ISSN: 0976-3104
SPECIAL ISSUE (SCMDSA)

www.iioab.org
THE IIOAB JOURNAL
www.iioab.webs.com
COMPUTER SCIENCE

ARTICLE OPEN ACCESS

AN INVESTIGATION ON THE TECHNIQUES USED FOR ENCRYPTION AND AUTHENTICATION FOR DATA SECURITY IN CLOUD COMPUTING

Tamilarasi Rajamani[*], PrabuSevugan, Swarnalatha Purushotham

VIT University, Vellore-Tamilnadu, INDIA

ABSTRACT

The paper deals with data security of cloud and their authentication techniques. Now-a-days, the cloud data security method uses the symmetric encryption and asymmetric encryption algorithms with their strong authentication techniques. The use of relevant algorithm deals with the level of data safety in cloud because data security in cloud computing is a serious issue as the data centers are located worldwide. Authentication is the most essential procedure to ensure the cloud data in a secured manner. However, strong user authentication is the main requirement for cloud computing that reduces the unauthorized user access of data on cloud. Data security is a more important issue of cloud computing. The survey is completely based upon the estimation for the cloud data security and authentication resolution. Almost, the inventors use the symmetric and asymmetric encryption algorithms with other authentication methods. Symmetric algorithms are AES, DES, Blowfish, RC2, 3DES and asymmetric algorithm are RSA, DSA, Diffie-Hellman and ELGamal. The Authentication techniques are one time password, Digital signature, and Biometric method. So a hybrid technique which is a combination of these encryption techniques and authentication method gives a more excellent and strong security on cloud data.

Received on: 30th-Nov-2015
Revised on: 11th-March-2016
Accepted on: 26th – March-2016
Published on: 18th–May-2016

KEY WORDS

Authentication; Cloud security; symmetric encryption; asymmetric encryption.

***Corresponding author: Email:** tamilarasi.r2014@vit.ac.in; **Tel:** +40-9001010010; **Fax:** +40-9001010012

INTRODUCTION

Cloud computing supports distributed service oriented architecture, multi-users and multi-domain administrative infrastructure, it is more prone to security threats and vulnerabilities. At present, a major concern in cloud adoption is its security and Privacy. Cloud computing nowadays is the precondition and essential part of the computing globe using whole day developing in its usages and popularity. Huge estimate of users is currently depending on cloud computing application for their everyday work of authority and produce services over the computer internet. Cloud represent as data centre. A client makes use of cloud resources, applications, storage and different services and is charged accordingly [1].

CLOUD SERVICE MODEL

Cloud computing providers' offers their service according to several fundamental models.

- Software as a Service(SaaS)
- Platform as a Service (PaaS) and
- Infrastructure as a Service (IaaS).

Software as a service

- In SaaS model, cloud suppliers introduce and work application, programming in the cloud and cloud clients get to the product from cloud customers.Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminate the need to install and run the application on the cloud users own computers which simplifies maintenance and support.

| Guest Editors | Profs. Swarnalatha & Prabu |

www.iioab.org

THE IIOAB JOURNAL

www.iioab.webs.com

Platform as a service

- In platform as a service, the cloud providers deliver a computing platform including operating system, programming language execution environment database and web server. The resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually.

Infrastructure as a service

- In cloud service model, providers of IaaS offers computer – physical/virtual machines, other resources include hypervisor, Virtual Machine (VM) disk image library, raw/file based storage, firewalls, load balancers, virtual LAN and internet Protocol (IP) address.IaaS cloud providers supply these resources on demand from their data centers. To deploy their applications, cloud users install OS and application, software on the cloud infrastructure.Cloud providers bill IaaS service on a utility computing basis (i.e.) cost which reflects the amount of resources allocated and consumed.This part is basically belongs to admin part or about service provider [2].

CLOUD DEPLOYMENT MODELS

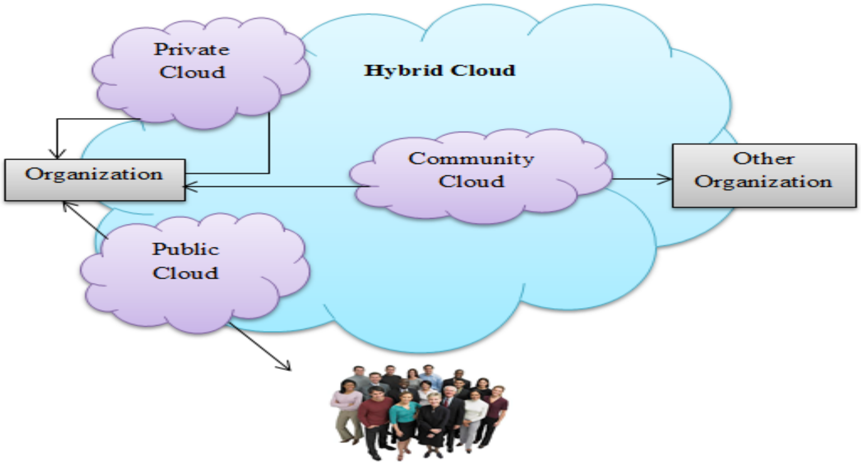

Fig.1: Cloud Deployment Model

Private cloud

- Private cloud computing model it’s operating solely for a single organization within the boundary of the organization.
- It maintains internally or externally to support business operation.
- Cloud providers share the accessible resources and applications, so that in private cloud users can flexibly share and use it. They work similar to an intranet within an organization. Unauthorized persons can’t access the data and share the resources. Using this security the private cloud is more secured when compared to the public cloud [3].
- To create a private network restructures the existing infrastructure by adding virtualization and cloud line interface.

