DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5569

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ENHANCED SECURITY FOR DATA TRANSFER IN CLOUD

S. Gurupriya
Sri Sairam Engineering College, Sai Leo Nagar, West
Tambaram, Chennai, India

H. Refana Parveen
Sri Sairam Engineering College, Sai Leo Nagar, West
Tambaram, Chennai, India

R. Aishwarya
Sri Sairam Engineering College, Sai Leo Nagar, West
Tambaram, Chennai, India

J. K. Periasamy
Sri Sairam Engineering College, Sai Leo Nagar, West
Tambaram, Chennai, India

Abstract: In recent times, Cloud computing is considered as one of the emerging trends in the field of Science and technology. With no doubt, it is one of the strategic directions for many organizations and the most dominating infrastructure for enterprises as far as end users are concerned.Instead of buying the IT equipments and managing themselves, many companies prefer to buy the services from service providers to inflate their chances of increasing profit by reducing the cost. With dramatic increase in the number of cloud providers and the need to access cloud for organisation's benefit, Cloud computing is the panacea or the tool of choice for more cloud storage services. However, there comes a question for privacy and data security as more sensitive data and personal information gets transferred to the cloud. The proposed system discusses a method for security improvement using AES-128, IDA and X13 hash algorithm. Where, AES takes care of symmetric encryption which encrypts the file with single public key. The IDA is responsible for routing the pieces of data set to different storage locations thereby providing sophisticated data management. X-13 is a mining algorithm with thirteen different rounds of hashes and it is energy efficient while mining with a GPU or CPU.

***Keywords*:** Advanced Encryption Standard (AES-128); Information Dispersal Algorithm (IDA) and X13 mining algorithm.

1. INTRODUCTION

Cloud computing is a technology that offers numerous services which attracts the consumers and organizations at all levels. A cloud is a pool of virtualised computer resources and has the ability to host variety of job loads. The cloud supports redundant, self-recovering, highly scalable programming models that allow workloads to manage from recovery. Cloud computing uses open source REST based API's that are universally available and allows users to access the cloud services through web browser efficiently. It provides agility to improve the reuse of cloud resources. Also it provides multi-tenancy for sharing a large pool of resources to the users with the additive features.

It is deployed using three models such as: public, private and hybrid each having its own conditions and restrictions. Public cloud can be accessed over the internet. It provides scalability of resources. Mostly private clouds are preferred due its high security. Hybrid cloud is a composition of two or more clouds (private, community or public) and offers the benefits of multiple deployment models.

The services offered by the cloud falls under three main categories namely: Software as a Service (Saas), Platform as a Service (Paas) and Infrastructure as a Service (Iaas). Saas is an alternative way of accessing the software which eliminates the need of purchasing the software and loading the same onto a device. It is a subscription based model where the software is hosted in the cloud and can be accessed by the users via internet. Saas examples include SalesForce, Google Apps, and Office 350 etc. Paas is another category of software service where the platforms and environments are rendered as service to the developers for building applications and services over internet. Windows Azure, Force.com, Google App engine are some of the Paas examples. Iaas provides virtualized computing resources which can be accessed through WAN (Wide Area Network) such as internet. It also provides a range of services that accompany the infrastructure components. Some independent Iaas providers are Amazon Web Services (AWS) and Google Cloud Platform (GCP). In addition to these, cloud offers a massive data storage which could be accessed from anywhere in the world. Thus cloud serves to a great tool of choice for many consumers. Wherever the data is stored, a question of security arises. Hence there is a great need for establishing security in cloud. The proposed system describes an efficient way to ensure security using cryptographic techniques. Before the data is sent to the cloud, it is encrypted, dispersed into slices and finally hashing is performed. This encoded data is transmitted through cloud. In the same way, retrieval of original data from the encoded form involves decoding where the sliced data is verified for its authenticity and then encrypted file is reconstructed with the help of IDA which is then decrypted to obtain the original data.

2. PRELIMINARIES

***Cryptographic Algorithm*:** Cryptographic algorithm is a method of transforming plain text into cipher text. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". Data confidentiality may be provided by one of two categories of encryption algorithm, namely symmetric cryptography and asymmetric cryptography. Symmetric, or conventional, cryptography requires that the sender and receiver share a key, which is an item of secret information used to encrypt and decrypt data.

