priyanka Arora, Arun Singh, Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal, pp.179-183, 2012.