IJRSET SEPTEMBER 2017 Volume 4, Issue 9 Pages: 8-13

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

SURVEY ON CLOUD COMPUTING AND SECURITY

[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 is sharing of computer hardware and software assets over the web with the goal that anyone. As cloud computing ends up popular, increasingly more delicate information is being centralized into the cloud nowadays. For the protection of data privacy, touchy data usually have to be scrambled before re-appropriating, which makes compelling data utilization an exceptionally challenging task because all the data which we re-appropriate are in encoded format. Its very nature in any case makes it open to an assortment of security gives that can influence both the providers and consumers of these cloud administrations. These issues are primarily related to the safety of the data coursing through and being put away in the cloud, with sample issues including data availability, data access and data privacy. This paper reviews that the cloud computing security issues and also examines about the cloud computing security algorithms.

Keywords: [Cloud Computing, Security issues, on-demand network, Data encryption, Cloud Security Standards, threats, attacks.]

1. INTRODUCTION

Cloud computing is another name for Internet computing. The definition of cloud computing gave by National Institute of Standards and Technology (NIST) says that: "Cloud computing is a model for empowering on-demand and convenient system access to a mutual pool of configurable computing resources (e.g., servers, storage applications, networks and services) that can be rapidly provisioned and released with minimal management exertion or service provider interaction. For some it is a paradigm that gives computing assets and storage while for other individuals, it is only a way to access software and data from the cloud [1]. Cloud computing is popular in organization and academic today because it gives its customers scalability, adaptability and availability of data. Also cloud computing decreases the cost by enabling the sharing of data to the organization. Organization can port their data on the cloud with the goal that their shareholders can use their data. Google apps is an example of cloud computing. Cloud computing, also known as on-demand computing, is a kind of online computing that allows end customers to share information and assets. Significantly more officially, the National Institute of Standards and Technology (NIST) portrays cloud computing as a model for empowering inescapable, that can be rapidly provisioned and released with

minimal management exertion or service provider interaction.

Figure 1: Cloud Computing Security

Cloud computing doesn't have a common accepted definition yet. The Na
tional Institute of Standards and Technology (NIST) described five fundamental attributes of cloud computing, to be specific: on-demand self-administration, wide system get to, resource pooling, fast versatility or expansion, and estimated administration [2]. Also, cloud computing is portrayed as a dynamic and often easily loosened up platform to give transparent virtualized assets to customers through the Internet. Cloud computing architecture consists of three layers: (i) Software as a service (SaaS); (ii) Platform as a service (PaaS) and (iii) Infrastructure as a service (IaaS). The clouds are also observed as five component architectures that include clients, applications, platforms, infrastructure and servers. The present clouds are conveyed in one of four arrangement models: (a) open clouds in which the physical infrastructure is claimed and managed by the service provider; (b) network clouds in which the physical infrastructure is had and managed by a consortium of organizations; (c) private clouds in which the infrastructure is had and managed by a particular organization and (d) half and half clouds which incorporate combinations of the past three models. Clouds bring out colossal advantages for the two individuals and adventures. Clouds support economic savings, re-appropriating mechanisms, asset sharing, any-where any-time accessibility, on-demand scalability, and service adaptability. Clouds could also offer better security advantages over individual server organizations [3]. Since a cloud totals resources, cloud suppliers sanction ace security personnel while run of the mill organizations could be restricted with a system overseer who most likely won't be knowledgeable in digital security issues. Similarly, clouds are stronger to Distributed Denial of Service (DDoS) attacks because of the availability of assets and the elasticity of the architecture. The clouds support versatile computations where Virtual Machines (VMs) migrate starting with one physical machine then onto the following. In addition to lightening devoted DDoS assaults, compact computations help to maintain a strategic distance from settings in which a singular director has select control over the computation.

