International Journal of Engineering & Technology, 7 (4.36) (2018) 368-372

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

PLIE- A Light-weight Image Encryption for data Privacy in mobile cloud storage

M.Sankari[1], P. Ranjana[2]

[1]Research Scholar,CSE dept,HITS,Chennai,India.
[2]Associate Professor,CSE dept,HITS,Chennai,India.
**Corresponding author E-mail: rs.sm1015@hindustanuniv.ac.in*

Abstract

Data privacy is the greatest challenge of mobile cloud computing to secure the image data. Traditional encryption techniques are mainly suitable for text data than image data. In this paper, we introduce a method called Privacy-preserving light weight Image Encryption (PLIE) to protect the image data in mobile cloud, maintains the user's privacy by keeping metadata in mobile. It improves the throughput, speed-up the encryption time in mobile and minimize the complexity. Basically,three processes handled on image data such as split, distribute and scramble (SDS) in mobile for maintaining the user's privacy and store it in cloud. For our analysis of gathering images, the encryption time of the PLIE method implemented in python language resulted as approximately 50% reduced than AES. We measured the performance analysis of existing method(AES) with the proposed method(PLIE) by various parameters. In addition,we present some security attacks to evaluate the level of security.

Keywords: Image Encryption;mobile cloud;Data Privacy;Throughput;

1. Introduction

Mobile cloud storage is a kind of cloud storage which is used to store the data in the cloud. The stored data can easily access wherever needed. The cloud storage providers offer services to allow the user for creating files, folders, images, pictures, and photos. Mobile Data Privacy defines the protection of user's personal information in mobile. The main drawback of mobile devices like smartphone are limited resources,less battery power and less memory. For previous techniques,we can outsource their data from mobile(Arshia Khan et.al.,2016) and encrypt it in the cloud. Here,privacy are not maintained. Further,partial encryption are handled in mobile and remaining computation in cloud.Then, Fully encryption are processed in mobile(Zhan Qin et.al.,2018) and store it in cloud where privacy is maintained.But computational overhead in mobile has increased due to large amount of memory,high complexity used for earlier encryption like DES,ADES,RSA,AES and takes high execution time.

The following current encryption techniques provide limited resources,less memory utilization in mobile are described as follows:The authors(Bahrami M and Singhal M,2015) described a light weight method for storing data, without using cloud computing resources for encryption, in multiple cloud by permutation method based on chaos systems to preserve data privacy and tested the image file to prove the concept. The authors(Mehdi et.al.,2016) described the parallel Data privacy method (DPM) and it provides a higher performance by using GPU (Graphic Processing Unit).It ensures the data as a secure and cost effective model to protect the users' data privacy. A light weight data privacy schema(Mehdi Bahrami and Mukesh Singhal,2016) introduced for Cloud based Databases to protect data on the cloud against an adversary inside or outside of an untrusted cloud vendor. A novel light-weight data privacy scheme(Arshia Khan et.al.,2016) introduced each device in IoT outsourced the data to the MCC directly and it allows IoT to keep data privacy. The author (Prathana Moden et.al.,)explains the survey of the techniques of various encryption with diagram and conclude to chaos concept is suitable for image encryption. In our proposed PLIE method,we describe the three processes (SDS) to maintain privacy by keeping metadata in mobile and secure image in cloud. It's speed-up the processing time and reduces computational overhead in cloud.

The following remaining sections are:In Section 2, we briefly explain the proposed PLIE method deeply with processes,diagram and its explanation. In Section 3, we describe the performance analysis of PLIE by various metrics. In section 4, we explain clearly the decryption process of the proposed method. In section 5,we present some security attacks in PLIE method. In Section 6, we conclude about the PLIE method and track the future direction for readers.

2. PLIE Method

PLIE method have used three different processes(SDS) to secure the image data by splitting,distributing and scrambled the image. At the same time,it's maintained the user's privacy by keeping metadata in mobile. And finally store it in cloud.

For **Splitting**,The original image file is divided into the header and the content of the file. The header file has some important privacy information such as type of file, file size, created date, chunk size, height, width, and resolution. The content has large amount of chunks.

