International Journal of Recent Trends in Engineering & Research

ISSN (ONLINE) : 2455 – 1457 IMPACT FACTOR : 4.101

An Overview of Security Algorithms in Cloud Computing

Karthija.T[1], Dr.A.S.Radhamani[2], V.G.Anisha Gnana Vincy[3], L.Amutha Swaminathan[4]
[1,2,3,4] CSE, VV College of Engineering, India

Abstract *:* Cloud Computing is an emerging technology in computer oriented services. Cloud computing is becoming more well-liked and is ever growing due to fast development in the field of "cloud computing ". It increases serious security concerns in the large organizations as they share valuable resources in a cost effective way. Due to increasing demand for more clouds and data are stored in an open environment several security issues like confidentiality, integrity and authentication may arise. To keep user data highly confidentially against un-trusted servers and from malicious attacks some security measures should be taken. Encryption is the one of the most secured way to prevent unauthorized access. This paper depicts various algorithms that ensure security in the cloud environment.

Keywords - Cloud Computing, Multi-Authority CP-ABE, RSA, Message Digest

I. INTRODUCTION

COMPUTING is being transformed to a model consisting of services that are commoditized and supplied to the end-users in a similar way how basic needs like water, electricity, gas, and telephony do[7]. Cloud computing is a computing model, in which a large pool of systems are connected in private or public networks, to provide enterprisingly scalable infrastructure for application, data and file storage. With invent of this technology, the cost of computation, application hosting, data storage and delivery is reduced significantly. If a computing system is secure, then we can trust both hardware and software of that system [3].

The National Institute of Standards and Technology specifies five essential characteristics of cloud [12].
On-demand self-service: On-demand self service refers to the service provided by cloud providers that enables the user to pay according to the usage of the cloud services.

Broad network access: Broad network access is a combination of private clouds that operate within a company's firewall, public clouds that are accessed by public users, or a hybrid deployment. It can be accessed by heterogeneous devices like mobile phones, tablets, laptops, and workstations.

Resource pooling: Resources like storage, processing, memory, and network bandwidth are pooled to serve multiple users using a multi-tenant model. This model consists of different physical and virtual resources dynamically allocated and reallocated according to the consumer demand.

Rapid elasticity: Cloud is flexible to add any number of resources at any location with different configuration and any devices can be isolated from the cloud. Cloud is scalable outwards and inwards according to the requirement of the customers and is deployed by the service providers.

Measured service: Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. Cloud systems are automatically controled and resource usage is optimized by leveraging a metering capability at some level of abstraction appropriate to the type of services like storage, processing, bandwidth, and active user accounts.

Huge amount of data can be stored in the cloud. Those data can be hacked by any hackers (unauthorized user). To avoid hacking the data should be well secured. In order to secure the data many cryptographic algorithms are available. In this paper we have described three algorithms in brief.

This paper is organized in the following sections. Section II deals with literature survey and the cryptographic algorithms are described in section III followed by performance analysis and conclusion in section IV and V respectively.

II. LITERATURE SURVEY

In [1], the authors explained how the resources are allocated to the users in a cost efficient manner. This research proposed a new Agent based Automated Service Composition(A2SC) algorithm. This algorithm is is not only responsible for searching comprehensive services but also considers reducing the cost of virtual machines which are consumed by on-demand services only. The components of this algorithm are of request processing unit and automated service composition phases.

In [2], the problem of data-integrity verification for the client's data residing on a Cloud Storage Server (CSS) was described. The authors proposed a modified Chameleon Authentication Tree to perform effective block-level and fine-grained dynamic-data update operations on the data stored on cloud.

In paper [3] the authors applied RSA algorithm and Fermat's theorem together to build a new trusted cloud computing environment. By using Fermat's theorem the speed of RSA Encryption can be increased.

Gunasekaran Manogaran, et.al., proposed MetaCloudDataStorage Architecture for protecting Big Data in Cloud Computing Environment. This framework ensures efficient processing of big data in cloud computing environment and gains more business insights [5].

Author Nabeel Khan and Adil Al-Yasiri identified 18 numbers of threats in cloud computing environment [6].

Victor Chang, et.al., presented a Cloud Computing Adoption Framework (CCAF) security algorithm to develop and integate three technologies like encryption, firewall and identity management based on the development of enterprise file sync and share technologies [10].

Yuh-Min Tseng, et.al,. proposed a new revocable Identity-Based Encryption (IBE) scheme with a Cloud Revocation Authority (CRA) to solve the two shortcomings, the performance is improved significantly and the CRA holds only a system secret for all the users [11].

