ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Survey on Various Data Encryption Algorithms Used in Cloud Security

S.Sandhya [1], U.Reshma[2], Dr.V.Praveena [3]

UG Students, Department of CSE, SNS College of Technology, India. [1] [2]

Assistant Professor, Department of CSE, SNS College of Technology, India [3]

ABSTRACT: In the latest developed technological world of computing and networking data, privacy and securities are the major threats. Cloud computing is the current prevailing fashion inIT industry. It allows the data storage and security of data. This paper mainly concentrate on the symmetric based encryption algorithm such as Data Encryption Standard(DES), Advanced Encryption Standards(AES), Triple Data Encryption Standards(3DES) and Blowfish algorithms. The cloud security refers to wide set of policies, technologies, and control deployed to protect data, applications and the resources adopting cloud computing services. It is the sub-domain of computer security, network security, more broadly information security. This paper also reports the compliance on security provided by the algorithms.

KEYWORDS: Block cipher, keys, encryption, virtualization,

I. INTRODUCTION

On basis of security issues associated with the cloud computing, It has two major categories

1. Provider based security issues(issues like platform, software, infrastructure).
2. User based security issues (the data's or applications stored on to the cloud by an organization or companies).

Both the client and the provider have major role in matter of securing the data's. Provider must make sure that the data's stored in cloud will be fortified. The user must take measures by enriching their applications or data's with the strong password and authentication. Out of these three major services which are provided by the cloud providers such as –PAAS, IAAS AND SAAS, SAAS is considered as a efficient service.

- SAAS-Software service helps the cloud user to deal with any software without installing it on to the system.
- This minimize from burdening the system with additional software which is not frequently used
- In this cloud user will have the minimum control over the cloud access.
- SAAS application have been given to the user through internet.

Virtualization technique was first started to run multiple operating system on a single hardware device. But now it plays a role in testing and cloud computing field. Cloud providers often give the virtualization technique as a product of their service packet provided to the customer.

Virtual Machine Monitor is a special technology also called as virtual managers which co-ordinates the basics of virtualization in the field of cloud computing.

Types of virtualization

1] Network virtualization
2] Storage virtualization
3] Server virtualization
4] Data virtualization
5] Desktop virtualization
6] Application virtualization

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

DATA ENCRYPTION:

To uplift the protection of the data's on the cloud computing, advanced encryption technique has been included. It is more commonly called as "Crypto Shredding". Cloud enhances the cryptography technique, which relates to data encryption, ensuring that information is not allowed by unauthorized persons in the way that is not detectable by authorized persons. Data encryption is a process in cloud for transferring or encoding the data before moving to cloud storage. Cloud encryption is almost identical to data and takes time to learn about the provider's policies and procedure for encryption and encryption keys. Because of one identical encryption on few database fields such as password, account numbers can be hided from the hackers. Methods of data encryption

- Encrypt the data before it is uploaded
- Secure access with cloud cryptography
- Protect the data in transit with cloud access security broker.

Algorithms for data encryption: There are two types of algorithm in data encryption

1. Symmetric
2. Non-symmetric

SYMMETRIC ENCRYPTION:

This is the simplest kind of encryption that involves only one secret key to cipher and decipher information. Symmetrical encryption is an old and best-known technique. It uses a secret key that can either be a number, a word or a string of random letters.

ASYMMETRIC ENCRYPTION:

Asymmetrical encryption is which extremely and absolutely a new method when compare to symmetric encryption and it is also called as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two different keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that the third persons cannot use the keys.

II. RELATED WORK

[1]This paper deals with the recent surveys on research related to single and multi-cloud security and also provides the possible solution. This paper aims to provoke the use of multi-clouds which reduce the security issues that affect the cloud computing users.

[2]In this paper the solution for complex access control on encrypted data. By using this technique the cipher text can be kept confidential. This methods are highly secured against the collusion attacks.

[3]This survey is about the cryptographic tools to provide efficiency for the data's in clouds and provides the distributed computing addressing these issues.

[4]This reports on recent attempts at breaking FHE challenges, and also discussing the difficulties in the security level of FHE challenges, based on the state-of-the-art. It precisely estimates that the security is either missing or too optimistic.