For **Distributing**,chunks are grouped into the different files based on the pattern. A pattern may be user-defined or predefined function or a key. In PLIE,pattern act as odd (file1)and even

chunks(file2) will be continued in order. The maximum number of chunks formed 'm' as
m=[(img_size/Chunk_size)-Header_size]
where img_size represents the size of image file(bytes),Chunk_size represents the size of chunks(bytes) and header_size as the size of header of original file(bytes).

For **Scrambling**,scramble the file within it by adding Key K1(first row of the file1) with all rows of the files. Key K_i stored in the database.

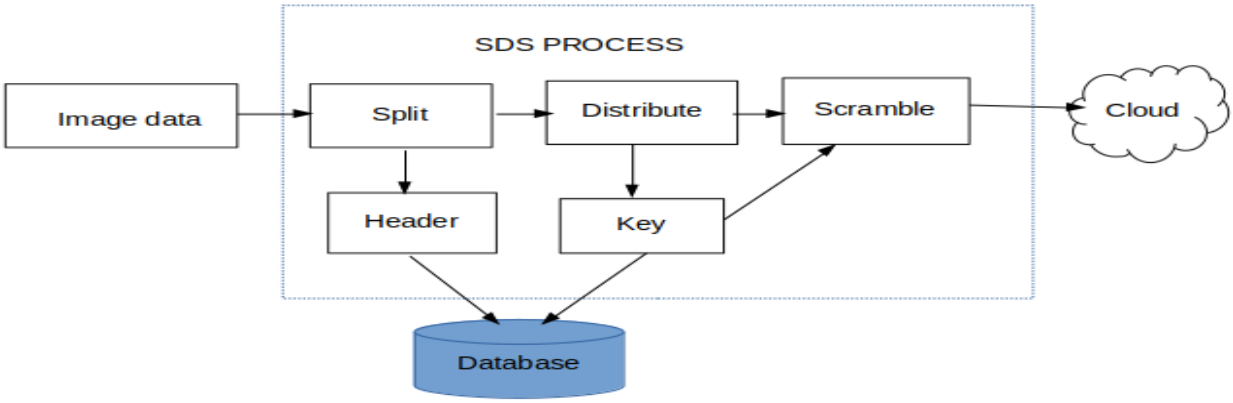

Figure1: Schematic diagram of PLIE Method

2.1 PLIE AlgorithmPLIE algorithm

Input:
he matrix of the image 'I',number of pixel in image 'n',maximum number of chunks formed 'm'.
Output:
The encrypted image E(I),key1,key2,H(i)
Process
Generate image file 'I'
Convert image file into binary data B(I)
Split:
for each pixel at position (i,n-1) in I do
for each pixel at position(k,m) do Split the image as header H(i)and content
C(i,k) B(I)← H(i)+C(i,k);
end for
end for
Distribute(pattern):
Distribute C(i,k) as different file by grouping of chunks based on pattern
File1←Collection of even chunks(C(i,k[even]) File2←Collection of odd chunks(C(i,k[odd])
Scramble:
Generate key1 as first row of the file1 and key2 as second row of the file2 Scramble file1 by key1 and file2 by key2
such as file1←key1+file1
file2←key2+file2 E(I)←encrypt(file1 and file2)
Return E(I),key1,key2,H(I)

3. Performance Analysis

We have implemented the PPIE method in python language. The performance analysis of PPIE are measured by the following metrics such as throughput,minimize the encryption time,Key sensitivity,low complexity to maintain privacy.

3.1 Encryption time minimized

The PLIE method is capable for image processing with high speed and reduce the encryption time in mobile. The time taken to encrypt the code is minimized as 50% approximately than AES. Consider the size of the chunk as 64,image of pixel size as 256*256, Key size of AES as 16 bytes, key size of proposed PPLiIE method varies based on the image file1 and file2 and pattern taken as even and odd chunks. Table 1 represents the various file size of image for encryption time of AES and PLIE method.