Public cloud

- Public cloud is a cloud infrastructure that is made available to the general public as pay per use concept-able model. The resources are hosted on the service provider’s premises.
- Resources are dynamically provisioned through publically accessible web application or web services (SOAP) from a third party premises.
- It is cost effective because all the computing resources are shared worldwide.
- It is fully customer self services; the customer can access the public cloud through internet.

www.iioab.org
THE IIOAB JOURNAL
www.iioab.webs.com

Hybrid cloud

- This cloud infrastructure is a combination of two or more different cloud infrastructures (community, private, or public) bound together by some standardized or using some technology and allow migradition data and application between them [4].

Community cloud

- The cloud infrastructure is combined by several organisms [5]. (or) In community cloud is a multi-tenant cloud service model that is shared among several or organizations and that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider [6].

CLOUD COMPUTING SECURITY

It refers to a broad set of policies, technologies and controls deployed to protect data, applications and associated infrastructures of cloud computing. Cloud computing can be implemented with different service models (Saas, Paas, Iaas) and deployment models (private, public, hybrid, community) so we need to provide security for cloud data. Security issues for cloud computing is classified as two levels they are.

Security issues faced by cloud providers (organization providing software platform (Infrastructure -as-a-service)) then cloud.

The cloud provider assures that the infrastructure is protected and secure. The cloud provider must protect the data and application of the cloud users.

Security issues faced by their customers

The provider must ensure that their infrastructure is secure and their clients, data and application are protected while the customer must ensure that the provider has takes the proper security measures to protect their infrastructure. The main security issue is virtualization. Virtualization must be properly configured managed and secure.

CLOUD SECURITY CONTROLS

Cloud security architecture is effective only if the right protective execution is set up. Efficient cloud security design ought to perceive the issues that will emerge with security administration. Security administration addresses these issues with security controls. These controls are placed set up to shield/secure any short coming in the framework and reduce the effects of attack.

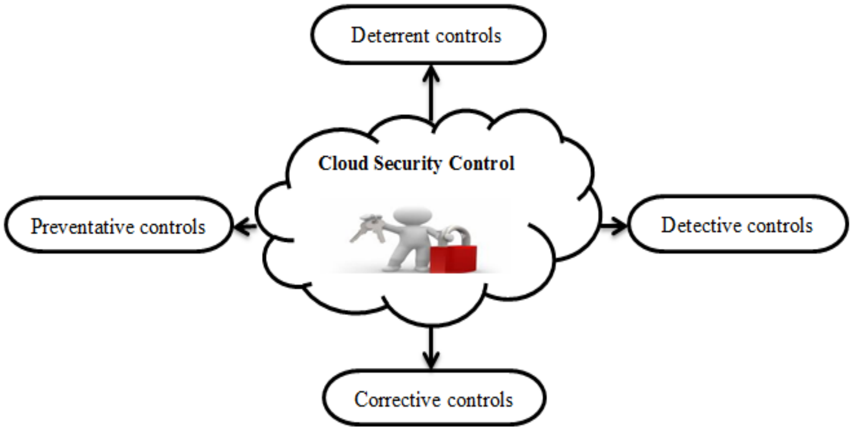

Fig: 2. Cloud Security Control

Deterrent controls

- These controls are set in place to prevent any purposeful attack on a cloud system. It is like a warning sign on a fence or a property. They do not reduce the actual vulnerability of a system.

Preventative controls

- These controls upgrade the strength of the system by managing the vulnerabilities. It safeguards vulnerabilities of the system. It attacks the users from the preventative controls in place to cover the attacks and reduce the damage and violation to the system security.

Corrective controls

- The corrective controls are used to reduce the effect of an attack. Unlike the preventative controls. The corrective controls takes action as an attack is occurred.

Detective controls

- Detective controls are used to detect any attacks that may be occurring to the system. In the event of an attack, the detective controls will signal the preventative or corrective controls to address the issues.

RELATED WORK

In proposed a data security in cloud computing. There are additionally existing algorithms. That use various encryption and decoding techniques to make safe client data on a cloud. This also makes user be able to load their data at cloud except for any worry and can retrieve their data as per use. Here many algorithms are provided to security for users data on cloud with secure the user information from malicious activity [7].

It presents the review which totally the estimation for the cloud assurance solution. The creators nearly advantage the encryption code strategy. The accepted encryption techniques were discussed the overview such as AES, DES, 3DES, RC2, RC6 and Blowfish. The cloud security approach has proposed the use of AES algorithms, without any gaps in AES [4].

The proposed a hybrid (combination) encryption method compresses of using asymmetric and symmetric cryptographic algorithms. The symmetric key distribution among cloud provider and legitimate users is executed utilizing asymmetric techniques. At the last moment, we compare hybrid (mixed) technique applying the connection of the AES and RSA algorithms. The present summary shows that the new method gives merits of symmetric algorithm by efficient processing time and the forcefulness of asymmetric algorithm in their key size. Actually the present lightweight algorithm is faster than other cryptographic methods in processing data [8].

In studied in user authentication to protect data of encryption techniques within cloud computing. Cloud computing permit client to access the internet browser without application installation and approach their information at any system utilizing internet browser. This framework approves the security of the data in cloud server. Here user is using AES algorithm for encryption and decryption structure to create cloud users data secured and also ensure the information privacy in the cloud. This paper presents the protected data mechanism to clarify the issues of data security and privacy in cloud computing [2].

Inproposed techniques that deal with secure of static data as well as dynamic data in cloud. AES is faster than RSA. RSA presentation depends on prime number and complication depends on that value of primes and also this paper provides linking viewpoint of security, protection, detection of threads [9].

