Survey on Data Security algorithms in Cloud computing

J. Sumitha, P. Poongodi

Abstract

The cloud computing is referred to the concepts of abstraction and virtualization. The cloud allows the user to storage the data and it has been accessed and retrieved from anytime and anywhere. Providing data security is one of the major concern of cloud computing technologies over the world. The importance of cloud security has been emerging so faster than even before. It provides scalability, availability, reliability and also the support of costs in todays increased IT environment that has been currently using the cloud computing technology. This paper has focused on the storage of data security on cloud, cryptography algorithms.

Keywords : Cloud computing, Cloud security challenges, Cryptography, Algorithms: AES, DES, TDES, RSA, Load balancing algorithm.

Introduction

The term "Cloud computing" refers to computing on the Internet, which is done computing on a desktop. Cloud Computing trend is rapidly growing were it has a technology connected with Grid Computing. It also refers to applications and services that run on a distributed type of network by using virtualized resources that are accessed by common protocols, procedures, rules, and networking standards. Now a day's the security of data has become more difficult issue. Possibly one can get the access of the cloud with the use of an ordinary client who can just simply access the information at anytime, anywhere without the need of any special software.

NIST definition of cloud computing Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., network servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [10]

The use of the word "cloud" makes reference to the two essential concepts:

Abstraction:

Cloud computing abstracts the details of system implementation from users and Developers. Applications that run on physical systems that aren't specified, data is stored in locations that are unknown, administration of systems is outsourced to others, and access by users is ubiquitous.

Virtualization:

Cloud computing virtualizes systems by pooling and sharing resources. Systems and storage can be provisioned as needed from a centralized infrastructure, costs are assessed on a metered basis, multi-tenancy is enabled, and resources are scalable with agility.

[1]II M.Sc Computer Science, Karpagam, University, Coimbatore. Tamil Nadu, India

[2]II M.Sc Computer Science, Karpagam University, Coimbatore. Tamil Nadu ,India

The "Cloud" means secure the Calculations and storage. The Security goals of data include three key points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography technique. Mainly the algorithms which is used are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing 4) Digital signature. The Integrity of data is ensured by hashing algorithms.

Characteristics of Cloud Computing

1) Self-service: The users will possibly make the decisions on the basis of how the computing power such as server time and network storage.

2) Broad Network Access: the computing amenities possibly are accessed over the network through the use of standardized mechanism that holds up different clients.

3) High Elasticity: The consumer can increase or decrease the computing mechanism using the requirements. The capacities are unlimited for the user.

Service Models in Cloud Computing

The cloud computing employs a service-driven of business model. To say as simple the hardware and platform-level resources are provided as services on an on-demand basis. The cloud computing offer services that can be grouped into three categories: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

1) Infrastructure as a Service : IaaS provide on-demand provisioning of infrastructural resources and it does not manage or control the infrastructure and only manage and control the storage, application and selected network components. Example : Amazon EC2.

2) Platform as a Service : PaaS provides software development frameworks and platform layer resources including operating system support. It controls either application and does not manage servers and storage. Example : Google App Engine, Microsoft Windows Azure etc.

3) Software as a Service : SaaS provides on demand application all over the internet. In SaaS user does not control or manage the servers, storage, network and application. Example: Rack space etc.

Deployment Models of cloud Computing

The deployment models of cloud computing are the following:

1) Public clouds are publicly accessible and in this type of cloud are managed by the third party.

2) Private clouds are only accessible in private network. Private cloud infrastructure those are available only in a specific member and managed by the organization itself or third party service provider.

3) Community clouds are only accessible to a few numbers of clients with known features.

4) Hybrid clouds are compositions of two or more clouds.

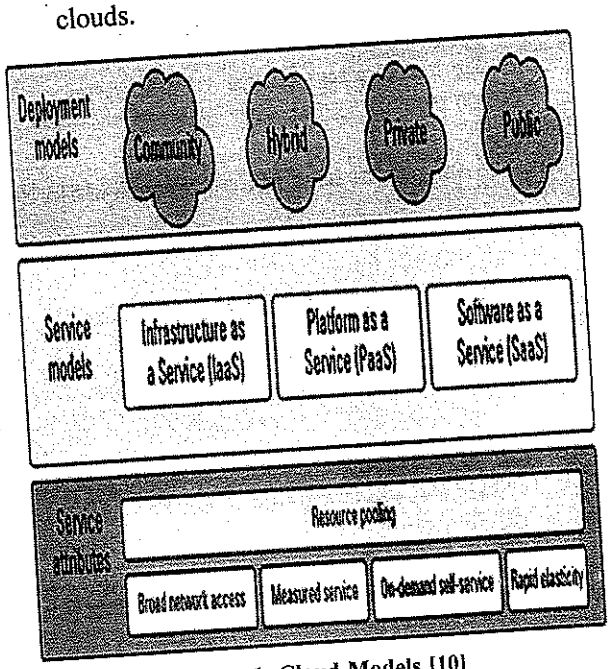


Figure 1. Cloud Models [10]

ADVANTAGES & DISADVANTAGES OF CLOUD COMPUTING

The following are the common advantages of cloud computing:

1) Lesser Cost : Pay as you go, negligible hardware investments or software Licenses.

2) Added performance : on demand processing time, even HPC, if required.

3) Fever Maintenance : somebody else manages the servers along with core Softvare.

4) Extra Security : easily repair, enforcement of policies, centralized data.

5) Wide storage Capacity : We can Use it when you require it.

The following are the Disadvantages of cloud computing are:

1) Dependency on Internet Connectivity : It requires a regular connection.

2) Loss of Control : The trouble of someone else hosting hardware, software

3) And data, which outcome in security concerns.

4) Unpredictable Cost : You can Pay as you go means that the price of computing will be differ every month.

DATA SECURITY ISSUES IN CLOUD COMPUTING

1) Data Confidentiality : It defines about the property that the data are made as available. It will disclose to illegal users. Example: Data Search, Data Share. The outsourced data is stored in cloud and out of owner's direct control.

2) Data Access Controllability : The cloud owner can perform certain amount of restriction of access of data. The legal users should only be authorized.

3) Data Integrity : It maintains and assures the accuracy of the complete data that are stored in the cloud.

4) Data Availability: It becomes a major legitimate issue because of the use of un-interruptible and seamless provision becomes relatively difficult.

Tips To Have Better Data Privacy Protection in Cloud Computing

1) The user should always avoid the sensitive information in cloud.

2) The user must read the agreement to find out how the cloud storage has been working.

3) The user should have a wide open of eye in each and every passwords.

4) Encryption of data.

5) The user should always use the encryption in the cloud.

Cloud Security controls

1) **DETTERENT CONTROL**
It is like a warning sign on the property of user data, who is working on the cloud.

2) **PREVENTIVE CONTROL**
It will strengthen the systems against the incidents or threats. It handles the system from the access of unauthorized person of activities.

3) **DETECTIVE CONTROL**
It will detect incidents and react to the appropriate incidents or threats.

4) **CORRECTIVE CONTROL**
It occurs during or after the incident which has been occurred in the cloud system. It is used to have a system restore and backups also.

Cryptography

The cryptography provides Confidentiality, Authentication, Data Integrity and Non Reputation.

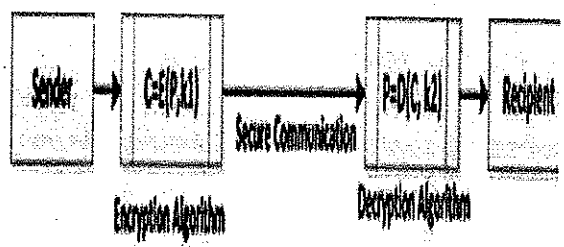


Fig.2.Encryption and Decryption Process [5]

Defining some terms used in Cryptography [5]:

1) Plaintext is the original intelligible source information or data that is input to algorithms.

2) Cipher text is the scrambled message output as random stream of unintelligible data.

3) Encryption Algorithm substitutes and performs permutations on plain text to cipher text.

4) Decryption Algorithm is encryption run in reverse by taking the secret key and transforming the cipher text to produce the original plain text.

5) A key are used as input for encryption or decryption and determines the transformation.

Sender and Recipients are persons who are communication and sharing the plaintext.

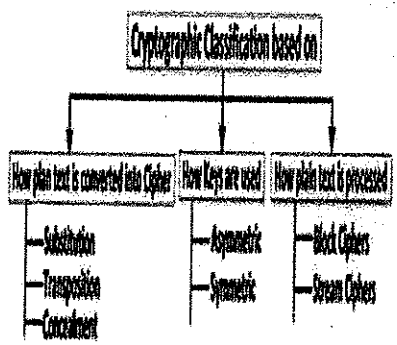


Figure. 3.Classification of Algorithms [5]

To provide secure communication over the distributed and connected resources the encryption algorithm [1] plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using " key" and only the user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Other technique is called as asymmetric key encryption where two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption.

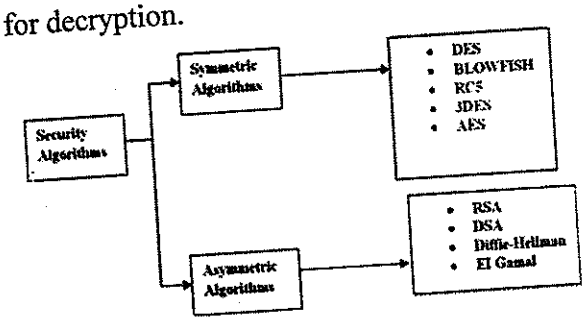


Figure 4. Security Algorithms [2]

The Cryptography acceptance of Cloud Computing by more security concerned companies. The first level of security where cryptography can help Cloud computing is secure storage. It is an art or science of keeping messages secure by converting the data into non readable forms. The cryptography is said to be as a combination of three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms, and Hashing. In Cloud computing, the main problems are related to data security, backups, network traffic, file system, and security of host. There are a number of existing techniques used to implement security in cloud storage. Some of the existing encryption algorithms which were implemented in research work are as follows.

Some of the Existing Algorithms in cloud Security

RSA Algorithm

RSA algorithm is public key encryption. This algorithm is brought to life by Ron Rivest, Adi Shamir and Len Adelman in 1977. It is hottest asymmetric key cryptographic algorithm. It may well use to provide secrecy. There in algorithm uses the top number to come up with people key and key depending on mathematical fact and multiplying huge numbers together. It uses the block size data during which plain-text and cipher text are integers between 0andn for a lot of n values. Size n is known as 1024 bits. There al challenge in the case of RSA algorithm would be the selection and generation of the public and private key. Within this two different keys can be used encryption and decryption. As sender knows about the encryption key and receiver knows about the decryption key, the way we can generate encryption and decryption get into RSA. The whole processes are made in below:

Choose large prime numbers p and q such that p~= q.

Compute n = p _ q

Compute _(pq) = (p ÀÛÜ 1) _ (q ÀÛÜ 1)

Choose the public key e such that gcd (_(n); e) = 1;

1 < e < _(n)

Select the private key d such that d _ e mod _(n) = 1:

So in RSA algorithm encryption and decryption are performed as:

Encryption : Calculate cipher text C from plain-text message M such that:

$C = Me \bmod n$

Decryption: $M = Cd \bmod n$

Key Generation	
Select two prime number, p,and q.	
Calculate $n = pxq$	
Calculate $\phi(n) = (p - 1)x(q - 1)$	
Select integer a; $gcd(\phi(n), a) = 1; 1 < a < \phi(n)$	
Calculate b.	
Public Key :	KU = {a, n}
Private Key :	KR = {b, n}

Encryption	
Plaintext :	$M < n$
Ciphertext :	$C = M^e \pmod n$

Decryption	
Ciphertext :	C
Plaintext :	$M = C^d \pmod n$

Figure 5. RSA Algorithm [2]

DES ALGORITHM

Data Encryption Standard (DES) also known as the Data Encryption Algorithm.

DES algorithm provides improvement over the RSA algorithm. The speeds of DES encryption can be several M per second, It can be well suited for encrypted numerous message. RSA algorithm will be based upon the issue of factoring, and it is computing velocity is slower than DES, RSA algorithm is merely well suited for encrypting a tiny bit of data, The RSA encrypt the data essentially 117 bytes of once. DES is really a block cipher. It encrypts the data in block height and width of 64 bits each. That's 64 bits are plain text goes as the input to DES, which produces 64 items of cipher text. Same key and algorithm can be used as encryption and decryption. DES uses 56 bit key but initial key is made up of 64bits. Key is 56 items of 8, 16, 24, 32, 40, 48, 56, 64 are discarded (these bits maybe used for parity checking to make certain the true secret doesn't contain any errors). Two fundamental features of cryptography Diffusion (Substitution) and Confusion (Permutation) rounds. In each round key and data bits are shifted, permuted, XORed and sent through, 8 round 64 bit plain-text is handed to initial permutation (IP).Then IP generates two halves left plain-text (LPT)and right plain-text (RPT).Each LPT and RPT goes through 16 rounds. At the last LPT and RPT are re-joined. Decryption is same process perform rounds in reverse order

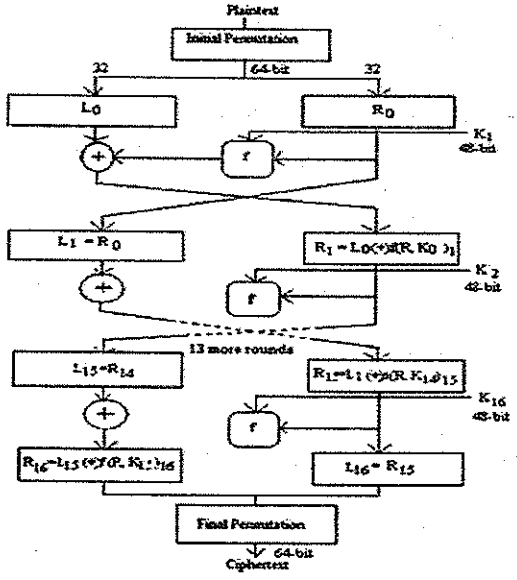


Figure 6. DES Algorithm [2]

AES ALGORITHM

AES algorithm is symmetric and parallel structure. AES is gives the implementation of the algorithm many flexibility. AES is usually compares well against cryptanalysis attacks. AES algorithm is useful with modern processor and deal with smart cards. AES key block size and length size from 128 and 256 Bits inside the step of 32 bits. AES necessitates that the plain text block size has to be 182 bits and key size should be 128,192 or 256 bits. In generally two versions of AES are widely-used: 128 bit plain text block joined with 128 bit key block and 128 bit plain text block with 256 bit key block.

TRIPLE- DES (TDES)

TDES is enhanced version of DES in TDES the key size is increased to increase i.e. 168 bits the security of data [14]. In TDES only size of key is increased rest of the working is similar to DES [12]. In TDES three different keys are applied on cipher block.

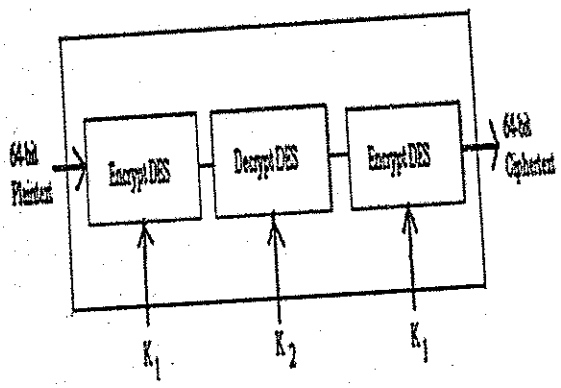


Figure 7. Triple-DES (TDES) [5]

DIGITAL SIGNATURE

Cryptographic digital signatures use public key algorithms to deliver data integrity. When you sign data which has a digital signature, other people can verify the signature, and may prove that the data descends from you and hasn't been altered after you signed it. In public key cryptography, anything 'A' encrypts with 'B"s public key maybe decrypted by 'B' while using corresponding private key. 'A' may encrypt a message along with her private key, meaning that 'B' can decrypt it with 'A"s public key. Because public key is, because the name suggests, publicly available, this is not good idea if 'A' wishes to keep that message a secret. Eve could also simply get a copy of A's public key thereby also decrypt the material. But because 'A' keeps her private key to herself, 'B' recognizes that only 'A' may have encrypted this message. 'B' is now sure that this message was compiled by 'A'. A signature on a paper message may serve as proof that it message was authored by the person who signed it. Encrypting having a private key thus might be thought to be a same as placing one's signature within the message. For this reason this is what's called setting up a digital signature to the message.

DIFFIE-HELLMAN KEYEXCHANGE

In 1976, Whitfield Diffie and Martin Hellman introduced a key exchange protocol with the use of the discrete logarithm problem. In this protocol sender and receiver will set up a secret key to their symmetric key system, using an insecure channel. To set up a key Alice chooses a random integer a [1; n] computes ga, similarly Bob computes gb for random b [1; n] and sends it to Alice. The secret key is gab, which Alice computes by computing (gb)a and Bob by

computing (ga)b. The important concepts on which the security of the Diffie-Hellman key exchange protocol depends are :

1) Discrete Logarithm Problem (DLP): If from g and ga Eve, an adversary can compute a, then he can compute gab and the scheme is broken.

2) Diffie-Hellman Problem (DHP): If from given the information g, ga and gb with or without solving the discrete logarithm problem, Eve can compute gab then the protocol is broken. It is still an open problem if DHP is equivalent to DLP.

3) Decision Diffie-Hellman Problem (DDH): If we are given g; ga; gb and gc, DDH is to answer the question, deterministically or probabilistically, Is ab = c mod n?

BLOWFISH ALGORITHM

Blowfish is a symmetric block cipher algorithm. It uses the same secret key to both encryption and decryption of messages. The block size for Blowfish is 64 bits; messages that aren't a multiple of 64-bits in size have to be padded. It uses a variable –length key, from 32 bits to 448 bits. It is appropriate for applications where the key is not changed frequently. It is considerably faster than most encryption algorithms when executed in 32-bit microprocessors with huge data caches. Data encryption happens via a 16-round Feistel network.

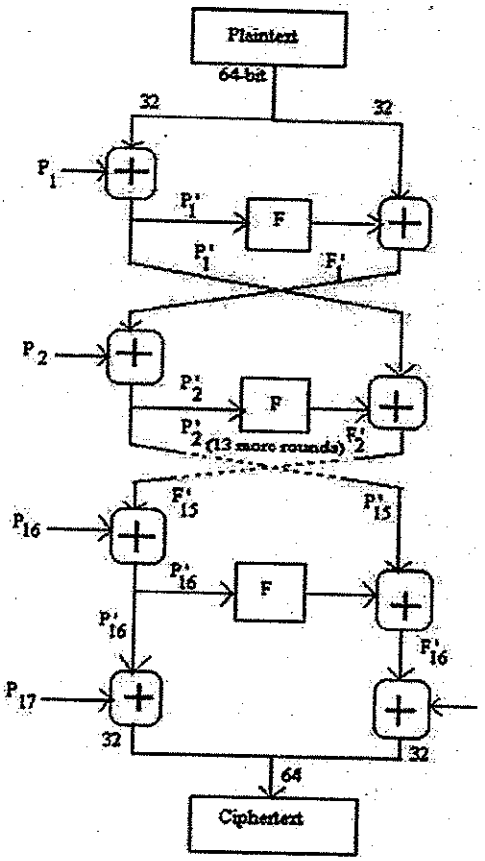


Figure 8. Blowfish Algorithm [2]

CONCLUSION

In this paper, the cloud computing algorithms for encryption and decryption, symmetric and asymmetric algorithms has been discussed. Here the Encryption is one such method that can provide feasible solution to the user and if the user have control over encryption and decryptions of data which will boost the consumer confidence and confidentiality. In the future, it can be extended by providing implementations for real data sets.

REFERENCES

1) M. Vijayapriya , *"SECURITY ALGORITHM IN CLOUD COMPUTING OVERVIEW"* International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345 Vol. 4 No. 09 Sep 2013.

2) Randeep Kaur1 ,Supriya Kinger2, *"ANALYSIS OF SECURITY ALGORITHMS IN CLOUD COMPUTING"*, International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN 2319 - 4847Volume 3, Issue 3, March 2014.

3) Abha Sachdev, Mohit Bhansali *"ENHANCING CLOUD COMPUTING SECURITY USING AES ALGORITHM"*, International Journal of Computer Applications (0975 – 8887),Volume 67– No.9, April 2013.

4) 1Omer K. Jasim, 2Safia Abbas, 3El-Sayed M. El-Horbaty and 4Abdel-Badeeh M. Salem, *"EFFICIENCY OF MODERN ENCRYPTION ALGORITHMS IN CLOUD COMPUTING"* International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN 2278-6856, Volume 2, Issue 6, November – December 2013.

5) Shakeeba S. Khan1, Prof.R.R. Tuteja2, *"SECURITY IN CLOUD COMPUTING USING CRYPTOGRAPHIC ALGORITHMS"*, International Journal of Innovative Research in Computer.

And Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015.

6) Akashdeep Bhardwaja*, GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastryd, *"SECURITY ALGORITHMS FOR CLOUD COMPUTING"*, International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science 85 (2016) 535 – 542.

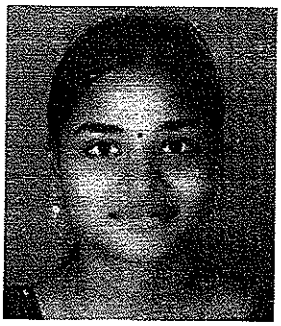
7) Er. Ashima Pansotra1 and Er. Simar Preet Singh2 *"CLOUD SECURITY ALGORITHMS"* International Journal of Security and Its Applications,Vol.9, No.10 (2015).

8) Rashmi Nigoti1, Manoj Jhuria2 Dr. Shailendra Singh3, *"A SURVEY OF CRYPTOGRAPHIC ALGORITHMS FOR CLOUD COMPUTING"*, International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), Vol. 3, Issue 1, January 2015.

9) www.wikipedia.com/clouddefinition

10) Barrie Sosinsky, *"cloud computing Bible"*, published by Wiley publications.Inc.

Authors Biography



J. Sumitha is currently pursing M.Sc Computer Science in Karapgam University, Her area of interest is network, cloud computing.

P. Poongodi is currently pursing M.Sc Computer Science in Karpagam University. Her area of interest is image processing and cloud computing