[5]This paper provides the leveled fully homomorphism encryption scheme. This can be transformed into pure fully homomorphism encryption scheme using bootstrapping, and its security is still based on the Approximate-GCD problem.

[6]This report shows the development of cloud computing, the also the factors hindering the adoption of cloud computing. The impact of cloud computing on IT manageability and cloud investments are briefly discussed. This paper mainly aims to quantify the potential, financial and environmental benefits that can be gathered from this technology.

[7]In this paper the design and implementation of a fully homomorphism encryption based on ring is explained completely.

[8]This paper study the security features and capabilities currently insisted in cloud computing field and the securities provided. Also tries to overcome the security pitfalls.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

[9]This paper reports on cloud security and privacy and focus on the confidential data's and query access privacy for sensitive data. These provide a comprehensive study on the state-of-the-art schemes and security techniques and explain their tradeoff in security, privacy, functionality and performance.
[10]This paper proposes an advanced version of proxy re-encrypted scheme and provided an comparison between the old and the new proxy re-encrypted scheme on the basis of turnaround time, energy consumption, CPU utilization and memory utilization. This incremental version has provided the better result.
[11]This paper provides the definition of security architecture with the open security alliance (OSA).
[12]This paper constructs an Attribute Based Encryption (ABE) that allows the users private keys to be expressed in terms of attributes and this paper provides the proof of security. Based on Decisional Bilinear Diffie-Hellman (BDH) assumption.
[13]This paper comes up with a new idea of ABE and IBE for fine grained access control of cryptographic solutions. ABE uses access policies t control the encrypted data's.
[14]This paper analyse the risk in virtualization technology and also given the specific measure for reducing the risks in order to improve the practical application and its development.
[15]In this paper the most important threats found in the literature related to Cloud Computing and its environment as well as to identify the state of a of being exposed to the possibility of being attacked and threats with possible solutions.
[16]This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.
[17]This is a paper of proposed design in which the user is flexible of distributed storage, utilizing the homomorphism token and distributed erasure-coded data. the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append.
[18]In this paper they have explained that the virtualization technique adopted for cloud security which is based on the management tools used in the physical server-based deployment won't meet the needs of the highly dynamic virtualized one .
[19]This paper analyzes eight security risks of typical cloud computing services, proposing risk control strategies and legal regulation proposals for safety supervision.
[20] The first design of an auditing framework for cloud storage systems are explained in this paper. Then by-extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model.

III. PROPOSED ALGORITHM

SOME OF THE SYMMETRIC ALGORITHMS ARE:

1.DATA ENCRYPTION STANDARD:

It is a symmetric key block cipher.DES is an implementation of Feistel cipher. Feistel cipher is a structure used in the construction of block cipher. It is an iterated cipher with an internal function called round function. In this algorithm 16 round feistel structure. The block size is 64-bit. The DES has an maximum key length of 56 bits. The remaining 8-bit functions as a check bits only.

Initial an final permutation:

The initial and final permutations are straight permutation boxes that are inverse of each other.

Round function:

This if the heart of the cipher in des function. This applies the 48 bit key at the rightmost 32 bit to produce a 32-bit output.

Key generation:

The round key generator creates sixteen 48-bit n-keys put of 56-bit cipher keys. The below flowchart describes about the key generation architecture.

