JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

Analysis of Security Algorithms used to secure Cloud Environment

A. Ahadha Parveen[1*], **P.S.S Akilashri**[2]

[1]Dept. of Information Technology, Jamal Mohamed College, Trichy-620020, India
[2]Dept. of Computer Science, National College, Trichy-620001, India

[*]*Corresponding Author: ahadha.parveen@gmail.com*, Tel.: *+91-9500653967*

Available online at: www.ijcseonline.org

Abstract— Cloud computing is an environment that enables its users to store data in virtualized storage. Cloud provides different services to users; the prime aim of this service usage is to store data in the cloud. When the users store data in the cloud, security of the data is becoming the topmost challenge to be considered in the cloud environment. There are different approaches and techniques which are proposed to address the security of data in the cloud. This paper presents a study and review of different security algorithms that are used in the cloud to secure the cloud environment. The paper presents the comparison of security algorithms with respect to different parameters. Findings and observations obtained from the study of different security algorithms are discussed. Finally, the paper suggests some points to be considered at the time of developing security algorithms for the cloud environment.

Keywords— Cloud computing; security; security algorithms; cryptography techniques;

I. Introduction

Cloud is a highly equipped infrastructure constructed by very big IT enterprise with thousands of server and computer. Each servers and computers are interconnected through network. This infrastructure is called as cloud data centre. Cloud data centre provides virtualized services for Software, Platform and Infrastructure [1]. Cloud services are delivered to user in a virtualized manner. Users interact with virtual images of the cloud services. Hardware and underlying details of the cloud infrastructure is hidden to users.

Cloud is evaluated from the prevailing computing like grid, pervasive, utility and etc. It reduces pitfalls in existing computing and provides unlimited services of computing resources like server, processor, storage and etc. It helps all level of users with its diverse services. The main usage of cloud is to store data in the cloud by using any of its services. Users can store as much as they need in cloud. Cloud provider collects money from the users based on their service usage. Users will pay based on the services consumed from the cloud, like pay per use service. Cloud dominates the business field by its advance essential characteristics like self-service, network access, elasticity, scalability and metered service [2].

Cloud services are delivered to users, irrespective of places and devices used by the cloud service users. Cloud has more number of APIs to automate the cloud environment. These benefits of cloud usage attract the users to adopt cloud in their business for outsourcing and etc. Users are very much interested in cloud and its services but there is always a question which exists,how data are secured in cloud? How is the security guaranteed, that data is not accessed by unauthorised users?. There are many other question which raises from the user side regarding the security of the data stored in cloud.

Security is the top most challenge in the cloud to be addressed. Many researchers are concentrating on their research to address the security in cloud. Security to be addressed in different level of cloud environment, data security in cloud is vital challenge to cloud users and providers. Data security is consideredasdata protection, whether it is in travel or in rest. Cryptography techniques are used to protect the data using the parameter Confidentiality, Integrity and Authentication (CIA). Each of this parameter is used to address security in different levels of data access in cloud environment [3]. It is necessary to have concrete infrastructure to avoid security related issues in cloud environment.

This research work makes a review on different security algorithm used in cloud for addressing the security issues. Comparison of security algorithms with respect to different parameters is presented in the paper. The paper also suggests some key points to be considered when developing security algorithm.

II. Related Work

In this section, different security algorithms proposed by researchers are reviewed and discussed. George et al., [4] proposed an enhanced RSA (ERSA) algorithm to reduce time taken for encryption and decryption by dividing file into blocks and enhance the strength of the algorithm by increasing the key size. The proposed algorithm uses two additional prime numbers which helps to improve speed and security. RSA algorithm uses two random numbers for key generation process.The results of the algorithms express the stable performance.

Prakash et al., [5] proposed an enhanced Hill cipher algorithm to solve the security issues in both cloud providers and consumers. Algorithm uses modulo37 and 26n2 matrices of dimension n × n. Additionally, it seems to be prudent to avoid too many zeroes in the key matrix. The net effect is that the effective key space of a basic Hill cipher is about 114 bits. Each alphabet and number is replaced by natural numbers 1to 36(26 alphabets +10 numerals (0-9)). Different file size ranges from 100 K byte to 1000 K Byte. The performance metrics are encryption time, CPU process time, and CPU clock cycles and battery power. All the plain text is decrypted using inverse matrix as a key. Therefore, it provides security from the unauthorized entities and susceptible. The proposed new algorithm is extending characters up to 37 letters. Most of the algorithms are working based on the 26 alphabets, especially Hill Cipher or Linear Block Cipher.