III. SECURITY ALGORITHMS

The data present in the cloud should be fully secured. Only the authenticated users should be able to access the data. The data should be secured from the outside world. In order to provide security to the data many security algorithms should be implemented. The selected security algorithm should be an efficient one in terms of performance, confidentiality and cost.

The cryptographic algorithms provide security by converting the plain text to cipher text and then store the cipher text to the cloud. Only an authenticated user can access the data in the cloud and convert the cipher text to plain text and use the same. This paper explains some of the cryptographic algorithm how they encrypt the plain text to cipher text and how the decryption is carried out at the user side. In order to analyze the performance of the algorithms parameters such as block size, key size and application area are considered.

MULTI-AUTHORITY Ciphertext-Policy-Attribute Based Encryption (CP-ABE):

In Attribute-Based Access Control only one system is responsible for the production and distribution of public keys and private keys respectively. In this type all the burden of creating and sending the different keys lies on a single system. This may cause some delay in transmitting the keys to different users. In order to reduce the load to the single system multi-authority CP-ABE was introduced. A party can act as an authority by creating public key and distributing the private keys to different users that reflect their attributes.

In multi-authority CP-ABE system for cloud computing consists of five types of entities: the Certificate Authority (CA), the Attribute Authorities (AAs), the data owners (owners), the data consumers (users) and the cloud server. The figure1 illustrates the model of multi authority system and depicts the communication between different entities like cloud service provider, AA, user, data owner and CA.

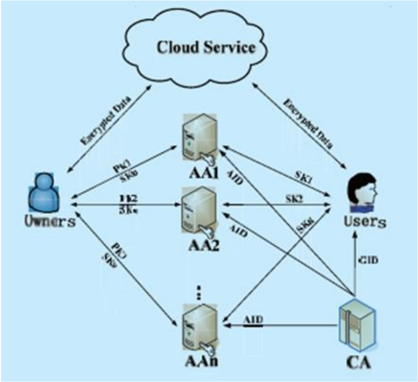


Figure 1:- Multi-Authority CP-ABE

Certificate authority is a trusted authority in the system. It accepts the registration of all the legal users and AAs in the system. The owner authority generates the secret key. The attribute authority with the owner's secret key and the attribute set generates the master key and public key.

Each attribute authority manages a different set of attributes. Different authorities can function entirely autonomously, and there is no requirement for any global coordination during the initialization phase. Failure of AA will not affect the security of the system and the rest AAs. The concept of global identity is used to link attribute-related private keys together that are issued to the same user by different authorities, which in turn achieves collusion resistant among any number of users.

Each owner holds its secret key and transmits it to the AAs. The attribute authorities use their own master keys and the owner's secret key to generate the public key and the user's private key. The owner defines an access structure and encrypts the data under this access structure by using the current public key. When the user's attribute revocation happens, which means a value of the attribute will not belong to the user, the corresponding authority needs to change the master key of the attribute value and generate the new public key of the attribute value and also the update key for the other users who still hold the attribute value. The owner can encrypt the new data by the new public key. All the users except the revoked one can efficiently update their private keys via the update key. Then, the owner sends a part of the cipher text to the corresponding attribute authority. The authority generates the update key for cipher text by using the new master key and the part of the cipher text and sends the update key to the cloud server for cipher text re-encryption. Then, the cloud server can re-encrypt the cipher text affected by the revoked attribute by using the proxy encryption method, so any new user who has sufficient attributes and the users who have not revoked the attribute value can still decrypt the newest cipher text by the new or updated private key. However, the revoked user cannot get the update key to update his private key, so he cannot decrypt the cipher text which is encrypted by the new public key or the updated cipher text.

RSA ALGORITHM:

RSA is a Public Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first described it in 1977. RSA is an algorithm that provides security by encrypting and decrypting the data, so that only authorized user can access the data. The data is encrypted and the cipher text is then stored onto the cloud. When an user is in need of the data, the user places a request to the cloud provider, then the provider authorizes the user and provides him the data.

Third-Party can detect Cloud service provider misbehavior with a certain probability by asking proof for a constant amount of blocks that are independent of the total number of file blocks [4]. Every message block is mapped to an integer value. RSA algorithm consists of Public Key and Private Key. Public Key is known to all cloud users, whereas Private-Key is known only to the user who originally owns the data. Encryption is performed by the Cloud service provider and decryption is performed by the Cloud user/cloud customer. Once the data is encrypted with the Public Key, it can be decrypted with the corresponding Private Key. Figure 2 outlines the working of RSA algorithm.