2. LITERATURE SURVEY

Mr. Niteen Surv, Mr. Balu Wanve, Mr. Rahul Kamble, Mr. Sachin Patil and Mrs. Jayshree Katti (2015) proposed client side AES encryption and decryption strategy utilizing mystery key. Client side encryption is a successful way to deal with give security to transmitting information and put away information. This system additionally gives security and protection to the information which is put away on the cloud. To execute this system utilized client side AES encryption and decryption procedures with single mystery key. This mystery key has various bits like 128 bits, 192 bits, 256 bits. Along these lines, client can utilize any bit of key from alternative. In this system, on the off chance that client utilize mystery key for encryption, at that point client ought to have utilize same mystery key for decryption. This encryption and decryption will do at client side. While decoding information it access record from

cloud safely and unscramble at client side with single mystery key which is utilized at encryption time. At the cloud side, the database contains just scrambled document. Along these lines, the security and protection is given to the information which is put away on cloud database. In the event that client need to impart the information to another client, at that point the mystery key likewise mandatory to share these information. This system utilized in public, private and network cloud. It imparts the mystery key to regard to cloud type. It bolsters all sort of information for example writings, sounds, recordings, pictures, other sort of information and so forth. **Nivedita Shimbre, Prof. Priya Deshpande (2015)** proposed the record conveyance and SHA-1 system. At the point when record is conveyed then information is likewise isolated into numerous servers. So here the need of information security emerges. SHA-1 and AES algorithm is a standard algorithm. Accuracy check and Error confinement Algorithm and Error Recovery Algorithms are client characterized algorithms. SHA-1 algorithm: SHA-1 algorithm is has a place with cryptographic family, it produces 20 byte hash esteem. In SHA-1 algorithm message digest length is fix that is 160 bit. • **Advanced Encryption Standard:** Advanced Encryption Standard algorithm is a Symmetric square figure. In which utilized just a single mystery key. A similar key is utilized for encryption just as decryption. Fundamentally AES standard key sizes are 128 bit, 192 bit and 256 bit. Here utilized 128 bit key size for encryption just as decryption. For 128 bit key size, calculation unpredictability is in every case less when contrasted with other key size. • **Correctness check and Error restriction Algorithm**: 1. Challenge for specific document 2. Get record parts from 3 servers of that document 3. Check all record part is available or not 4. Get total document from reinforcement server. 5. Gap that reinforcement record into three sections 6. Think about each hash code of document part from principle server with each hash code of record part from reinforcement server. 7. In the event that Hash codes are not coordinated, at that point it returns which server is making trouble. • **Error Recovery Algorithm**: 1. Once distinguish which record part from which server is acting mischievously.2. Get that document parts from reinforcement server. 3. Once get place that document part into fundamental server. 4. Presently when download record get total our unique document. **Nasrin Khanezaei, Zurina Mohd Hanapi (2014)** proposed information security in cloud information storage was explored, which is basically a conveyed storage system. Cryptography method often used to verify the information transmission and putting away among client and cloud storage administrations. The focal point of this paper was on giving secure records transmission between these two substances. Advanced Encryption Standard (AES) is symmetric cryptographic algorithm. It is one of the most ordinarily utilized and most secure encryption algorithms accessible today. The algorithm depends on a few substitutions, changes and straight changes. It said that up until today, no practicable assault against AES exists. Subsequently, governments, banks and high security systems around the globe are favored utilizing AES for the encryption standard. The substances of the system are: Sender, Receiver and Cloud Storage System (CSS). **Mr. B.Thiyagarajan, Mr. Kamalakannan.R (2014)** proposed a structure which includes verifying of documents through record encryption. Aes Algorithm The Advanced Encryption Standard (AES) is a symmetric-key square figure distributed by the National Institute of Standards and Technology (NIST). The criteria characterized by NIST for choosing AES fall into three zones: 1. Security 2. Cost 3. Implementation. AES is a non-Feistel figure that encodes and decodes an information square of 128 bits. It utilizes 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, relies upon the quantity of rounds. To give security, AES utilizes four kinds of