Priya et al., [6] discussed the file distribution and SHA-1 technique. When a file is distributed then data is also segregated into many servers. It is necessary in data security that every block of file contains its own hash code, using hash code which will enhance user authentication process; only authorized person can access the data. The data is encrypted using advanced encryption standard, so data is successfully and securely stored in cloud. Third party auditor is used for public auditing for handling of some security issues. Fast error localization, data integrity and data security provides users to audit the data with lightweight communication and computation cost. The proposed approach has used four algorithms ensures data storage security in cloud, SHA-1 and AES algorithm is a standard algorithm, Correctness verification, Error localization Algorithm, Error Recovery Algorithms. The proposed scheme is highly efficient for server colluding attack and malicious data modification attack with minimum computation overhead.

Samrat et al., [7] proposed an advanced two-step security mechanism of cloud computing.RSA is used to provide initial protection of the first level. RSA approaches message as input to the hash function and generated hash values is encrypted by using generated sender key. And the receiver will generate a hash code and decrypts the message using the sender’s public key.The Genetic algorithms (GA) are generalized search algorithms based on the mechanics of natural genetics. GA maintains a population of individuals that represent the candidate solutions. After successful completion of Genesis, mutation and crossover GA will provide a framework to match the desired pattern. Moreover, a media access control address (MAC address) of a device is a distinctive identifier assigned to network interfaces for communications at the data link layer of a network segment. The MAC address is used to generate the 3D Quick response code for user verification. Through experiments the combination of GA and 3D QR Code approach with RSA for two-step security mechanism archives strong potential to increase the security of Cloud Computing.

Prabu et al., [8] proposed a novel identity based hybrid encryption (RSA with Elliptical Curve Cryptography (ECC)) to enhance the security of outsourced data. The sender encrypts the sensitive data using hybrid algorithm then the proxy re encryption is used to encrypt the keyword and identity in standardize toward enrichment security of data.The techniqueis to use an identity based encryption (IBE) to cover the output of public key encryption. This is achieved by hybrid encryption and proxy re encryption techniques. Thesender encrypts their data using the hybrid algorithm with receiver identity (IDi) which is added to the encryption of receiver identity and the keyword for generating the resulting Ciphertext. Proxy Re Encryption (PRE) is applied to the identity of receiver and the keyword. The secret and top secret are the tags used as keywords. Theuser sends a message M with keyword K to receiver, the data has to send to the server E(IDa,M)||PRE(IDa,K). To decrypt the ciphertext at any time, through using the decryption key according to its identity this is provided by the PKG.

Somani et al., [9] proposed a scheme to encrypting the data while transferring it over the network. A digital signatureor digital signature schemethe authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit.The digital signature with RSA algorithm scheme is used to ensure the security of data in cloud. RSA is the most recognizable asymmetric algorithm, it is the only asymmetric (i.e. needs two different keys) algorithm used for private/public key generation and encryption. This method uses both digital signature scheme and public key cryptography to enhance the security.

Suganya et al., [10] proposed a technique for continuous auditing method which helped the verifier to perform block level and file level checking to ensure the process. The objective of this work is to provide the secure cloud service. The already existing problem is that attackers can hack the information sometimes from cloud even though the data integrity checking protocol is installed, and they didn’t maintain auditing technique as well. To avoid these issues, an unused successive cloud auditing technique is proposed and it provides uninterrupted certificates to the user and as well audits the data which is verified with help of fresh data integrity checking protocol. The data integrity technique will address the issues if attacker corrupts the data in Multi-Cloud.The data integrity by the continuous auditing algorithm based on MD5 (DICAA) technique provides more confidentiality to cloud service. As in cloud storage, clients are maintaining a huge amount of data files.

Jay singh et al., [11] proposed a method using RC5 algorithm to secure stored data in cloud. The user has no supreme control over the software applications including secret data. User has to depend on the provider's action, maintenance and administrate it. The user does not have direct access to the software, to fix the problems when something goes wrong in any application and its valuable data.The efficient computing by centralized storage, memory, processing and bandwidth using RC5 Encryption Algorithm is used to store data in cloud. Resulted encrypted method is secure and easy to use. It fulfils the needs of cloud users and providers.