RSA algorithm involves three steps:
1. Key Generation
2. Encryption
3. Decryption

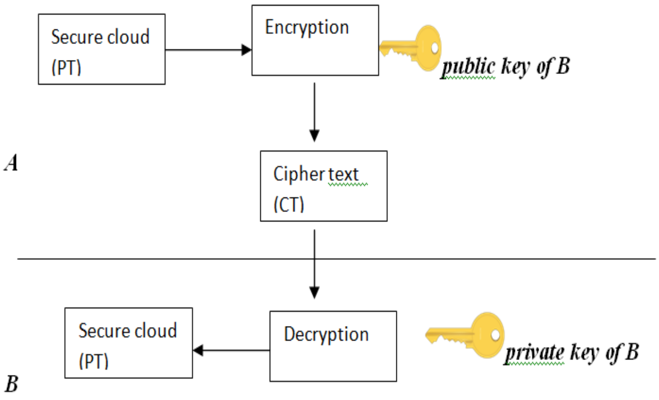


Figure 2 :- working of RSA

Key Generation:
Key is generated by the cloud service provider and the user
Steps:
1. Choose two distinct prime numbers x and y. For security purposes, the integers x and y should be chosen at random and should be of same bit length.
2. Compute n = x * y.
3. Compute Euler’s totient function, Ø(n) = (x-1) * (y-1).

4. Chose an integer PU, such that 1 < PU < Ø(n) and greatest common divisor of PU , Ø(n) is 1. Now PU is released as Public-Key exponent.
5. Now determine PR as follows: PR = PU-1(mod Ø(n)) i.e., PR is multiplicate inverse of PU mod Ø(n).
6. PR is kept as Private-Key component, so that PR * PU = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent PU i.e, (PU, n).
8. The Private-Key is a combination of modulus n and the private exponent PR, which must be kept secret i.e, (PR, n).

Encryption:
The process of converting original plain text to cipher text is called as encryption.
Steps:

1. Cloud service provider should transmit the Public Key (n, PU) to the user who wants to store the data with him or her.
2. User data is now mapped to an integer using an agreed upon reversible protocol,named as padding scheme.
3. Data is encrypted using the calculation CT = PTPU (mod n)
4. This cipher text is now stored in the Cloud storage.

Decryption:
The process of converting the cipher text to the original plain text is known as decryption.
Steps:

1. The cloud user requests the CSP for the data.
2. CSP verify's the authenticity of the user and gives the encrypted data (CT).
3. The Cloud user then decrypts the data by computing, PT = CT PR (mod n).
4. Once PT is obtained, the user can get back the original data by reversing the padding scheme.

MESSAGE DIGEST ALGORITHM:
Message Digest Algorithm (MDA) uses public key encryption, symmetric encryption and standard hashing algorithm in the registration process, authentication process and generating the message digests respectively. As MDA does not have any specification for algorithms, any standard combinations of encryption algorithms and hashing algorithms could be used in the operations of MDA [8].

Message digest function, also known as hash function is used to generate Digital Signature of the information. The digital signature produced by the hash function is known as message digest. MD5 algorithm is used to implement integrity of the message and it produces message digest of size 128 bits. There are mathematical functions that process data to produce different message digest for each different message. Message digest algorithm has two advantages. The first advantage is that identical messages always generate the same message digest and even if any changes occur in the message bit, it produce different message digest for that message. The second advantage is that message digests are much shorter than the document from which message digests are generated. It processes the message and generates 128 bits message digest. Figure 3 traces the working of MDA. The algorithm contains the following steps:

1. Appending the padding bits
2. Appending the length
3. Initializing a MD buffer
4. Processing message in 512 bit blocks
5. Generating output

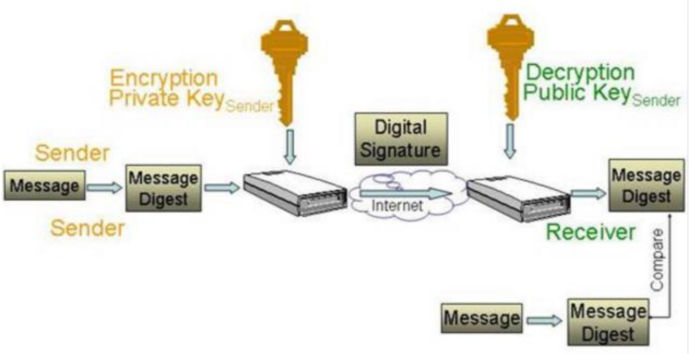


Figure 3:- Working of Message digest

The algorithm consists of 5 functions:
1. Key Generation
2. Digital Signing
3. Encryption
4. Decryption
5. Signature Verification

1) Key Generation:
Randomly generate two large prime numbers: a and b.
Compute $n=a * b$
Compute the totient: $\Phi(n)= (a-1) * (b-1)$
Choose an integer ‘c’ such that $1< c < \Phi(n)$ and $\gcd(c, \Phi(n)) = 1$
Compute d, such that $d * c = 1 \bmod \Phi(n)$
The public key is (n, c) and the private key is (n, d).