Symmetric and Asymmetric Algorithm: In symmetric key algorithm, the same algorithm and key is used for both encryption and decryption. Symmetric-key ciphers can be used as primitives to construct various cryptographic techniques. In asymmetric key algorithm uses pair of keys based on public key cryptosystem. One key used for encryption and other is used for decryption.

***AES*:** AES is a non feistel cipher that encrypts and decrypts a data block of 128 bits. The key size can be 128,192 or 256 bits. It depends on number of rounds. NIST evaluation criteria for AES are security, cost and algorithm implementation characteristics. Provides speed and code compactness on a wide range of platforms. For 128-bits AES, each round contains four steps: Byte substitution, Row shift, Column mixing and Round key addition.

Hashing algorithm: A hash function is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length. The output string is generally much smaller than the original data. A change to any bit or bits in the message can results in a change to the hash code.Hash code is also referred to as a message digest or hash value.

***IDA**:* IDA splits the files into small parts and make it unrecognizable when they in storage array.

3. RELATED WORKS

Cloud computing applies a virtualised platform with flexible and reliable resources. The idea is to move desktop computing to a service oriented platform using server clusters and huge databases at data centres. One of the primary concerns of IT and business decision makers regarding services provided by cloud is security management. Although most service providing vendors have been able to demonstrate that their cloud based applications are secure from an operational point of view. SAAS applications are gaining popularity due to their low barriers. In some cases business units are sidestepping IT and directly engaging with SAAS vendors, which can lead to additional IT headaches. Amazon web services [AWS] came out with Encryption as a service for providing security to data while transmission. Amazon EC2 provides the following services: resources from multiple data centres globally distributed, CL1, web services, web based console user interface etc. Also one can ensure that sufficient number of Amazon EC2 instances is provisioned to meet desire performance.

Recently proposed models are based on cryptographic algorithms [1, 8, 9, and 10] such as Data encryption Standard, Advanced Encryption Standard and Elliptic Curve Cryptography. To ensure the confidentiality of data before it is transformed to cloud, it is encrypted with the help of AES-128,192,256 depending on the file size and data format. [10]. Zhang X. and Wang H. proposed a system based on IDA for providing security in data storage [11].Proxy server is been used as key element. Using network drives files are copied by the users. Proxy server caches the files and generates random matrices to transform the desired files into multiple slices. In [7] IDA algorithm provides efficiency in computation and space. IDA has enormous application related to reliable and secure data transmission over a computer network. It also provides fault tolerance and efficient bandwidth to establish communication between parallel computers even for a single disk. By using constant size buffers time efficiency and highly fault tolerant are routed on n-cubes. [3]. A Combination of AES 256, IDA and SHA 512 are being used for the encryption, splitting and hashing respectively.

4. PROPOSED MODEL

A big hurdle that daunts from embracing the cloud is the vulnerabilities or the security concerns that prevails in the system. The proposed system consists of encoding and decoding data with the help of Advanced Key Encryption Standard with 128-bits key, Information Dispersal Algorithm and then X-13 hash algorithm. According to [5], AES 128 is suffice to provide security. Regarding CPU overhead, usage of 256 bytes increases 40% CPU overhead than 128 bytes [13].Hence 128 bytes is sufficient enough to provide the same level of security as the latter but with a improvement in performance.According to [2], the operation time for encryption and decryption for 128 bytes is found to be lesser than 256 bytes which is illustrated in the figure 1(a)

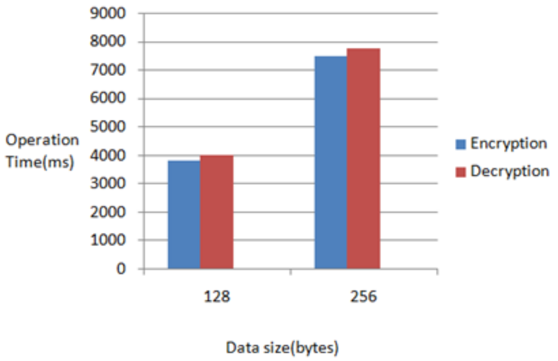


Figure 1(a)

Similarly, from the Figure 1(b) the number of CPU cycles was found to be lesser for 128 bytes than 256. X13 is a mining algorithm with 13 different hash rounds and functions defined for each round. These functions include blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo, hamsi and fugue. It uses 536 MB of RAM and is less vulnerable to ASIC attacks [11].