changes: substitution, stage, blending, and key-including. Stage a transposition step where each line of the state is moved consistently a specific number of steps. Mixing a mixing action which takes a shot at the fragments of the state, joining the four bytes in each section. Key-Adding In the AddRoundKey step, the subkey is gotten together with the state.. For each cycle, a subkey is gotten from the principle key utilizing Rijndael's key timetable; each subkey is a similar size as the state. The subkey is incorporated by joining each byte of the state with the relating byte of the subkey using bitwise XOR. AES is a calculation for performing encryption (and the reverse, decryption) which is a progression of well-portrayed advances that can be sought after as a strategy. **Vishwanath S Mahalle, Aniket K Shahade (2014)** proposed a hybrid encryption algorithm utilizing RSA and AES algorithms for giving data security to the client in the Cloud. A hybrid encryption strategy utilizing the AES and RSA algorithms is utilized where 128 bit mystery key for AES and 1024 bit key for RSA is utilized. Transfer alternative prompts an age of RSA public key-n, RSA public key-e, .RSA private key-d and AES mystery key, client will require to spare the RSA private key and AES mystery key, As soon as client attempts to transfer the data on cloud, the data is first put away in a transitory index and in the wake of calling AES and RSA algorithm, requiring the client to enter the AES mystery key the document will get put away into the data base forever comparing to the client account and the brief record get erased. Presently, when the client needs to get to the data put away in cloud or needs to download the data, it experiences the download technique whereby client needs to determine the filename to be downloaded and needs to give the AES mystery and RSA private key which is stayed quiet by the client and is known distinctly to him. The primary reason behind utilizing RSA and AES encryption algorithm is that it gives three keys for example public key for encryption, and private key and mystery key for decryption. **Vikas K.Soman, Natarajan V (2017)** proposed an improved hybrid data security algorithm for the cloud to verify data assurance of the cloud. The Cryptographic data Encryption is one of the answer for secure data in cloud figuring stage. There are symmetric (for example DES, AES) deviated (for example RSA, EIGamal, ECC), Digital mark (MD5, SHA) algorithms are available and the mix of these algorithms structure hybrid data security cryptographic algorithm. Here proposing a blend of ECDSA, SHA256 and AES is utilized for sending and getting data message on the cloud. The best possible utilization of public and private key activity will make the data in the cloud as a lot higher security. The message record transfer hybrid data security algorithm: The cloud client is having the data message or document to be secure before that must be sent to the Cloud Service Provider. The ECDSA with SHA 256 message digest and comparing advanced marks are created in the client machine. The data message or document with public key is encrypted utilizing AES encryption algorithm. The encrypted data or record is sent to cloud specialist co-op. The data message document is then store it in to comparing cloud server. The message download hybrid data security algorithm: The cloud client needs to demand the cloud specialist organization to download his/her put away secure data message or document. **Punam V. Maitri, Aruna Verma (2016)** proposed security component utilizing symmetric key cryptography algorithm and steganography. System AES, blowfish, RC6 and BRA algorithms are utilized to give square savvy security to data. Hybrid cryptography algorithm present by creator A. Shahade. AES and RSA algorithms are utilized into hybrid algorithm.AES algorithm require a solitary key. In hybrid algorithm three keys are utilized. For data transfer on cloud mandatory keys are AES mystery key and RSA public key. Private Key of RSA and AES mystery key are basic to download data from cloud. At whatever point use tries to

transfer data on cloud first that record put away onto index for brief time. In encryption process first AES algorithm is connected on document after that RSA algorithm is connected on encrypted data. Turn around procedure is pursued for decryption. Subsequent to applying keys that record clandestine into encoded structure and put away on cloud server. Focal points of hybrid algorithm are data honesty, security, classification and accessibility. **PRABU KANNA, V.VASUDEVAN (2017)** an Improved Hybrid Encryption is proposed, in which the data to part and to stock up in various different cloud condition to offer high security for the data put away in multi cloud and execution of nature is additionally better and the outcome is contrasted and the AES RC6, Blowfish, DES encryption algorithm and it is examine better data security and concerning the time required for procedure. Its exhibition force of encryption strategy is additionally expanded and the data is put away with higher security. an Improved Hybrid Encryption is utilized to verify the data content data put away in multi cloud. The improved hybrid encryption is the mix of AES, Blowfish and RC5 and ECDH encryption algorithm. The data are separated into different number of pieces dependent on multi cloud assets. And the split pieces are put away in multi cloud utilizing various sorts of encryption procedure. This kind of procedure encourages the clients to confide in the earth. The method for putting away records in various cloud are pursues. **N. Jayapandian, Dr. A. M. J. Md. Zubair Rahman and S. Radhikadevi, M. Koushikaa (2016)** proposed symmetric DES and unbalanced key RSA encryption algorithms is done by various needs. The key utilized is characterized as far as encryption and decryption it is possible that it is same or extraordinary. The DES methods for the data encryption standard on cloud. This kind of algorithm where same key is utilized for encryption and decryption and essentially secure by the mystery key strategy. DES is one of the most broadly acknowledged, publicly accessible encrypted systems. It was created in 1970s by IBM organization, yet was later control by the National Institute of Standards and Technology (NIST) here that DES algorithm works by utilizing a similar key to make protection of the guidance by the procedure of encrypt and unscramble a message in a system, so both the client of the space and the supplier must know and they same will utilize mystery key for further security. Here, will actualize to move the record on , symmetric-key algorithm for the encryption of electronic data, DES has been done by the more secure Advanced Encryption Standard algorithm of the symmetric key procedure in the encryption and decryption philosophy.. **G.Sai Vennela, N.Venkata Varun, N.Neelima and L.Sai Priya (2018)** proposed symmetric key cryptography the Blowfish algorithm sets aside less encryption effort for content records and recordings. Despite the fact that the DES algorithm has fast of encryption while encrypting content records of little size (1 MB), yet it can without much of a stretch be split on account of animal power assault. Data Encryption Standard (DES): DES was presented by the IBM in late 70's. In this strategy the key size is 56(bit). In Encryption stage, DES takes 64-bit plain message as information and produces 64-bit figure content utilizing 16 round Feistel structure. Triple Data Encryption Standard (3DES): In cryptography 3DES uses a symmetric key which applies DES algorithm 3 times on every datum square. It comprises of 3 distinctive keys which are K1, K2 and K3. That implies it gets triple of unique key size, so it takes 168bit length key for the procedure. The procedure begins with encrypting the plain message with k1 later decoding the acquired figure utilizing key K2. At long last encrypting the figure created utilizing K2 with key K3. In view of this encrypt-decrypt-encrypt process the assaults can be decreased and the data can be verified than DES.