In displayed symmetric key encryption strategies, for example, DES and AES encryption quality. The study tells that the symmetric key encryption strategies are utilized for the majority well-organized than asymmetric key encryption techniques. Data security in cloud can be improved by applying a grouping of separate methods at the same time [10].

Inproposed to store secure data in various cloud, Data encryption and separation (splitting) are the two techniques used. Then AES-256 also used to secure with data encryption purpose. And also data splitting is used which

www.iioab.org THE IIOAB JOURNAL www.iioab.webs.com

separates file into subparts to store into different clouds. These techniques benefit to secure files from unauthorized users in looking all files [11].

In proposed analytical study of different data security methods on cloud computing as it produce a huge number of security problems like RASP It issues secure and effective series request and ken query services for secured data, TRSE, CP-ABE, KP-TSABE, KP-ABE, RSA, AROCrpyt, AES, Blowfish, DES, RSA, ASIF. Different data security algorithms are referred in the following section [3].

In proposed an algorithm called RSA technique. It is a new method which assembles the essentially of public key systems. While using this method data security will increase with minimum execution time and cost. But RSA also have disadvantages like imitation public key techniques, complication of key production, security requirements and with low speed [12].

In proposed 512 bit AES encryption algorithm that is used to provide security on medical data present moment in cloud in other side.Only the authorized user can decrypt the data. It is very securable and highly powerful. It has only one drawback that is AES 512 is the requirement for huge design area [13].

Inpresented the issue of data security in cloud data storage is considered, which a distributed storage system is basically. Using cryptography method is used to transformthe secure data and storing between user and cloud storage services. A hybrid method of symmetric and asymmetric encryption methods like AES and RSA are used. These techniques mainly achieve the confidences of data security in cloud. RSA encryption will provide complexity for attackers for decreasing the time of data communication by using AES encryption techniques [14].

In proposed an Elliptic curve cryptography that provides the higher level ofsecurity and also presentation is very much improves than another encryption techniques. The paper proposed ECC algorithm which deals with one views smallest amount of time to encrypt the data. Here there are three security frameworksnamely Authentication, encryption and separation of customs for the security that has been fulfilled which benefits to succeed the greater level of safe and secure. The solution displays that ECC is more secured and has the well execution than other encryption techniques [5].

In proposed Architecture is based on block based symmetric cryptography Algorithms, Block based symmetric is efficient & secured. Using Symmetric encryption techniques but it has only one drawback the authors have not proved with real time implementation of the architecture [15].

In proposed Encryption and obfuscation techniques increase the confidentiality of data, obfuscation as two different systems to ensure the data in the cloud storage. Encryption is the procedure of changing over the discernable (readable) content into incomprehensible structure utilizing an algorithm and a key. Obfuscation is same like encryption. Obfuscation is a procedure which masks illegal clients by executing a specific scientific capacity or utilizing programming methods. Based on the kind of data, encryption and Obfuscation can be applied. Encryption can be applied to letters in order and alphanumeric sort of data and obscurity can be applied to a numeric sort of data. Applying encryption and Obfuscation methods on the cloud data will give more provide against unapproved use. Classification could be accomplished with a mix of encryption and obscurity [16].

In presented Rijndael EncryptionAlgorithm and EAP (Extensible Authentication Protocol) the proposed design and architecture that can help to encrypt and decrypt the document at the client side that gives security to data at rest as well as while moving. The authentication is utilized for the transport and utilization of keying material and parameters produced by EAP strategies [17].

In studied conceptual paper Comparison of Symmetric and Asymmetric algorithms, shows the superiority of symmetric algorithm and AES shows superior algorithm performance among the various algorithms [18].

In proposed group based authentication and key agreements protocols. This framework was executed in the cloud environment with a test bed of 20 systems. This usage results in appropriate authentication with access control for query signature based cloud services.This plan likewise acknowledges with important control for authentication for multi-group. Additionally, the user can get the cloud benefit once they are enrolled as an individual from a group, also ensured the exactness of the authentication and data sharing for the user in the dynamic group.Hence

www.iioab.org
THE IIOAB JOURNAL
www.iioab.webs.com
COMPUTER SCIENCE

by dealing with this authentication time and movement in the dynamic group. At long last, the capacity and computational cost are stable [19].

In presented this paper induced brief analysis on data security in cloud environment, It is well-known that cloud computing has numerous potential focal points, there are still many actual issues that should be tackled and the data is moving to the public or hybrid cloud.As indicated by the analysis of data security, it is required to have an incorporated and extensive security solution for addressing the issues of safeguard top to bottom [20].

In studied symmetric and asymmetric algorithms, the paper draws the inference proxy re-encryption and hierarchical attribute-based encryption is most proposed approaches to ensure data security but nearly 33% is not validated. But this paper considered 15 research papers to draw conclusion [21].

In presented a hybrid encryption algorithm using RSA and AES algorithms for providing data security to the user in the Cloud. The greatest purpose of interest it gives us is that the keys are delivered on the reason of structure time in this way no intruder can even figure them there by giving us extended security close by convenience. Private Key and a Secret key are just known to the client and in this manner client's private data is not accessible to anybody not even the Cloud's Administrator. [22].

In proposed AES Algorithms three way mechanism techniques. Firstly Diffie-Hellman algorithm is utilized to create keys for key exchange step. Then digital signature is utilized for authentication, from that point, AES encryption algorithm is utilized to encrypt or decrypt client's data file. This is executed to give trusted processing environment with a specific end goal to avoid data change (modification) at the server end. The AES (Advanced Encryption Standard) encryption algorithm to protect confidentiality of data stored in cloud [23].

In proposed Elliptic curve Diffie-Hellman (ECDH) and vicariate polynomial secret sharing. The main goal of these schemes is to ensure the data protection and security in the cloud serverandinclude the symmetric property in secret sharing to effectively decrease the expense to share the shares the customer and the server [24].