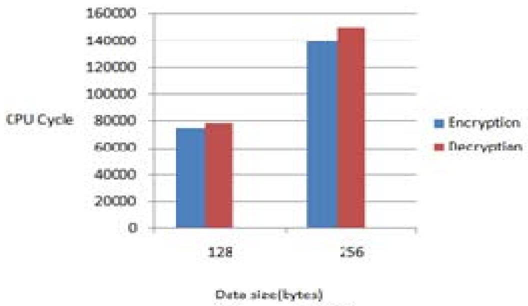


Figure 1(b)

4.1 Encoding:

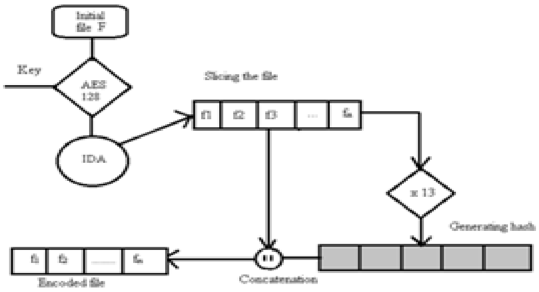
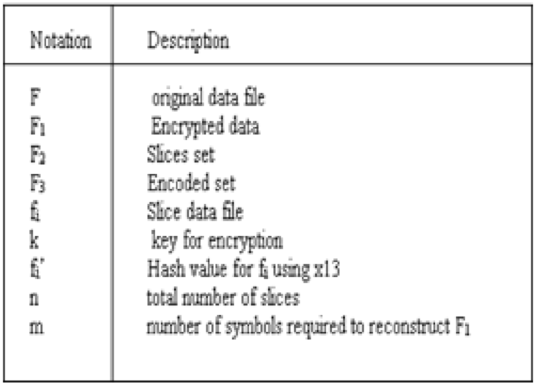


Figure 2

Initially, the input data stream is applied to Advanced Encryption Standard (AES 128) which works on data through ten rounds and produces encrypted data.

Table 1 shows the notation description used in both encoding and decoding. Using [3] for IDA CR-S slicing algorithm, the file is broken into separate slices such that the knowledge of the subset of these slices will help to reconstruct the original data file. The file F' is split into blocks of m symbols or bytes. A matrix is constructed of size m×w (Ω).And a Cauchy matrix (G) of order n×m is generated to transform the original matrix into n slices. Both the matrices are multiplied for dispersal to produce a matrix say δ with n rows and w columns.



Notation	Description
F	original data file
F_1	Encrypted data
F_2	Slices set
F_3	Encoded set
f_i	Slice data file
k	key for encryption
f_i'	Hash value for f_i using x13
n	total number of slices
m	number of symbols required to reconstruct F_1

Table 1

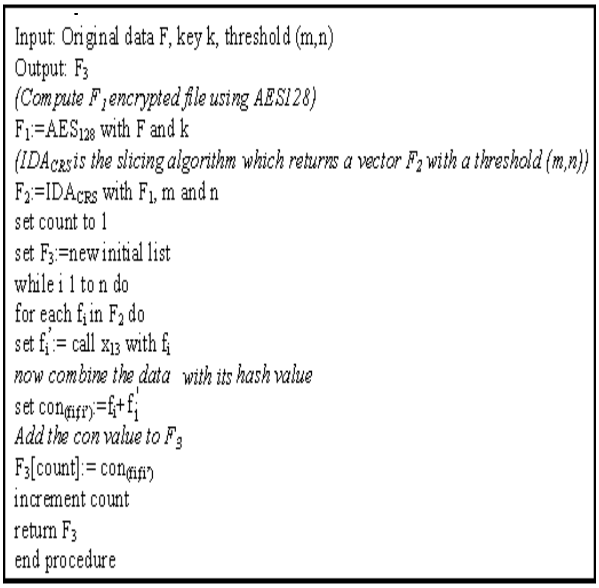
Thus a file F_2 of n slices is produced out of which, any m out of n can be used for reconstruction.

Finally, we apply x-13 algorithm to compute the hash values using 13 different hash functions through 13 rounds which makes it less vulnerable to attacks.

The output of slices from the encoding system (F_3) can now be uploaded in cloud with secure connection. These dispersed slices can be stored in at least three cloud service providers [6] so that even if one fails, other CSPs can be used for recovery.

4.1.1. Encoding Algorithm Pseudo Code:

The following pseudo code is used for encoding the raw data and converting it into a secured form.



```
Input: Original data F, key k, threshold (m,n)
Output: $F_3$
(Compute $F_1$ encrypted file using AES128)
$F_1$:=$AES_{128}$ with F and k
($IDA_{CRS}$ is the slicing algorithm which returns a vector $F_2$ with a threshold (m,n))
$F_2$:=$IDA_{CRS}$ with $F_1$, m and n
set count to 1
set $F_3$:=new initial list
while i 1 to n do
for each $f_i$ in $F_2$ do
set $f_i'$:= call $x_{13}$ with $f_i$
now combine the data  with its hash value
set $con_{(f_i f_i')}$:=$f_i$+$f_1'$
Add the con value to $F_3$
$F_3$[count]:= $con_{(f_i f_i')}$
increment count
return $F_3$
end procedure
```

4.2. Decoding:

Decoding step consists of verification and reconstruction. In verification part (figure 3), we check the integrity of the file with the help of hash values by de-concatenating the m slices and later used those slices for reconstruction. If there is any corruption, an authenticated message is displayed and the corresponding slice of data is replaced by another.

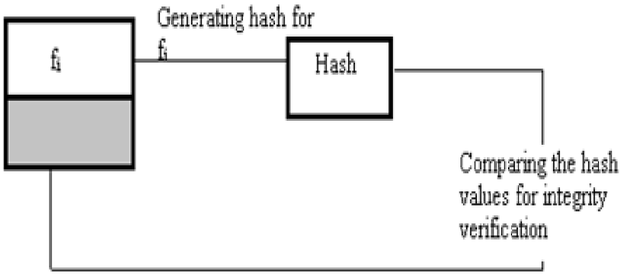


Figure 3

After verification is done, IDA is applied to the slices for reconstruction of encrypted data F_1 and finally original data (F) is obtained with the help of AES_{128} decryption. Using [3], IDA is performed to those recovered m part of slices. Now that the file F_1 is got, AES decryption is applied with the same key k used for encryption such that F=D (F_1, k).

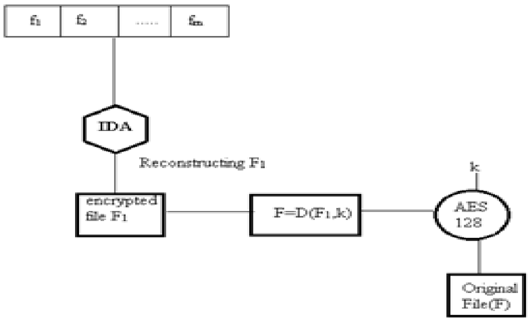
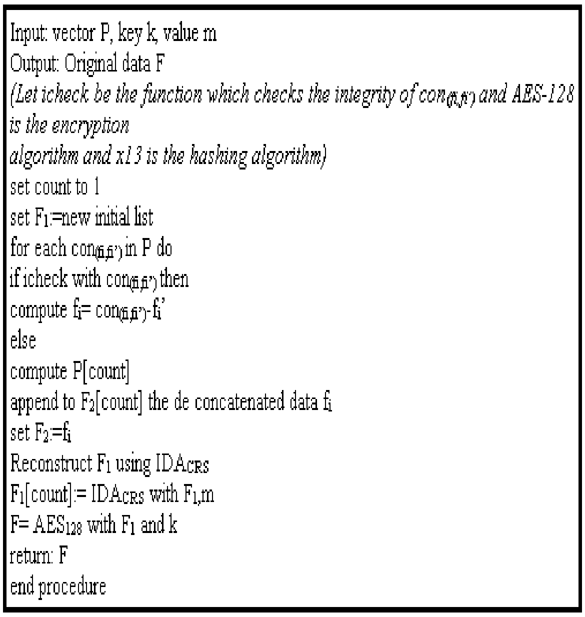


Figure 4

4.2.1. Decoding algorithm pseudo code

The following algorithm performs verification using icheck function, reconstructs the file using IDA and finally decrypts it to obtain the original data.



```
Input: vector P, key k, value m
Output: Original data F
(Let icheck be the function which checks the integrity of con(fi,fi') and AES-128
is the encryption
algorithm and x13 is the hashing algorithm)
set count to 1
set F1:=new initial list
for each con(fi,fi') in P do
if icheck with con(fi,fi') then
compute fi= con(fi,fi')-fi'
else
compute P[count]
append to F2[count] the de concatenated data fi
set F2:=fi
Reconstruct F1 using IDACRS
F1[count]:= IDACRS with F1,m
F= AES128 with F1 and k
return: F
end procedure
```

5. CONCLUSION

In the modernized era, the dependency on computer is inevitable and is almost mandatory.And in order to manage the voluminous amount of computer users and the large amount of data generated by these users and to efficiently share the resources, there is major demand for Cloud computing. Threats can be inside or outside the shared environment. For mitigating the threats and the vulnerabilities and for providing a secured environment for the users, we propose the system 'Enhanced Security for Data Transfer in Cloud'.

We have described in this paper, the risks involved in cloud data storage and provided a better solution of mitigating data security and privacy threats by improving the existing system. Our proposed solution is based on the combination of AES-128, IDAs and x13 algorithms for encoding, decoding and hashing operations. For encoding, AES-128 is used for encryption; IDA is used for partitioning of slices and x13 for hashing. AES-256 provides almost the same security as AES-128 but with a larger execution time. The hashing algorithm proposed in the system. Thus 'Enhanced Security for Data Transfer in Clouds' can be practically used in the cloud to provide a secured environment for the users to enable better communication in future.

6. REFERENCES

[1] M. Ahmadi, F. Fatemi Moghaddam, A. J. Jam, S. Gholizadeh and M. Eslami, "*A 3-level re-encryption model to ensure data protection in cloud computing environments*," *2014* IEEE Conference on Systems, Process and Control *(ICSPC 2014)*, Kuala Lumpur, 2014, pp. 36-40.

[2] H. Lee, K. Lee and Y. Shin, "*Implementation and performance analysis of AES-128 CBC algorithm in WSNs*," 2010 The 12th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, 2010, pp. 243-248.

[3] Jean Raphael Ngnie Sighom *, Pin Zhang and Lin You, "Security Enhancement for Data Migration in the Cloud" Future Internet 9, 23(2017), pp 1 – 13.

[4] Li, M. On the Confidentiality of Information Dispersal Algorithms and Their Erasure Codes. arXiv 2013,arXiv:1206.4123v2.

[5] LukeO'Connor"http://lukenotricks.blogspot.in/2010/04/aes-128-versus-aes-256-encryption.html" April 13, 2010

[6] K. K. Mar, C. Y. Law and V. Chin, "*Secure personal cloud storage*," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 108-113.

[7] Rabin, M.O. Efficient dispersal of information for security, load balancing, and fault tolerance. J. ACM 1989, 36, 335–348.

[8] G. Raj, R. C. Kesireddi and S. Gupta, "Enhancement of security mechanism for confidential data using AES-128, 192 and 256bit encryption in cloud," *2015 1st International Conference on Next Generation Computing Technologies (NGCT)*, Dehradun, 2015, pp. 374-378.

[9] S. Singh and V. Kumar, "Secured user's authentication and private data storage- access scheme in cloud computing using Elliptic curve cryptography," *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2015, pp. 791-795

[10] Surv, N.; Wanve, B.; Kamble, R.; Patil, S.; Katti, J. "*Framework for client side aes encryption technique in cloud computing*". Proceedings of the IEEE International Advance Computing Conference, Bangalore, India,(2015), pp. 525–528.

[11] Ugtarmas and Ystarnaud , "https://getpimp.org/what-are-all-these-x11-x13-x15-algorithms-made-of/"

[12] Zhang, Xuesong & Wang, Honglei. (2013). "A Study of the Use of IDAs in Cloud Storage. International Journal of Future Computer and Communication". 212. 10.7763/IJFCC.2013. Volume 2, pp -67-70.

[13] "https://crypto.stackexchange.com/questions/20/what-are-the-practical-differences-between-256-bit-192-bit-and-128-bit-aes-enc"

[14] Periasamy J.K.; Latha, B.; "*The Enhancement Of* Storage And Bandwidth Optimization Using Data De-Duplication", International Journal of Applied Engineering and Research, Volume 9, (2014), pp 4728 – 4732.