Arokiamet al., [12] proposed a technique that uses encryption and obfuscation as two different techniques to protect the data in the cloud storage. Encryption is the process of converting the readable text into unreadable form using an algorithm and a key. Obfuscation is same like encryption. Obfuscation is a process which disguises illegal users by implementing a particular mathematical function or using programming techniques. Based on the type of data, encryption and obfuscation can be applied. Encryption can be applied to alphabets and alphanumeric type of data and obfuscation can be applied to a numeric type of data. Applying encryption and obfuscation techniques on the cloud data has provided more protection against unauthorized usage. Confidentiality could be achieved with a combination of encryption and obfuscation.

Akanksha et al., [13] proposed a technique to secure data in the cloud storage in an efficient way which requires less CPU Power and Processing time. Using Electronic Curve Cryptography (ECC) algorithm for security purpose and for integrityto encrypt Meta data using certain algorithm for enhancing the security and confidentiality of data.The system decreasesthe amount of work to the customer and provides security, integrity and authentication. As the data is not physically obtainable to the user the cloud should deliver the user a method to check for integrity. This method providedevidenceto integrity of data in the cloud, which the client employs to check the accuracy of user data in the cloud.

Prashant et al., [14] proposed a mechanism to make use of a combination of authentication technique and key exchange algorithm blended with an encryption algorithm. This combination is referred to as "Three-way mechanism" because it ensures all the three protection scheme of authentication, data security and verification, at the same time.The mechanism have proposed to make use ofdigitalsignature and Diffie Hellman key exchange blended with(AES) Advanced EncryptionStandard encryption algorithm toprotect confidentiality of data stored in cloud. Even if thekeyin transmission is hacked, the facility of Diffie Hellman keyexchange renders it useless,since key in transit is of no usewithout user's private key, which is confined only to thelegitimate user. The scheme firstly Diffie Hellman algorithm is used to generate keys for key exchange step. Then digital signature is used for authentication, thereafter AES encryption algorithm is used to encrypt or decrypt user's data file. All this is implemented to provide trusted computing environment in order to avoid data modification at the server end.

III. COMPARISON OF ALGORITHMS REVIEW IN LITERATURE

Security algorithms reviewed in previous section are compared based on certain parameters. Table 1 shows the comparison of the security algorithm.

Table 1. Comparison of Security Algorithm

S.No	year	Proposed Algorithm	Symmetric or Asymmetric	Key Size and Rounds	Security considerations	Result	Comparison with Related Algorithm	Outcome
1.	2017 IEEE	Enhanced RSA Algorithm with varying Key	Asymmetric	Block Size= (2 *Key Size) -1	Encrypting their own sensitive data before sending it to cloud for storage. In addition, two more prime numbers, namely, PR1 and PR2 are included in the proposed algorithm	High Speed and Secure RSA algorithms in encryption speed and decryption time.	RSA algorithm uses two prime numbers.	Confidentiality Strengthen security

					ERSA.			
2.	2015 IEEE	Enhanced Security for Cloud Storage using Linear Block Cipher Algorithm Or (new modified hill cipher symmetric key algorithm)	Symmetric	Supports key sizes of 128, 192 and 256 bits. Proposed algorithm is26^{n2} matrices of dimension n × n.	Securing cloud data storage by using modulo 37, but existing hill cipher working with modulo 26.	Increase the security bandwidth 37 instead of existing 26	Each alphabet and number is replaced by natural numbers 1to 36(26 alphabets +10 numerals (0-9))	Security from the unauthorized entities. Avoid too many zeroes in the key matrix. Reduce diffusion. Power consumption.
3.	2015 IEEE	Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm.	Symmetric	128 bit key size for encryption.	Ensures data storage security in cloud.	Minimum computation time.	Four algorithms. SHA-1 and AES. Correctness verification and Error localization Algorithm. Error Recovery Algorithms. User defined algorithm.	Achieved data assurance in cloud storage. Guarantee of identification of misbehaving server. Malicious data modification attack with minimum computation. Secure and highly efficient.
4.	2017 IEEE	Enhancing the Security of Cloud Computing: Genetic Algorithm and QR Code Approach	Asymmetric	values are encrypted and decrypted with $C=M^E$ mod N	Amplifying the security of cloud computing**.**	Enhance the security of cloud with the combination of Genetic Algorithm and QR Code. Proposed a two-layer security mechanism which consists of Genetic Algorithm for Face Recognition and Quick Response (QR) technique for verification purpose.	Encryption method RSA, Genetic Algorithm (GA), and 3D Quick Response (QR) code using MAC address.	Not yet good enough to be adopted in any commercial product for cloud computing devices
5.	2016 IEEE	Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud	Asymmetric	E(IDa,M)|| PRE(IDa,K)	Achieved by authenticated client for their backup, Data storage and sharing.	RSA with ECC to enhance the security of outsourced data. Sender encrypts the sensitive data using hybrid algorithm. The proxy re encryption (PRE) is used to encrypt the keyword and identity security of data.	identity-based hybrid encryption method (RSA with Elliptical Curve Cryptography (ECC)	Ensures the security of user data. Less computation time.
6.	2010 IEEE	Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing	Asymmetric Encrypting the data while transferring it over the network.	Proposed a concept of digital signature with RSA algorithm. Hash value is referred as message st.	Protect data in transit Cloud Storage Data Security	Try to achieve the security of data when it is transferred	Digital signature with RSA algorithm	Authenticity of a digital message or document.
7.	2017 IEEE	Improving Cloud Security by Enhancing Remote Data Integrity Checking	Symmetric Stored data	Less time to compute. File sizes are in MB and Time in millisecond	Secure cloud service and this process to be efficient in all cases.	More security to the cloud service provider and heavy confidential against cloud auditing.	data integrity by the continuous auditing algorithm based on MD5 (DICAA)	cloud auditing data integrity confidentiality

		Algorithm		(ms)				
8.		Improving Stored Data Security In Cloud Using Rc5 Algorithm	Asymmetric Applied to the data transmission.	Manjra soft Aneka 2.0 Cloud Environment	Applied to the data transmission. Data encrypted, Even if the data is stolen.	Secure and easy to use of cloud users and providers.	RC5 Encryption Algorithm.	Data is stored only on trusted storage servers. Cannot be accessed by administrators or intruders.
9.	2014 IEEE	Integration of Encryption and obfuscation to protect data in cloud	metric at Rest	its	Confidentiality	Compared to existing algorithm, it produce better result in performance and security	Result is compared with DES, 3DES and Blow fish	Time and Security is considered for analysing result of the proposed algorithm
10.	2017 IEEE	Providing Security, Integrity and Authentication Using ECC Algorithm in cloud storage	Stored Data	256-bit ECC public key provides differentiate security to a 3072- bit RSA public key.	Security integrity and authentication. Confidentiality, Integrity, and Availability	Security with lower computing power and battery resource usage, it is becoming widely used for mobile application.	Electronic Curve Cryptography (ECC) algorithm. Providing Security using ECC as compared to RSA	Less CPU power and execution time.
11.	2013 IEEE	Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing	Protecting Data stored in cloud.	Key Exchange –Diffie Hellman Digital Signature – SHA-I Uploading / Downloading Data Encryption-AES Data is stored / retrieved from Storage server	Combination of authentication technique and key exchange algorithm blended with an encryption algorithm.	Three ways protection scheme. Diffie Hellman algorithm is used to generate keys for key exchange step. Digital signature is used for authentication, AES encryption algorithm is used to encrypt or decrypt user's data file.	Achieved Authentication Data security Verification Confidentiality	Three way Mechanism makes it tough for hackers to crack the security system, thereby protecting data stored in cloud.

IV. FINDING AND OBSERVATION

From the review of different security algorithms, it is found that, it is highly challenging to secure the data in the cloud computing environment from unauthorized access. Many authors have proposed different solutions for securing the data or file in cloud. But, there is no practical implementation proof for this entire proposal. It is observed that some of the proposals are trying to enhance the existing algorithm or they have tried to integrate two or more existing algorithms. Just integrating two or more algorithms will not provide an efficient result for the security issues in cloud.
Generally, in a cloud environment, to secure the data stored in cloud, only symmetric algorithms [15]has thepossibility to secure the data at rest. Asymmetric algorithms are not suitable for securing the data at rest. Because, due to its processing time, it takes more time to process small amount of data.

It is also observed that, security is not considered as parameter to prove the security of an algorithm. Security of algorithm is measured by the security level of the algorithm. Many authors have considered time as a main parameter for their algorithm to compare with existing algorithms. Time is one of the parametersthat might be considered as an additional measurement for a security algorithm but security level should be analysed to prove the security of the algorithm.

V. SUGGESTIONS TO IMPROVE SECURITY

Security is a major issue in cloud. It is also difficult to address the various security issues in cloud. There are different areas in cloud where security needs to be addressed like data level, infrastructure level, virtualization security and etc.Security dominates every area of the cloud environment.
Securing the data stored in the cloud is mainly discussed in all literatures. Following points are some suggestions to be considered when addressing to the security of cloud data.

- Data is in different forms like data in motion and data at rest; columnist should decide that whether they going to address the security of data at rest or in motion.
- Definein which cloud deployment model, the security needs to be addressed.
- Data is attacked by insider or outsider. Data is secured by using cryptography techniques. Cryptography techniques are generally categorised into two types, they are, symmetric and asymmetric encryption.
- Encrypt the data in cloud that may help to protect data from outsider attacks.

- Data inside the cloud may be disclosed by the cloud administrator, this is called insider attack. To Protect data from insider attack, data must be encrypted before it is transferred to cloud environment.
- While proposing an encryption algorithm, it must be compared with the existing algorithm with respect to security level.

.

VI. CONCLUSION

Cloud data centres provide computing resources as a service to users in the form of software, platform and infrastructure. Users are often fascinated by the cloud capabilities and they keep migrating to cloud. The important area in cloud that needs more attention is security. Security is the most important challenge in any cloud computing environment. There are number of research works which are carried out to solve this hurdle, but still then the problemdoespersist. This paper has reviewed some security algorithms used in cloud and compares it with certain parameters. Each algorithm has specific nature of procedure and tries to protect the cloud environment. All algorithms have considered only the relational data but it should be extended to consider the other type of data like video, audio and images. Having a concrete framework or architecture for securing cloud environment is a predominant necessity in the IT field. It is an open research area to be addressed in the near future.

REFERENCES

[1] Arockiam, L., Monikandan, S. and Parthasarathy, G., Cloud computing: a survey. Int. J. Internet Comput, 1(2), pp.26-33, 2011.

[2] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", Technical Report-800-145, Version 15, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2011.

[3] Dr. L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, pp 3064-3070., 2013.

[4] Dr. D.I. George Amalarethinam, H. M. Leena, "Enhanced RSA Algorithm with varying Key Sizes for Data security in Cloud", World congress on Computing and communication Technologies (WCCCT), 978-1-5090, DOI 10.1109,pp.172-175, 2017 IEEE.

[5] Prakash Kuppuswamy, Dr. S. Nithyarekha" Enhanced Security for Cloud Storage using Linear Block Cipher Algorithm", 978-1-4673-6618,-2015 IEEE.

[6] NiveditaShimbre, Prof.Priya Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm", International Conference on Computing Communication Control Automation, 978-1-4799-6892-3, DOI 10.1109, pp.35-39, 2015 IEEE.

[7] Samrat Kumar Dey, Md.Raihan Uddin, Kh.MohaimenulKabir, Md. Mahbubur Rahman, "Enhancing the Security of Cloud Computing: Genetic Algorithm and QR Code Approach", 4th International Conference on Advance in Electrical Engineering 28-30 September, 978-1-5386-0869-2,pp.181-186, 2017 IEEE.

[8] G.Prabukanna, V.Vasudevan "Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud" ,International Conference on Electrical, Electronics, and Optimization Techniques(ICEEOT),978-1-4673-9939-5,pp.3688-3693,2016 IEEE.

[9] Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", International Conference on Parallel, Distributed and Grid Computing(PDGC),978-1-4244-7674,pp.211-216, 2010 IEEE.

[10] S. Suganya, P.M Durai Raj Vincent "Improving Cloud Security by Enhancing Remote Data Integrity Checking Algorithm" , International Conference on Innovation in Power and Advance Technologies[i-PACT],978-1-5090-5682,pp.1-6, 2017 IEEE.

[11] Jay Singh, Brajesh Kumar, Asha Kharti, "Improving Stored Data Security in Cloud Using Rc5 Algorithm", 2017 IEEE.

[12] Arockiam, L., and S. Monikandan. "Efficient cloud storage confidentiality to ensure data security." In Computer Communication and Informatics (ICCCI), 2014 International Conference on, pp. 1-5. 2014, IEEE.

[13] Akanksha Bansal, Arun Agrawal, "Providing Security, Integrity and Authentication Using ECC Algorithm in cloud storage", International Conference on Computer Communication and Informatics (ICCCI), Jan 05-07, 978-1-4673-8855, 2017 IEEE.

[14] Mr.PrashantRewagad, Ms.YogitaPawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", International Conference on Communication System and Network Technologies, 978-0-7695-4958, DOI 10.1109, pp.437-439, 2016-IEEE.

[15] Tim Mather, Subra Kumaraswamy, and Shahed Latif, "Cloud Security and Privacy", O'Reilly Media, Inc., chapter 4, September, pp. 61-71, 2009.