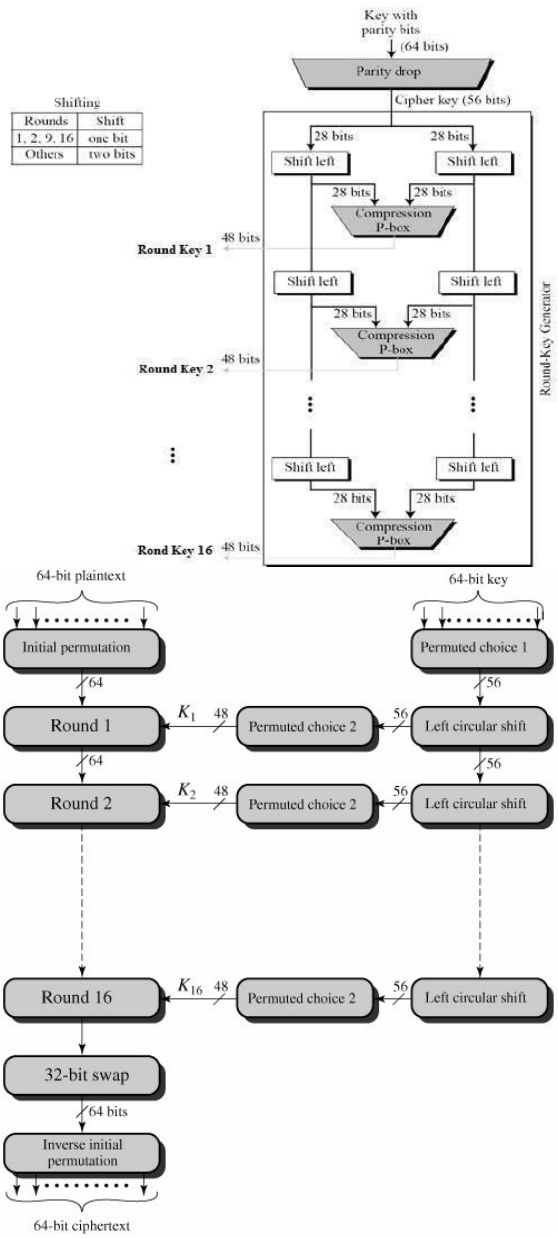
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017



DES analysis:

The DES satisfies both desired properties of block cipher. The two properties which made cipher strong are
1)Avalanche effect: A small change in the plain text makes a big change in the cipher text.
2)Completeness: Each bit of cipher text depends on many bits of the plain text.

From the past few years of analysis cryptanalysis has have analysed some weakness that is the keys that are selected are the weak keys.. eventhough DES have a very nice block cipher but it has an attack on “exhaustive key search”.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

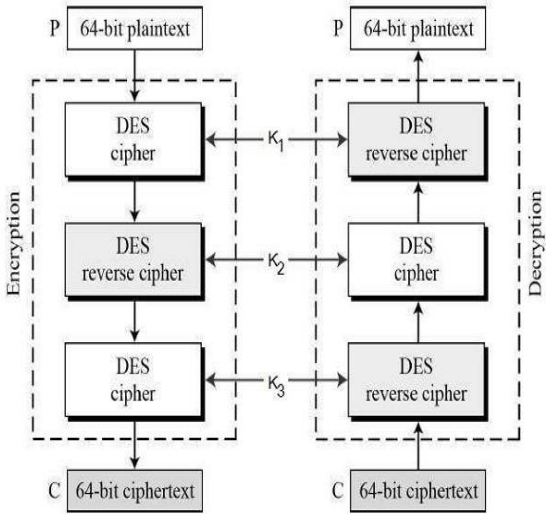
Vol. 5, Issue 9, September 2017

The major disadvantage is that DES fails in front of cryptanalysis during its design the attack wasn't invented but where as at the age of parallel computing breaking the DES security has become so easy for the hackers with the help of brute force attack. That's the reason for moving to the advanced technology than DES known as triple DES.

2.TRIPLE DATA ENCRYPTION STANDARD ALGORITHMM (3DES):

The speed of executive key searches in DES has begun to cause discomfort among the users of DES. Since it takes enormous amount of time to switch over from one algorithm to another algorithm that are widely adopted and embedded in large security architecture.

Triple DES operates in three steps: Encrypt-Decrypt-Encrypt (EDE). It functions by using three 64 bit keys such as k1 to encrypt, k2 to decrypt and k3 for last encryption. 3DES has two-key and three-key versions. In two key version the same algorithm runs three times, that is it uses k1 for both the encryption steps.



Keying option 1: All keys are independent.It is strong with 168 independend key bits .
Keying option 2: This provides a shorter key length of 112 bits and a reasonable compromise between DES and K1.This is an improvement over k1.
Keying option 3: All three keys are identical, i.e. $K_1 = K_2 = K_3$.This is backward compatible with DES, since two operations cancel out. Each DES key is with 56 bits of key and 8 bits of error-detection.

The reason for using the triple DES is to build a composite cipher that is stronger then single DES.Triple DES is much slower process than encryption using single DES. But the major defects in using triple DES is that it is more susceptible to cryptanalysis

3. BLOWFISH ALGORITHM:

Blowfish is a symmetric key block cipher designed in 1993 by Bruce Schneier. This algorithm provides the best encryption rate in software and not effected by cryptanalysis till date.

It is designed as an alternative measure to the DES algorithm. That is this algorithm is free from problems that other algorithm contains. While the other algorithms where hindered by the patents this algorithm is placed on the public domain, that it can be freely used by all

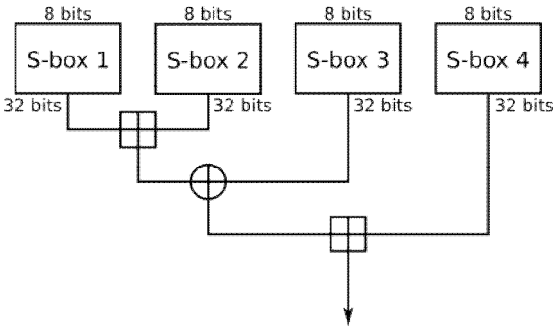
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017



Blowfish contains 64 bit blocks size and it also has the length varying 32 bits to 448 bits. It is a round feistel cipher at'nd uses large keys. In blowfish encryption routine there are five sub-key arrays: one 18-entry P-array and four 256 entry S-boxes(S0, S1, S2 and S3).

Every round consist of four actions that are performed during the process. Initially XOR is performed on the left half of the data with the rth P-array entry. Second, use the data's that are XORed as an input to the blowfish's function. Third, XOR the functions output with right half of the data and last step is to swap left and right data's.

The function splits the 32 bit input into four eight bit data'sand use the splitted data's as an input to the S-boxes. The S-boxes accepts each 8 bit data's and produce 32 bit output data's then the outputs are added and XORed to produce the final 32-bit output. After the 16th round the last swap is reversed and XOR left with K18 and right with K17.

Since blowfish use 64 bit block size makes it vulnerable to few attacks particularly in context like HTTPs and a reduced round variant of blowfish is vunerable to known plain text attacks on reflectively week keys. This algorithm uses 16 rounds and that are not susceptible to these kind of attacks .Blowfish can't provide authentication and non-repudiation as two people have same key. It also has weakness in decryption process over other algorithms in terms of time consumption and serially in throughputthis is the major reason that we go for AES algorithm.

4.ADVANCED ENCRYPTION STANDARD:

The AES algorithm is more popular and commonly used in world wide. It is used to overcome the defects of DES algorithm. This algorithm is a symmetric key symmetric block cipher. It is stronger and faster than triple DES. It gives full specification and design details. This algorithm is software implementable in basics languages like C and Java. AES contains three block ciphers such as: AES-128, AES-192 and AES-256. Each cipher do bth encryption and decryption process in the block of 128 bits using the cryptographic keys. It contains Rijndael cipher which is been accepted as a candidate for AES algorithm. It is the new symmetric block cipher that accepts the keys which size upto 128, 192 and 256 bits. The structure of rijndael displays high degree of modular design which can modify to any counter attack developed in the feature. This is the basic feature used inn the development of AES algorithm. But rijndael can accept additional block size and key length which is not possible in AES.

AES Design:

Symmetric cipher also called as secret key use same key for encrypting and decrypting hence the sender and receiver must use the same secret key. All key lengths are sufficient to protect the information which are classified under secret data to top secret data's. There are 10 rounds for 128-bits, 12 round for 192-bits and 14 rounds for 256-bit keys. Eachround consist of several levels of processing that indulge substitution, transposition and mixing of all plain text and transform into the cipher text. The first level of transformation is the substitution process using substitution table. The second transformation shifts the data rows and the third mixes the columns. Then the last level of transformation is to perform XOR function on each column using different part of encryption key-longer key needs more rounds to complete.

AES analysis:

AES is widely supported in both hardware and software. From the current analysis there have been no attacks on AES algorithm. AES has an in built flexibility if key length, which allows a degree of 'future proofing' against

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

progress in the ability to perform exhaustive key searches. AES security is assured only if it is correctly implemented and good key management.

V. CONCLUSION

As far as the current survey cloud security is one of the most important key factor in securing the information's that have been send through the internet. In the symmetric encryption algorithms DES, Triple DES and blowfish are considered to be hindered by cryptanalysis attacks bt where as the AES algorithm is so flexible and can extend its length and its highly secured way of data transfer. Thus Advanced Encryption Standard (AES) is considered to be the best outcome among the symmetric encryption algorithms.

REFERENCES

[1]M.AlZain, E.Pardede, B.Soh and J.Thom, **"Cloud Computing Security: From Single to Multi-Clouds".** In System Science (HICSS), 2012 45th Hawaii International Conferenceon jan 2012, pp.5490-5499.
[2]J.Bethncourt, A.Sahai and B. Waters. "**Cipher-text Policy Attribute-based Encryption".** In security and Privacy , 2007, SP'07. IEEE Sympoosium on IEEE, 2007, pp. 321-334.
[3]C.Cachin, I.Keidarr and A. Shraer, "**Trusting the Cloud".** ACmMSIGACT News, vol. 40, no. 2, pp. 81-86, 2009.
[4]J.Fan and F.Vercauteren. **"Fully Homomorphic Encryption. Cryptology ePrint Arechive".** Report 2012/144, 2012.
[5]C.Gentry and S.Halevi**. "Public Challenges for Fully Homomorphic Encryption"** TBA, 2010.
[6]S.Hemalatha, Dr.R.Manickachezian. **"Present and Future of Cloud Computing: A Collaborated Survey Report".** International Journal of Innovative Technology and Exploring REngineering (IJITEE)ISSN: 2278-3075. Volume-1, Issue-2, july 2012.
[7]S.Hemalatha and Raguram(2014). **"Performance of Ring Based and Fully Homomorphic Encryption for Securing Data in Cloud"**. International Journal of Advanced Research in Computer and Communication Engineering.
[8]Hickey, Kathleen. **"Dark cloud: Study finds Security Risk in Virtualization"**. Goverment Security News. Retrieved 12th feb 2012.
[9]Jun Tang, Yong cui(2016). **"Ensuring Security and /privace Preservation for Cloud Data Services".** ACM Computing Surveys.
[10]A.N.Khan, M.M.Kiah, S.A.Madani, M.Ali, S. Shamshirband et al**., "Incremental Proxy Re-encryption Scheme for Mobile Cloud Computing Environment"**, The Journal of Supercomputing, vol. 68, no. 2, pp. 624-651, 2014.
[11]Krutz, Ronald L and Russell Dean Vines. **"Cloud Computing Security Architecture".** Cloud Security: A Comprehence Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print.
[12]R. Ostrovsky, A. Sahai and B.Waters**, " Attribute Based Encryption with Non-monotonic Access Structures"**. In Proceedings of the 14th ACM conference on Computer and Communication Security. ACM, 2007, pp. 195-203.
[13]Z.Qiao, S. Liang, S.LDavis and H.Jiang. **"Survey of Attribute Based Encryption",** in Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2014 15th IEE/ACIS International Conference on , june 2014, pp. 1-6.
[14]M.H.song. **"Analysis of Risk for Virtualization Technology".** In Applied Mechanisms and Materials, vol. 539. Trans Tech Publ, 2014, pp. 374-377..
[15]Srinavasin, Madhan (2012). **"State-of-the-art Cloud Computing Security Taxonomics: A Classification of Security Challenges in the Present Cloud Computiing Environment".** ACM ICACCI'.
[16]S.Subashini and V.Kavitha "**A Survey on Security Issues in Services delivery models of Cloud Computing".** Journal of Network and Computer Applications. Vol. 34, no. 1, pp.1-11.2011.
[17]C.Wang, S.Chow, Q.Wang, K. Ren and W.Lou, **"Towards Secure and Dependable Storage Services in Cloud Computing".** Services Computing IEEE Transactin on, vol. 5, no. 2, pp. 220-232,2012.
[18]Winkler, Vic**. "Cloud Computing: Virtual Cloud Security Concerns".** Technet Magazine Microsoft. Retrived 12th feb 2012.
[19] J.Yang and Z.Chen, **"Cloud Computing Research and Security Issues",** in Computational Intelligence and Software Engineering (CISE), 2010 Internnational Conference on. IEEE, 2010, pp. 1-3.
[20]K.Yang and X.Jia**, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing".** Parallel and Distributed Systems, IEEE Transactions on, vol. 5, no. 2,pp. 220-232, 2012.