In proposed RSA algorithm,it only authorized person can use the data. Since Cloud Computing stores the data and dispersed assets in the open environment, security has become the fundamental obstruction which is hampering the organization of Cloud environments. Even though the Cloud Computing is promising and productive, there are many difficulties for data security as there is no region of the data for the Cloud client. [25].

In presented Symmetric algorithms (AES, Triple DES and DES). Transferred of data is encrypted in the upper layer on top of the transport layer instead of using IPS and SSL. In this manner, the plan for the execution change can be connected without altering the execution of IP layer and efficient secure communication by pre-handling of encryption in the upper-layer is realized [26].

In proposed Fragmentation techniques. To applies the fragmentation techniques in the cloud environment with minimal encryption to prevent data exposurethe fragmentation method which is efficiently stores the data on CSP servers utilizing the base possible measure of encryption. The fragmentation procedure is applied to a relational database where the tables are treated as independent fragments. This fragmentation and distribution the methodology reduces the trust expectancies towards the outer administration suppliers and subsequently enhances security and privacy [27].

In studied symmetric encryption algorithm, AES is found suitable and the most secured algorithm for Amazon EC2, the model utilized three-layer framework structure, in which every floor performs its own obligation to guarantee that the information security of cloud layers. The main layer: in charge of user authentication, nearly this is two component confirmations; however, free cloud suppliers utilize one element as samples eyeos, cloudo, and freezoh. The second layer: responsible for user's data encryption, and ensure the protection of user through a specific path by utilizing one symmetric encryption algorithms. Likewise, permit security from a user.The third layer: The user data for fast recovery this depends on the speed of decryption [28].
In studies in issues relevant of cloud data storage techniques and security in virtual environment. The paper proposed RSA public key cryptosystem that provides data storage and security in cloud computing. RSA algorithm provides more security in high possibility data encryption organization [29].

www.iioab.org
THE IIOAB JOURNAL
www.iioab.webs.com

In this paper encryption algorithms have been proposed to make cloud data secure, defenseless (vulnerable) and offered worry to security issues, challenges furthermore algorithms have been made between AES, DES, and RSA calculations to locate the best one security algorithm, which must be utilized as a part of cloud computing for making cloud data secure and not to be hacked by attackers [30].

In proposed another patient-centric Personal Health Record framework, which would be packaged with a two stage validation instrument. The framework likewise utilizes a standout amongst the best encryption methods of AES encryption for securing the Personal Health Record (PHR) which are put away in the Third party semi-trusted cloud server and also proposed OTP authentication for using secure data in a cloud [31].

In presented the requirement for data integrity through Third Party Storing so as to inspect and the data heterogeneously over multiple servers or databases and thus provides gives additional security to cloud clients. Furthermore, utilize One Time Password for client authentication like the banking system. This distributed data split vertically when consolidated with encryption gives an additional layer of security and ensures clients information access and capacity storage in a simple and cost effective manner as well [32].

In proposed data security model gives client authentication and data assurance. This makes certain safe correspondence framework and concealing data from others. In this model message digest based document encryption framework and secure open key encryption framework utilizing RSA for trading data is incorporated. This model additionally incorporates one-time password (OTP) framework for client validation process [33].

EXISTING ALGORITHMS FOR SECURITY

To provide data security in cloud computing there are all the more existing methods. Which utilizes encryption and decoding strategies for well-being and security with client information on the cloud? Here we are utilizing symmetric and asymmetric encryption algorithms. The symmetric encryption method is having only one key that is used to encrypt and decrypt the data. Another method is asymmetric encryption that is having two key one is private key and another one public key. Private Key is used for decryption and public key is used for encryption. [34].

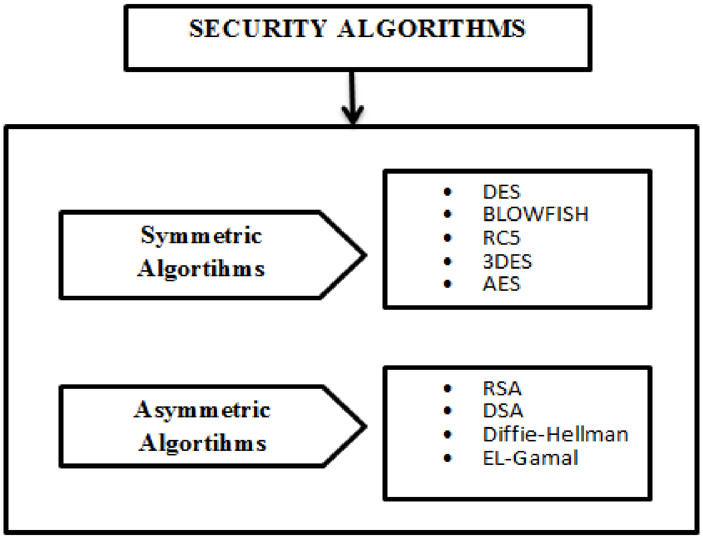

Fig: 3. Security Algorithms

COMPUTER SCIENCE

www.iioab.org

THE IIOAB JOURNAL

www.iioab.webs.com

SYMMETRIC TECHNIQUES

DES

DES stands for Data Encryption Standard established in 1977. It applies a 56-bit key to each 64-bit block of data. It was the first encryption standard to be approved by NIST. This Method can run in number of modes and requires 16 rounds or controls, even though this is designed with "strong" encryption. We have used DES algorithm with destruction-editing approach for providing data security with integrity [35]. Each round in the deals with uses a separate 48-bit round key which is produced from the consistent cipher key according to the DES techniques [10].The Data Encryption Standard (DES) is a formerly transcendent symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of present day cryptographic systems.DES is the block cipher an algorithm that takes a fixed length string of plaintext bits and changes into a series of muddled operations into another cipher-text series of bits with the same length. On account of DES, for the most part, the block size is 64 bits. DES additionally utilizes a key to altering the change, so that decryption must be performed by the individuals who know the specific key used to encrypt. At the present DES issued to be unconfident for multiple applications, and therefore it has been replaced by the Advanced Encryption Standard (AES)[36].