2) Digital Signing:
Message digest of the document to be send is generated.
The digest is represented as an integer msg.
Digital Signature DS is generated using the private key(n, d), DS= msgd mod n.
Sender sends this signature DS to the recipient.

3) Encryption:
Sender exemplifies the plain text message as a positive integer value msg.
It converts the message into encrypted form using the receiver’s public key (c, n).
CT= msgc mod n
Sender sends this encrypted message to the recipient B.

4) Decryption:
Recipient B does the following operation:
Using his private key (n, d), it converts the cipher text to plain text ‘msg’.
msg= CTd mod n

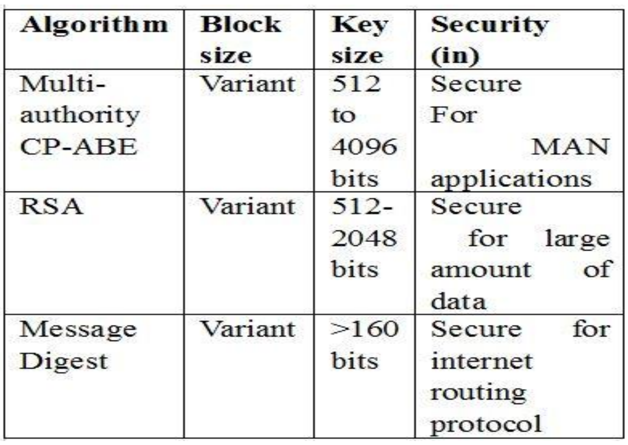
5) Signature Verification:
Receiver B does the followings to verify the signature:
An integer V is generated using the senders public key (n, c) and signature DS
V= DSc mod n
It extracts the message digest M1, from the integer V using the same MD5 algorithm.
It then computes the message digest M2 from the signature DS.
If both the message digests are identical i.e. value (M1)= value(M2), then signature is valid

IV. PERFORMANCE ANALYSIS

The Multi-authority attribute based encryption algorithm provides collusion resistance against any number of colluding users. Each authority's attribute set must be disjoint. To overcome this problem, a separate copy of each attribute for each clause may be created. The CA can decrypt every cipher text so that the user privacy and confidentiality of the data is less in this system.

The system structure of RSA algorithm is based on the number theory. It is the most security system in the key systems. A third party cannot break the private key because of factorization of larger numbers. If you want to break the information, you need to decompose a large number. In order to make the RSA safety, it must choose a large value for x and y. Users' usually choice more than 100 decimal digits, so that the attacker cannot decompose the N in polynomial time effective internal. The RSA encryption and decryption algorithm need a lot of calculation and the speed is slow when compared with the symmetric cryptographic algorithm. Size of the key is inversely proportional to security. In order to increase the level of security the size of the key should be greater. If the size is long the computational speed will be greater.

Message digest functions are faster than the traditional symmetric key cryptographic algorithms. The recently used message digest algorithms have no pattern restrictions. MACs based on message digests provide the "cryptographic" security for most of the Internet's routing protocols. Message digest functions appear to provide an excellent means of spreading the randomness from an input among all of the function's output bits. The performance of the algorithm has been analyzed by considering the parameters like block size, key size and the application of the algorithm, and is summarized in table 1



Algorithm	Block size	Key size	Security (in)
Multi-authority CP-ABE	Variant	512 to 4096 bits	Secure For MAN applications
RSA	Variant	512-2048 bits	Secure for large amount of data
Message Digest	Variant	>160 bits	Secure for internet routing protocol

Table:- 1 Performance comparison for the algorithms

V. CONCLUSION

CLOUD Computing is still a new technology where the cloud services are readily accessible as on a pay-per-use basis. Once the organization moves off from the cloud, it loses control over the data in the cloud. The protection level of the data is directly propotional to the value of the data. Cloud security depeds on trusted computing and cryptography. Only the authenticated and authorized user can access the data, even if some unauthorized user gets the data accidentally or intentionally and if captures the data also, user cannot decrypt the data and get back the original data from it. Data security is provided by implementing different algorithms like RSA, Message Digest, Multi-Authority CP-ABE ,SHA1, HMAC, DES,AES algorithms etc,. among these RSA, Message Digest, Multi-Authority CP-ABE algorithms are discussed. The performance of an algorithm on a cloud network varies according to the type of the algorithm such as symmetric, asymmetric or hashing algorithms and also varies with the size of the input. Our future work concentrates on the implementation of these algorithms to provide more secured cloud environment.