CONCLUSION

Cloud computing gives many advantages like storage capacity, cost reduction and handling power and so forth. Anyway it has its own security related issues that threaten the organizations to adopt the cloud technology. Many researches are going at present to distinguish the security threats and the potential solutions to those threats. This paper gives a review of the various frameworks associated with cloud data verification. In this paper various strategies for reliability verification for re-appropriated data on cloud are examined.

REFERENCES

[1]. Mr. Niteen Surv, Mr. Balu Wanve, Mr. Rahul Kamble, Mr. Sachin Patil and Mrs. Jayshree Katti, "Framework for Client Side AES Encryption Technique in Cloud Computing", c 2015 IEEE.

[2]. Nivedita Shimbre, Prof. Priya Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm", © 2015 IEEE.

[3]. Nasrin Khanezaei, Zurina Mohd Hanapi, "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", ©2014 IEEE.

[4]. Mr. B.Thiyagarajan, Mr. Kamalakannan.R, "Data Integrity and Security in Cloud Environment Using AES Algorithm", ©2014 IEEE.

[5]. Vishwanath S Mahalle, Aniket K Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", ©2014 IEEE.

[6]. Vikas K.Soman, Natarajan V, "An Enhanced hybrid Data Security Algorithm for Cloud", ©2017 IEEE.

[7]. Punam V. Maitri, Aruna Verma, "Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm", c 2016 IEEE.

[8]. G. PRABU KANNA, V. VASUDEVAN, "A NEW APPROACH IN MULTI CLOUD ENVIRONMENT TO IMPROVE DATA SECURITY", © 2017 IEEE.

[9]. N. Jayapandian, Dr.A.M.J.Md.Zubair Rahman and S.Radhikadevi, M.Koushikaa, "Enhanced Cloud Security Framework To Confirm Data Security on Asymmetric And Symmetric Key Encryption", © 2016 IEEE.

[10]. G. Sai Vennela, N.Venkata Varun, N.Neelima and L.Sai Priya, "PERFORMANCE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS FOR CLOUD SECURITY", © 2018 IEEE.

[11]. Xidan Song, Yulin Wang," Homomorphic Cloud Computing Scheme Based on Hybrid Homomorphic Encryption",@2017 ieee.

[12]. Zainab Hikmat Mahmood, Mahmood Khalel Ibrahem," New Fully Homomorphic Encryption Scheme Based On Multistage Partial Homomorphic Encryption Applied In Cloud Computing",@0218 IEEE.

[13]. Ming-quan Hong,Wen-bo Zhao, Peng-yu Wang," Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing", © 2016 IEEE

[14]. Yong Ding, Xiumin Li," Policy Based on Homomorphic Encryption and Retrieval Scheme in Cloud Computing", 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)

[15]. Adil Bouti, Jorg Keller," Towards Practical Homomorphic Encryption in Cloud Computing", 2015 IEEE 4th Symposium on Network Cloud Computing and Applications.