BLOWFISH

It is symmetric encryption algorithm. It have 64 bit block cipher developed by Bruce Schneider; enhanced for 32-bit mainframes with huge data stores, it is greatly faster than DES on a Power PC-class machine. Key lengths can differ from 32 to 448 bits in range. Also it's have 16 rounds. Blowfish, accessible easily and developed as an alternate for DES or IDEA which is in use in a large number of production [7].

RC5

It is symmetric encryption algorithm that deals with 128 bit block cipher based upon, and a development done, RC5. Also its have 12 rounds. The utilization of RC5 algorithm for encryption, cloud computing can be connected to the data transmission security.Transmission of data will be encrypted, regardless of the fact that the data is stolen, there is no relating key can't be restored[37].

3DES

In Triple DES (3DES) Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher encryption is discussed with the development ofthe Data Encryption Standard (DES) cipher techniques. TDES uses a block size of 64 bits and operate 48 processing round corresponding to DES. In 3DES three times iteration is produced to improve the encryption and security level [38]. It makes three encryption and decryption permits done the block using DES 56 bit keys [7].

AES

Advanced Encryption Standard (AES) uses a symmetric key encryption design known as called Rijnadael, a block cipher proposed by Belgian cryptographers Joan Daemen and Vincent Rijmen [7]. The key size can have variable lengths such as 128,192 or 256 bits. The default keysize is 256 bits. AES encryption standards are very fast, it is flexible and effective than DES. It has had total 14 rounds contingent on the key sizes which are used in [10]. It is one of the very regularly used and isavailable for utilizing the data secure purposes; the algorithm depends on a few substitutions, permutations and direct changes. It said that up until today, no functional assault against AES exists. In this manner, governments, banks and high-security frameworks around the globe are favored utilizing AES for the encryption standard. [14]. It is highly securable and more efficient algorithm and it secure all types of data that deals with medical information's but only thing need for more design area. Here AES algorithm is used that consists of 22 rounds it may minimize to 18 rounds which reduce time consuming and cost [13]. The use of AES encryption algorithm is highly securable with no loopholes and AES encryption and decryption is highly

www.iioab.org

THE IIOAB JOURNAL

www.iioab.webs.com

COMPUTER SCIENCE

secured and fastest method.AES is the main algorithm which is not inclined to any of the cryptanalysis assaults (attacks).[4].

ASYMMETRIC TECHNIQUES

RSA

Ronald Rivest Adi Shamir and Leonard Adlemandesigned the RSA algorithm 1977 cryptosystem uses the properties of the generative homomorphism encryption. RSA key size is having1024 bit. Then its have one rounds [10]. RSA is generally use public key techniques and RSA is accomplished to maintain encryption and digital signatures. RSA provides the best security plan by encrypting the data that is confidential; this is the motivation behind why the enormous administration suppliers like Google mail, Yahoo mail and so on are utilizing this algorithm to give their clients the protection of secrecy in utilizing their administrations.[14].RSA today is utilized as a part of a few programming items and it can be utilized for digital signatures, key exchange, or encryption of a little block of data. RSA uses a changeable size key and a variable size encryption block but RSA encrypts and decrypts data that consumes more time [7].

DSA

In presented an autonomous investigation of security algorithms in cloud computing. Which provides the particular technique to secure data on cloud computing.The DSA techniquegives digital signature possibilities for the authentication of messages [7] DSA (Digital Signature Algorithm) is a Federal data processing Standard for digital signatures. DSA was introduced by the NIST (National Institute of Standards and Technology) it is used to detect the unauthorized alterations to the data send by the source to the receiver [10].

Diffie-Hellman

Diffie-Hellman introduces secret-key exchange protocol only. It is not for authentication or digital signatures and it is public key exchange methods, it uses of the discrete logarithm problem. Actually the sender and receiver set the secret key [7]. These techniques protect the data confidentiality and safe and security, Diffie Hellman Key Exchange method tolink organization and Elliptic curve cryptography for data encryption [39].

El-Gamal

El-gamalalgorithm is also public key cryptographic techniques. The private key will be secret. It is not capable to expose the information. So encryption and decryption of message will gives more security for the data, ELGamal's cryptosystems have numerous helpful applications, with its strong properties. It is an exceptional sec. This is most certainly not restrictively difficult to encrypt the message in the cloud also [40].The bit operation of encryption or decryption in El-Gamal cryptosystem is polynomial used in the paper. The ElGamal algorithm is utilized as a part of this Paper for homomorphic encryption. The unique data is then acquired by the user with the cipher Keys. This must be reached out for a various number of clouds and with various operations. [41].

AUTHENTICATION TECHNIQUES

Authentication is an important part of an environment. The cloud is no exclusion. Actually, in some aspects, authentication is still more important in a public cloud environment than in a traditional environment. Authentication use primary techniques of exclusive of access of the applications and data. This paper discusses the three levels of authentication techniques. The paper discusses given below.