VI. ACKNOWLEDGEMENTS

T.Karthija has received her Under Graduate in Computer Science and Engineering from Anna University Chennai and Post Graduate in Computer Science and Engineering from NI University Kumarakoil in the year 2009 and 2012 respectively. Currently, she is working as a Assistant Professor in Computer Science and Engineering Department, V V College of Engineering, Tisaiyanvilai. Her area of interest is on Cloud Computing and IoT. She has five publications in her credit.

A.S.Radhamani has received her Doctoral degree in Computer Science and Engineering from Manonmanium Sundaranar University, Tirunelveli in 2015, Master's degree in Computer Science and Engineering from Manonmanium Sundaranar University, Tirunelveli in 2004 and Under Graduate degree in Electronics and Communication Engineering from Bharathiyar University, Coimbatore in 1995. She is the author of fifteen journal publications in her credit. Currently she is working as an Associate Professor in VV College of Engineering,Tisaiyanvilai. Her research interest includes multi core computing, parallel and distributed processing and cloud computing.

V.G.Anisha Gnana Vincy has received his Under Graduate and Post Graduate in Computer Science and Engineering from Anna University in the year 2008 and 2011 repectively. Currently,she is working as an Assistant Professor in Computer Science and Engineering Department, VVCOE, Tisaiyanvilai. Her area of interest is on Cloud Computing and IoT.She has five publications in her credit.

L.Amutha Swaminathan has received his Under Graduate in Electronics and Communication Engineering from Anna University Chennai and Post Graduate in Applied Electronics from PRIST University in the year 2008 and 2011 respectively. Currently, he is working as an Assistant Professor in Electronics and Communication Engineering Department, V V College of Engineering, Tisaiyanvilai. His area of interest is on Cloud Computing, IoT and Robotics. He has seven publications in his credit.

REFERENCES

I. Aarti Singh, Dimple Juneja, Manisha Malhotra, (2017). A novel agent based autonomous and service composition framework for cost optimization of resource provisioning in cloud computing. Journal of King Saud University – Computer and Information Sciences, 29, 19–28.

II. Anirudha Pratap Singh, Syam Kumar Pasupuleti, (2016). Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing. 6th International Conference On Advances In Computing & Communications, Procedia Computer Science 93 (2016),751 – 759.

III. Balkees Mohamed Shereek, ZaitonMuda, SharifahYasin, (2014). Improve Cloud Computing Security Using RSA Encryption With Fermat's Little Theorem. IOSR Journal of Engineering,4(2),1-8.

IV. Bin Feng, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu, And Tie Qiu,(2016). An Efficient Protocol With Bidirectional Verification For Storage Security In Cloud Computing. Special Section On Emerging Trends, Issues And Challenges In Energy-Efficient Cloud Computing, 4, 7899-7911

V. Gunasekaran Manogaran, Chandu Thota, M. Vijay Kumar, (2016). MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing. 4th International Conference on Recent Trends in Computer Science & Engineering, Procedia Computer Science 87(2016), 128 – 133.

VI. Nabeel Khan, Adil Al-Yasiri, (2016). Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework. The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies, Procedia Computer Science 94, 485 – 490.

VII. Rajkumar Buyya,(2013).Introduction to the IEEE Transactions on Cloud Computing. IEEE Transactions On Cloud Computing, 1(1), 3-21

VIII. Saurabh Dey, Srinivas Sampalli and Qiang Ye, (2016). MDA: message digest-based authentication for mobile cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 5(18),1-13 EARCH Open Access

IX. Victor Chang and Muthu Ramachandran, (2016). Towards Achieving Data Security with the Cloud Computing Adoption Framework. IEEE Transactions On Services Computing, 9(1), 138-151

X. Victor Chang, Yen-Hung Kuo, Muthu Ramachandran, (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems 57, 24–41.

XI. Yuh-Min Tseng, Tung-Tso Tsai, Sen-Shan Huang, and Chung-Peng Huang,(2015). Identity-Based Encryption with Cloud Revocation Authority and Its Applications. IEEE Transaction. Cloud Computing, PP(99),1-1.

XII. https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf