Strengthen Security And Trust In Public Cloud Using- Symmetric Key Cryptographic Algorithms

Nida[1] Pinki[2]

[1, 2] M. Tech (CSE), School Of Computing Science And Engineering, Galgotias University, Greater Noida, India

Abstract— Cloud computing is an emerging technology which is widely adopted by today's information technology world. In the current scenario, it has broadly been used for data reposition and computational means. It targets to provide on-demand scalable access to shared pool of computing resources over the internet. Despites of its innumerable benefits such as cost, on-demand availability to its customers, various security concerns are evolving particularly in public cloud. As many organizations are moving towards the cloud there arises the need to protect their valuable data and hence, security of public cloud becomes a challenging issue and must be addressed. This paper presents an overview of several symmetric cryptographic techniques useful for data security, establishing trust and mutual authentication in public clouds.

Key Word:- Cloud computing, public cloud, cryptographic techniques, AES, DES, BLOWFISH, TDES, trust.

I. INTRODUCTION

Due to agile growth in technological advancement, business trends and technologies are changing day-to-day. An emerging cloud computing paradigm renders several benefits to its consumers among them are resource availability, compromising cost model, on-demand scalable services, pay-per use model etc. It helps their consumers by providing mainly three services; infrastructure as a service (IAAS), platform as a service (PAAS) and software as service (SAAS) [1].By employing these services users can store their sensitive data in servers and can access their data anywhere, anytime and need not to worry about the concerns of system failure or disk errors. Thus, cloud computing frees up of consumers from the concerns of infrastructure, hardware or software. Currently, cloud computing has three deployments models, Private cloud: also known as internal clouds, they are private network which provides cloud computing services to only restricted set of customers within internal network, Public cloud: also known as external clouds, in which the resources are shared by every user in a common space and is solely possessed by cloud service provider, Hybrid cloud: It is a composition of both private and public cloud and [2][3].Despite of its innumerable benefits, few challenging concerns must be addressed. One of them is security issue in public cloud. Public cloud offers cloud computing services to the public user and offers enormous value to businesses in respect of improved economics, agility, rapid elasticity, scalable resources etc.

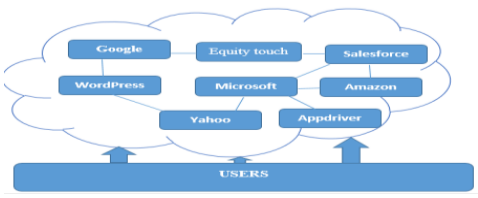

Fig. 1: Public Cloud Network

The public cloud model is operated by cloud service provider (CSP) and the services are provided throughout the internet. As several organisations are adopting cloud computing paradigm, they are constantly moving their valuable data on the cloud, which highlights the need to protect the data against unauthorized users, modifications in data, denial of access[16]. Protection of user's data in a public cloud can be achieved by implementing symmetric cryptographic key algorithms. The next section will discuss basic concepts of cryptography and will be proceeded by description of symmetric cryptographic algorithms in details.

II. OVERVIEW OF CRYPTOGRAPHY

With the technological growth in cloud computing, for data storage many organisations are migrating towards the cloud. Thus, security of user's data from unauthorised sources becomes a very critical issue in public clouds. Cryptography is technique that facilitates the security of users' data while it is being transmitted over the network. It converts the information in a form that is not understandable and thereby, prevent it from unauthorized access, modifications, repudiation etc.

A. Some Key Terminologies Related To Cryptography Are:

- Plain Text – Original message at sender side, which is to be transmitted.
- Key- An alphanumeric value which is applied to the plain text.
- Cipher Text- An un-understandable text format produced by encrypting plain text with an alphanumeric cryptographic key.
- Encryption- It is a process of converting plain text into cipher text using a secret key. It requires two main things an algorithm and a secret key to encrypt a message. It takes place at sender side.
- Decryption- It a process of converting cipher text back to original message (plain text).It takes place at receiver side.

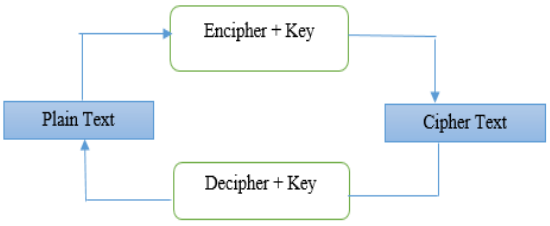

Fig. 2: Encryption /Decryption Process

B. Classification Of Cryptography

1) *Symmetric Key Encryption:* Symmetric key is a type of encryption technique in which same key and algorithm is used both at sender and receiver side. Is is also called as private key cryptography technique.

Some of the examples of secret or private key encryption are AES, DES, TDES, Blowfish, RC4, and RC5.

2) *Asymmetric Key Encryption:* Asymmetric key encryption differs from symmetric key by the fact that it uses two different keys for encrypting and decrypting the data. It is also called as public key encryption. In public key cryptography sender has its own private key and receiver has its own public key. Some of the examples of public key cryptography are RSA, Diffie -Hellman, Elliptic Curve Cryptography (ECC)**.**

With the innumerable benefits of cloud the user decides to use cloud services and will move his valuable data to the cloud [4]. So, there arises the need to protect valuable data of user by several different attacks. Thus, several symmetric key algorithms have been discussed responsible for data security in public cloud environment.

III. Description Of Symmetric Key Cryptographic Algorithms

A. Advanced Encryption Standard (AES)

AES is widely used these days for providing security to the cloud services and cloud user data. Advanced encryption standard (AES) ensures that the hash code is encrypted in extremely secure way.AES is designed by Joan Daemen and Vincent Rijimen in 1998 and was recommended by NIST in 2001 to replace Data encryption standard(DES).AES is a 128 bit block text encryption algorithm with a variable key length of 128,192,256 bits. It is grounded on permutation structure and, performs 10, 12, and 14 on AES-128, AES-192, and AES-256 respectively. The performance of AES is significantly higher than other related algorithm and is highly secure for public clouds. It is a non-fiestal cipher [5, 6].

1) Features of AES

- AES encryption algorithm requires less memory for implementation, which make it useful when low space condition occurs.
- AES techniques supports any block and key sizes which are multiple of 32.
- AES supports effective implementation both in hardware and software stages.
- No linear cryptanalysis and differential attacks have yet been showed on AES encryption algorithm.
- It is fast and flexible security algorithm.

B. Data Encryption Standard (DES)

Data encryption standard (DES) was designed by IBM in 1976 and it is 64 bit (8 byte) block cipher. In DES, the key is stored as 64bit and every 8^{th} bit is used in a parity check at the time of key generation. Thus, the key length becomes 56 bits.DES is based on Fiestal Network which means that deciphering is the same as enciphering process, it only uses the key in reverse order and both process uses the same algorithm[7].

C. Triple Des

DES was not secure due to its key length. So, TDES was developed which was backward compatible with DES. Triple DES provides three times encryption and decryption then DES and uses three different keys.TDES uses 8 byte (64bit) text block and uses 168(56*3) bit key. Three steps are used in encryption and decryption process of TDES, that is it uses DES three times [8, 9].

Let us suppose, there are three different keys K1,K2,K3.In the phase of encryption, in the first step ,the plaintext(information) is encrypted using key K1,Secondly, the cipher text attained from first step in decrypted using key K2, finally, the attained output of step 2 is again encrypted using key K3[9,10].

Triple DES Encryption steps:

$CT= (Enciypt)_{K3}((Decriypt)_{K2}((Encrypt)_{K1}(PT)))$ [9].

Triple DES Encryption Steps:

$PT= (Decrypt)_{K1}(Encrypt)_{K2}((Decrypt)_{K3}(CT)))$

Where ,PT stands for plain text, CT= Cipher text.And encrypt and decrypt are same process of DES encryption and decryption.

D. Blowfish Encryption Algorithm

Blowfish encyption algorithm was developed by Bruce Schneier in 1993 and is termed as very strong symmetric block cipher encryption algorithm[14].It is also an alternative for DES encryption algorithm.In this algorithm the same key is used for encrypting and decrypting the text at sender and receiver side respectively.It utilizes variable length key in the range 32 bit to 448 bit and 16 round fiestal cipher with S-Boxes independent of key.Blowfish encrption algorithm has two parts Key expansion and Encryption[15].In the part of key expansion ,448- bit key is split up into various subkeys , which gives the approximation of these subkeys to 4168 bytes.It takes 64 bit block at a time and divides this block into two equal halfs,each of 32 bits. Data encryption occurs by using 16 rounds of fiestal network[11,12]. Blowfish is slow compared to other algorithm and requires 3 to 4 times more memory space for cipher text than as required by plain text.

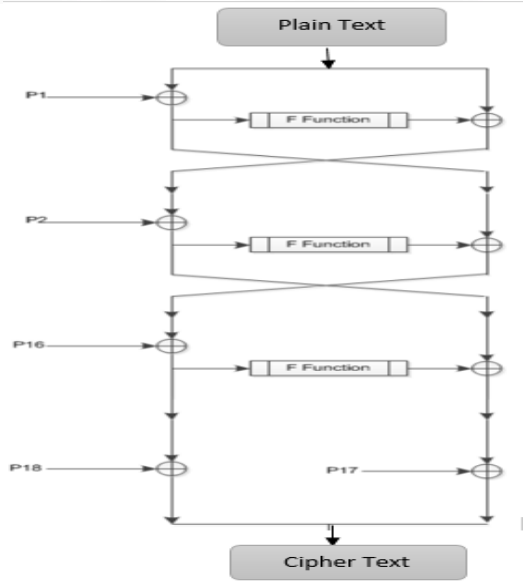

Fig. 3: Fiestal structure of blowfish [13]

IV.CHARATERSTICS AND COMPARSION OF SYMMETRIC ALGORITHMS

PROPERTIES	AES	BLOWFISH	DES	TDES
Platform in Use	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing
Cipher Text	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Key Size	128,192,256 bits	32-448 bits	56 bits	(56*3) bits
Key to be Used	For enciphering and deciphering same key is used	Same key is used for both processes	Same key is used for encryption and decryption	For encryption and decryption same key is used
Scalability	Scalable	Scalable	Scalable	Scalable
Block Size	128	64	64	64
Rounds	10,12,14	16	16	48
Space Required for Cipher text	Requires 3-4 times more space needed than plaintext	Takes 4 times more space than plaintext	It takes Almost 2 times more space	Requires 2-3 times more space than plaintext
Speed	High	High	Low	Moderate
Security	It is Secure technique for both service provider and client	It is Secure technique for both service provider and client	It is Secure technique for both service provider and consumer	It is Secure technique for both service provider and user
Capacity of data encryption	Used for encrypting large amount of data	Used for encrypting less data then AES	Used for encrypting less data then AES	Used for encrypting less data then AES
Authentication type	It is best provider for authentication	It is comparable to AES	Less than AES	Less than AES
Possible Attacks	Suffers from side channel attack	Does not have yet	Suffers from Brute force attack	Possible theoretically

REFERENCES

[1] Suresh Kumar RG1, S.Saravanan2, Soumik Mukherjee 3,"recommendations for implementing cloud computing management platforms using open source", IJCET, Volume 3, Issue 3, October - December (2012), pp. 83-93.

[2] Sun (2009a) A Guide to Getting Started with Cloud Computing. SunWhite paper. https://www.sun.com/offers/docs/cloud_computing.

[3] Cloud Computing – A Practical Approach by Velte, Tata McGrawHill Edition (ISBN-13:978-0-07-068351-8).

[4] Rachna Arora, Anshu Parashar ,"Secure User Data in Cloud Computing Using Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.ISSN: 2248-9622.

[5] Federal Information Processing Standards Publication 197,"Specification for the Advanced Encryption Standard (AES) "National Institute of Standards and Technology (NIST), November 26, 2001.

[6] A.K.Mandal,C,Parakash and M.A.Tiwari,"Performance evaluation of cryptographic algorithm: DES and AES",2012 IEEE Students's Conference on Electrical,Electronics, and Computer Science.

[7] Kruti R. Shah, Bhavika Gambhava, "New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[8] Kruti R. Shah, Bhavika Gambhava, "New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[9] Shashi Mehrotra Seth and Rajan Mishra, "ComparativeAnalysis of Encryption Algorithms for Data Communication", ISSN: 2229-4333, IJCST Vol. 2, Issue2,June 2011.

[10] Prasun Ghosal, Malabika Biswas and Manish Biswas, "A Compact FPGA Implementation of Triple DES Encryption System with IP Core Generation and On-Chip Verification", Proceding of the 2010 International Conference on Industrial Engineering and Operation Management, Dhaka, Bangladesh, January 9-10-2010.

[11] Gil-Ho kim, Jong-Nam Kim "An improved RC6 algorithm with the same structure of encryption and decryption", IEEE, ISBN 978-89-5519-139-4, Feb-2009.

[12] T.Gunasundari and Dr. K.Elangovan "A Comparative Survey on Symmetric Key Encryption Algorithms",International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 2, February- 2014.

[13] Rasheed Mokhtar Ahmed, Adel Zaghlul Mahmoud, "An Implementation of High Security and High Throughput Triple Blowfish Cryptography Algorithm", IJRRSAP Vol. 2, No. 1, ISSN: 2046-617X, March 2012.

[14] Russell K. Meyers and Ahmed H. Desoky," An Implementation of the Blowfish Cryptosystem", IEEE-978-1 -4244-3555-5/08, 2008.

[15] S. M. Dehnavi, M. R. Mirzaee Shamsabad, A. Mahmoodi Rishakani and Einollah Pasha,"Generalization of Statistical Criteria for Sboxes", IEEE, 978-1-4673-2386-4/12, May2012.

[16] Gansen Zhao, Chunming Rongy, Jin Liz, Feng Zhangx and Yong Tang, "Trusted Data Sharing over Untrusted Cloud Storage Providers," 2nd IEEE International Conference on Cloud Computing Technology and Science.