ONE TIME PASSWORD

In this paper we have proposed to create of factor one time password with two factor authentication as a powerful authentication method that is necessary mobile phone as an authentication device. In this technique mobile phones are in control to produce OTP which is valid only for 3 minutes [42]. This is oldest techniques but it also provides secure authentication. In order to secure the system, the produced OTP must be strong to find, recover, or trace by hackers. Therefore, it’s very important to develop a secure OTP generating algorithm. Users appear to be willing to utilize straight forward variables, such as their mobile number and a PIN for administrations, such as approving mobile micropayments [43]. One time password can be produced in any of the two ways, HMAC based One Time Passwords (HOTP) and Time based One Time Passwords (TOTP) The user creates a one-time password and submits it to the server. Server additionally creates a one-time password for that inhabitant for that instance of time and confirms it with the password received from a user[44].

DIGITAL SIGNATURE

The digital signature gives a dynamic solution to implement services that assure data protection and data integrity. RSA Digital Signature Scheme guarantees legitimacy and respectability of data [45]. The digital signature authentication method is better than all techniques. Digital signature is a method supports authenticity and integrity of information. Digital signature is public key cryptography. Digital signature is used with any kind of data whether data is encrypted or not [46]. Digitally signed messages may be everything that represents strong bit string: examples include electronic mail, contracts,or a message sent by any other cryptographic protocol. Digital signature is a mathematical structure for establishing the authenticity of digital information or document [47]. The reasonable digital signature provides a receiver cause to believe that the message was produced by an identified user, which was not chanced in transit. It is generally used for software distribution, financial transactions, and in other instance to detect the forgery which was important to use [48].In proposed another security design which executes RSA for both encryption and secure correspondence purposes though MD5 hashing is utilized for digital signature and hiding key data. This model gives security to the whole cloud computing environment.Both RSA encryption and Digital Signatures algorithms subsequently a capable security and information respectability administration framework is acquired [52].

BIOMETRIC AUTHENTICATION

This proposes a new approach based on biometric encryption for to increase the security of data sharing in public cloud. The biometric based authentication to make sure that the user is unauthorized person. For the authentication purpose we usethe physiological assessment as the encrypted image, here it is analysis graph of heartbeat [49].In this proposal thumbnail expression of user for Authentication is used. When register with the new user, it take the thumbnail expression of user using thumb recognition device and stored in image format in System Database. Whenever the user logs in, user should give the thumbnail expression using thumb detection device then system checks that image is same or not. If wrong then provide the error and if it is accurate then gives approval for other authentication scheme [50]. Generally traits used for biometric recognition are: faces, fingerprints, irises, palm-prints, speech etc. Designing biometric services in cloud highlight with result that has to be built with value to that mechanism of the biometric system that should be transferred to the cloud. Biometric is the authentication process which is used for the security purpose. In proposed system we are using biometrics like figure print and iris images are used. It also uses the minute matching algorithm to compare the images [51].

Here correlation of symmetric block cipher and unbalanced algorithm talked about, DES (Data encryption standard) algorithms have a key size of 56 bit key, it's called as private key type and block size 64 bit furthermore it's have 16 rounds. Blowfish is likewise symmetric algorithm its have 32 to 448-bit level, it has 16 round to handling and execution time is quick. At that point RC5 is a symmetric algorithm it has 0 to 2040 key sizes and square size 64 bit, it's similar to a private key type yet execution speed is low. 3DES key size is 32, 64 or 256 bit and block size 64, its have 48 rounds. AES (Advanced encryption standard algorithm) it is quick and secure technique and it have 128,192 or 256 pieces then the number rounds are 10, 12, and 14. It has quick execution speed too. In last RSA is have a 1024-bit level and square size is variation number of rounds is 1 and it's called as public key algorithm.

www.iioab.org
THE IIOAB JOURNAL
www.iioab.webs.com
COMPUTER SCIENCE

COMPARISON OF SYMMETRIC AND ASYMMETRIC ALGORITHMS [6][8][9][13]

Table: 1. Comparison of symmetric and asymmetric techniques

Algorithms	DES	Blowfish	RC5	3DES	AES	RSA
Key Size	56 (+8 parity bits)	32-448(default 128)	Max 2040	112,168	128,192 or 256	1024 to 4096
Block Size	64	64	32,64 or 256	64	128,192 or 256	Variant.
Number of Rounds	16	16	1-255(12 suggested)	48	10(128),12(192),14 (256)	1
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher
Key type	Private Key	Private Key	Private Key	Private Key	Private Key	Public Key
Speed	Very slow	Fast	Slow	Slow	Very fast	Slow

CONCLUSION AND FUTURE WORK

The paper concludes with an independent study of security algorithms and authentication methods in cloud computing such as symmetric, asymmetric and authentication techniques. The symmetric and asymmetric techniques such as DES, Blowfish, RC5, 3DES, AES,RSA, DES, Diffie-Hellman and El-Gamal and the authentication methods includes Onetime password, Digital Signature and Bio-metric. The study says that on comparison with many secured algorithms available till date, blowfish is faster than other encryption algorithms. Also the survey shows that the authentication method, an oldest method, restricts the user to access easily for incorrect password can be handled by digital signature and biometric methods.

The future work of the paper closes with a usage of information security and verification in cloud computing with respect to the AES and Blowfish algorithms. Both of them can be best compared.We are going to have correlation examination of AES and Blowfish strategy and then we will analyze and consider which one gives more security and we can enhance the blowfish systems.

FINANCIAL DISCLOSURE

No financial support was received to carry out this research.

ACKNOWLEDGEMENT

Authors would like to thank School of Computing Science and Engineering, VIT University for providing resources and support to carry out this research work.

CONFLICT OF INTERESTS

Authors declare no conflict of interest.

REFERENCES

[1] RamandeepKaurBhinder el al. [2015] A Review on Using Cryptography Techniques for Securing User Data in Cloud Computing Environment. *International Journal of Computer Science & Communication* (IJCSC),.6:83–86.