Table 1 Comparison of encryption time with PLIE method and AES

Image File	File size(KB)	Average Encryption algorithm(millisec)	
		AES	PLIE
Baby	4.9	0.7	0.33
Leaf	5.7	0.9	0.45
Wheel	6.5	1.13	0.4
Ball	8.7	1.13	0.41
People	13.3	1.1	0.49

The conclusion of the proposed PLIE method has reduced the encryption time as 50% approximately than AES. It clearly represents in line chart as mentioned below Fig 1.

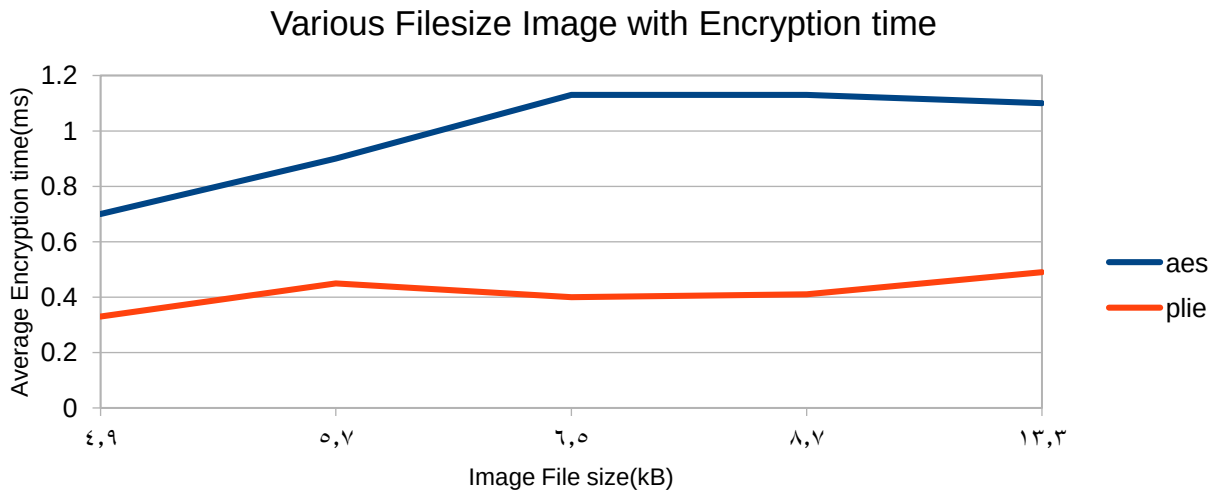

Figure 2 Various File size Image with Encryption time

3.2Low Complexity(number of rounds/iteration,splitting and time taken for execution)

We have taken the calculation of complexity in PLIE based on the three important factors such as splitting,number of rounds formed and encryption time of images. Basically,AES algorithm conducts four step processes to encrypt and decry pt the image data. Key length is high to secure the data effectively. In addition, execution time has increased due to the usage of more memory,CPU. Iteration are also increased. But in PLIE method,split the image to improve the speedup of the processing time and reduces the number of iterations formed. At the same time,it maintains the data security and privacy in mobile. Table 2 represents the number of loops handled in AES and PLIE.

Table 2 Comparison of AES and PLIE iteration

Image File	File size(KB)	Number of iteration	
		AES	PLIE
Baby	4.9	77	20
Leaf	5.7	90	25
Wheel	6.5	102	18
Ball	8.7	136	35
People	13.3	208	44

Finally,we conclude that the low complexity of PLIE method based on splitting image,encryption time minimized and iteration reduced than traditional encryption like AES,DES.