[2] NiteenSurv et al. Framework for Client Side AES Encryption Techniques in Cloud Computing. *International Advance Computing Conference (IACC)*, 525– 528.

[3] Periyanatchi S, Chitra.K. [2015] Analysis on Data Security in Cloud Computing-A Survey. *International Conference on Computing and Intelligence Systems* 04:1281 – 1284.

[4] LovepreetKaur et al. [2015] A Survey on the Encryption Algorithms in the Cloud Security Applications. International journal of Science Technology & Management (IJSTM), pp.1– 9.

[5] Neha A Puri et al. [2014] Deployment of Application on Cloud and Enhanced Data Security in Cloud Computing using ECC Algorithm. pp. 1667– 1671.

[6] Thiyagarajan B, Kamalakannan R. [2014] Data Integrity and Security in Cloud Environment Using AES Algorithm. Information communication and Embedded Systems. 1– 5.

www.iioab.org

THE IIOAB JOURNAL

www.iioab.webs.com

[7] CharanjeetKaur et al. [2015] Data Security Algorithms In Cloud Computing: A Review. *International Journal For Technological Research In Engineering* 2:372– 375.

[8] Sana Belguith et al. [2015] Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm. *The Eleventh International Conference On Autonomic and Systems*. 98– 103.

[9] Tembhurne S et al. [2015] An Improvement In Cloud Data Security That Uses Data Mining. *International Journal of Advanced Research in Computer Engineering & Technology* 4: 2044– 2049.

[10] Nikhitha K, Navin K S. [2015] A Survey On Various Encryption Techniques For Enhancing Data Security In Cloud. *International Journal of Advanced Research Trends in Engineering and Technology* 194– 197.

[11] Rashmi S et al. [2015] Architecture for Data Security In Multi-cloud Using AES-256 Encryption Algorithm. *International Journal on Recent and Innovation Trends in Computing and Communication* 157-161.

[12] Masthanamma V et al. [2015] An Efficient Data Security in Cloud Computing Using the RSA Encryption Process Algorithm. *International Journal of Innovation Research in Science, Engineering and Technology* 4: 1441– 1445.

[13] SaiSindhuTheja R et al. [2015] Data Security in Cloud for Medical Sciences using AES 512-bit Algorithm. *International Journal on Recent and Innovation Trends in Computing and Communication* 1746– 1749.

[14] Nasrin K, ZurinaMohd. [2014] A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services. *IEEE Conference on Systems, process and Control* pp. 58-62.

[15] Sugumaran M et al. [2014] An Architecture for Data Security in Cloud Computing. 2014 World Congress on Computing and Communication Technologies. pp. 252– 255.

[16] Arockiam L, Monikandan. [2014] Efficient Cloud Storage Confidentiality to Ensure Data Security. International Conference on Computing Communication and Information. 5:1– 5.

[17] Anuj Kumar et al. [2014] Cloud Data Security using Authentication and Encryption Technique. *International Journal of Innovative Research In Technology* 1: 388– 391.

[18] Vanya divan et al [2014] Cloud security solution: comparison among various cryptographic Algorithms. *International journal of advanced research in computer science and software Engineering* 4:1146– 1148.

[19] pradeep Kumar et al [2014] An authentication approach for data sharing in cloud environment for dynamic group. International conferences on issues and challenges in intelligent computing techniques(ICICT)9:262–267.

[20] Meenakshi et al. [2014] Data security analysis in cloud environment. *International journal of innovations & advancement in computer science* 2:14– 19.

[21] Aized Amin Soofi et al [2014] Encryption Techniques for cloud data confidentiality. International Journal of Grid Distribution computing. 7:11–20. .

[22] Vishwanth, S.Mahalle et al [2014] Enhanced the data security in cloud by implementing hybrid(RSA&AES)encryption algorithms. *International conference on automation and communication*. pp.146–149.

[23] Prashantrewagad et al. [2013] Use of digital signature with Diffie Hellman key Exchange and AES encryption algorithm to enhanced data security in cloud computing. *International conference on communication systems and network technologies*. 3:437-439.

[24] Ching-Nung yang, jia-bin lai. [2013] Protecting data privacy and security for cloud computing based on secret sharing. *International symposium on biometrics and security technologies* 7:259–266.

[25] ParsiKaplana ,sudha. [2012] Data security in cloud computing using RSA algorithm. *International journal of research in computer and communication technology*, vol.1.

[26] Rohit ,sunil [2012] A proposed secure framework for safe data transmission in private cloud. *International journal of recent technology and engineering*, vol.1

[27] Aleksandar et al. [2012] Data confidentiality using fragmentation in cloud computing. *International journal of networks and distributed system*, 1:85–90.

[28] Mohand M et al [2012] Enhanced data security model for cloud computing. International conference on Informatics and systems. vol.36, pp.cc-12.

[29] PachipalaYellamma et al. [2013] Data Security In Cloud Using RSA. 4'th International Conference on Computing Communication and Networking Technologies, pp. 1-6.

[30] Sonia sindhu. [2015] A survey of security algorithms in cloud computing. International journal of Advanced Research in Computer Engineering & Technology,.4(5):2368–2371.

[31] Ramesh K, Ramesh S. [2014] Implementing One time password based security mechanism for securing personal health records in cloud. International Conference on control, Instrumentation, Communication and computation technologies. pp. 968–972.

[32] Subbhiah S, Selva S [2015] Distributed data security for data prevention in cloud computing using One time password for user authentication. Journal of Environmental Science, *Computer Science and Engineering & Technology* 4:752–758.

[33] Priyanka Nema [2014] An Innovative Approach for dynamic Authentication in Public cloud: Using RSA, Improved OTP and MD5. *International Journal of Innovative Research in Computer and Communication Engineering*. 1(11):6697–6702.

[34] RandeepKaur, SupriyaKinger. [2014] Analysis of Security Algorithms in Cloud Computing. *International Journal of Application or Innovation in Engineering & Management* 3: 171–176

[35] SunithaSharma et al. [2013] Enhancing Data Security In Cloud Storage. *International Journal of Advanced Research in Computer and Communication Engineering* , 2: 2132–2134

[36] Vijendra et al. [2014] Data Storage Security in Cloud Environment with Encryption and Cryptographic Techniques. *International Journal of Application or Innovation in Engineering & Management*, 3: 209–213

[37] Jay Singh et al. [2012] Improving Stored Data Security In Cloud Using RC5 Algorithm. Nirma University International Conference on Engineering. pp. 1–5.

[38] DeepikaVerma, Karan Mahajan. [2014] To Enhance Data Security in Cloud Computing Using Combination of Encryption Algorithms, 2: 41–44.

[39] Honey Patel, JasminJha. [2012] Securing Data in Cloud Using Homomorphic Encryption. *International Journal of Science and Research*. 4, :1892–1895.

[40] Jayanthi M et al. [2014] Analysis on Secure Data Sharing using ELGamal's Cryptosystem in Cloud. *International Journal of Computer Science and Electronics Engineering*, 4:50–55.

[41] Raghul et al. [2015] Data Security in Federated Cloud Environment using Homomorphic Encryption Technique. *International Journal of Emerging Technology and Advanced Engineering*, 5:137–141.

THE IIOAB JOURNAL ISSN: 0976-3104

[42] Vishal Paranjape, VimmiPandey [2013] An Approach towards Security in Private Cloud Using OTP. *International Journal of Emerging Technology and Advanced Engineering* 3:.683–687.

[43] Abhishektripathy, TarunGoyal. [2014] Cloud Data Security Using Encrypted Digital Signature & 3D Framework. *International Academic of Science, Engineering and Technology* 3:114–121.

[44] ShikhaChoksi. [2014] Comparative Study on Authentication Schemes for Cloud Computing. *International Journal of Engineering Development and Research*, 2: 2785–2788.

[45] HanumanthaRao et al. [2013] Data Security in Cloud using Hybrid Encryption and Decryption. *International Journal of Advanced Research in Computer Science and Software Engineering*. 3: 494–497.

[46] Roshani et al. [2015] Data Security in Cloud through Confidentiality and Authentication. *International Journal for Scientific Research & Development* 3: 1735–1738.

[47] Dimpi Rani, Rajiv. [2014] Enhanced Data Security of Private Cloud Using Encryption Scheme with RBAC. *International Journal of Advanced Research in Computer and Communication Engineering* 3: 7330–7337.

[48] Pradeep et al. [2012] Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption. International Journal of Engineering Research & Technology. 1:1–8.

[49] Ranu S, Hasna. [2015] Biometric Based Approach for Data Sharing in Public Cloud. *International Journal of Advanced Research in Computer and Communication Engineering*. 4:95-97.

[50] SuchitaKolhe et al. [2015] Five-Level Authentication Security in Cloud Computing. *International Journal for Research in Emerging Science and Technology*, 2:116–118.

[51] Sasi E, Saranyapriyadharshini.[2015] Secured Biometric Authentication In Cloud Sharing System. *International Journal of Computer Science and Mobile Computing*, 4: 572–577.

[52] Sudhansu & Biswaranjan [2014] Enhanced data security in cloud computing using RSA encryption and MD5 Algorithm. International *Journal of Computer Science Trends and Technology* 2(2):60–64.

ABOUT AUTHORS

Ms. Tamilarasi R is a Research Scholar in School of Computing Science and Engineering, VIT University, Vellore. She graduated M.S c in Computer Science. She is doing research in Cloud Computing. She published two papers in reputed Journals. Her area of specialization is Cloud Computing.

***Dr. Prabu Sevugan** completed Bachelor of Engineering in Computer Science and Engineering from Sona College of Technology (Autonomous) and Master of Technology in Remote Sensing from College of Engineering Guindy, Anna University Chennai and one more Master of Technology in Information Technology at School of Computer Science and Engineering, Bharathidasan University Trichy. Did his Doctoral studies on Integration of GIS and Artificial Neural Networks to Map the Landslide Susceptibility from College of Engineering Guindy, Anna University, Chennai. He was a Post-Doctoral Fellow at GISE Advanced research lab, Department of Computer Science and Engineering, Indian Institute of Technology Bombay. He has more than 45 publications in national and international journals and conferences. He organized 3 International Conferences which includes one IEEE Conference as chair and also participated in many workshops and seminars. He is a member of many professional bodies and senior member of IACSIT, UACEE and IEEE. He is having more than ten years of experience in teaching and research. Currently I am working as a Division Chair for Parallel and Distributed Computing, School of Computing Science and Engineering, VIT University Vellore.*

***Swarnalatha Purushotham** is an Associate Professor, in the School of Computing Science and Engineering, VIT University, at Vellore, India. She pursued her Ph.D degree in Image Processing and Intelligent Systems. She has published more than 57 papers in International Journals/International Conference Proceedings/National Conferences. She is having 15+ years of teaching experiences. She is a senior member of IACSIT, CSI, ACM, IACSIT, IEEE (WIE), ACEEE.She is an Editorial board member/reviewer of reputed International/ National Journals and Conferences. Her current research interest includes Image Processing, Remote Sensing, Artificial Intelligence and Software Engineering.*

www.iioab.org THE IIOAB JOURNAL www.iioab.webs.com COMPUTER SCIENCE