3.3 Throughput Throughput

Throughput(Dudhatra nilesh and MaltiNagle,2014) is defined as the amount of encrypted image data per unit time. Its measured by the speed of the image encryption. When there is an increase in throughput,power consumption has reduced. Consider $Image\_file\_size_i$ denotes the size of image file and $time\_ENC_i$ as the time taken for image encryption. We analyzed the throughput of AES($Throughput_{AES}$) and PLIE Method($Throughput_{PLIE}$) to understand the speed of PLIE method.

$$Throughput_{AES}=\Sigma_{i=1\ to\ n}(Image\_File\_size_i/time\_ENC_i)$$

=((4.9+5.7+6.5+8.7+13.3)/5)/(0.7+0.9+1.13+1.13+1.10)/5)

Ω7.882Mbps

$$Throughput_{PLIE}=\Sigma_{i=1\ to\ n}(Image\_File\_size_i/time\_ENC_i)$$

=((4.9+5.7+6.5+8.7+13.3)/5)/(0.33+0.45+0.41+0.4+0.49)/5)

Ω 22.73 Mbps.

Throughput comparison are represented by the column chart in Fig 2.

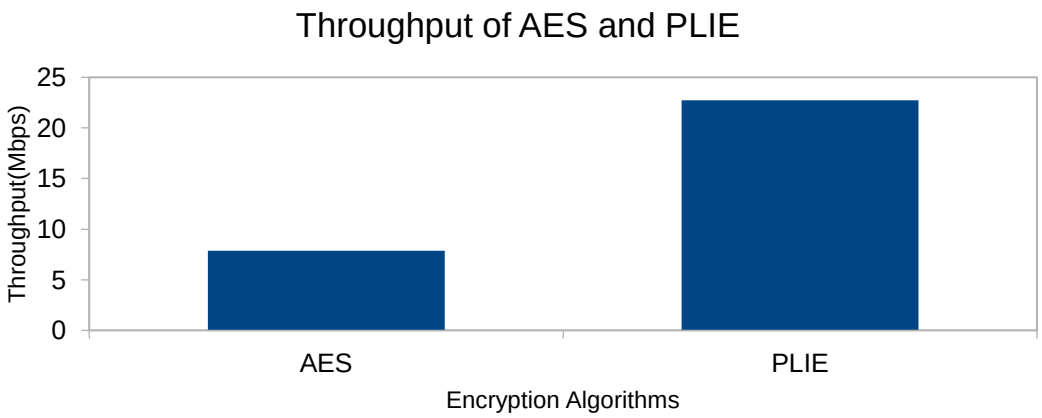

Figure 3 Throughput of AES and PLIE

Through this result,the throughput of the proposed PLIE method increased by 3 times than AES to evaluate the speed of the image encryption time and reduced the power consumption.

3.4Key sensitivity

A small change of key can reflect the large changes in encryption and decryption. Key sensitivity of an encryption is an important factor to have the large key makes more secure compared to a small key. Basically, AES performs 16, 24, 32 bytes long key used to encrypt the image data. But small key reduces the usage of resources in mobile. Our proposed PPLiIE method uses the small key and identifies it from the first row of the distributed first file and scrambles the binary file. Key is taken automatically from an image. Key size is reduced. Meanwhile, the proposed method maintains the security and storing the key in user's mobile to assure privacy.

4. Decryption Algorithm

The original image are regained from the reverse of encryption process.
Input:
Encrypted Image E(I),key k1,key k2,Header of the file H(I)
Output:
The original image 'I'
Process:
Fetch E(I)
Decrypt(E(I)) from cloud
Collection of file1 and file2
Compute key k1,key k2←mobile
file1←file1-key k1
file2←file2-key k2
Collection of chunks C[i,k]←file1 &file2
B(I)← H(I)+C[I,k];[Header of the file as H(I)]
Convert B(I) to I
return I

5. Security Attacks:

We have described various cases of security attacks in the PLIE method to prove the image retrieval impossible by the attacker. Basic need of attacker are key,pattern,header information and chunk size. Consider an image of pixel size as 12*12 and chunk size as 3 bytes.
Case 1:*If the attacker know the key and the pattern but he doesn't know the chunk size.*
If the attacker knows the key,even though he doesn't know the scrambled method. So,he wouldn't retrieve the image. If we apply brute force attack to collect the scrambled method,probability have more than 1 million possibilities. This is impossible to retrieve and wastage of time.
Case 2:*If the attacker know the key,pattern,chunk size ,but he doesn't the header of the file.*
If the attacker does scrambled image,retrieve the pattern,key and move to the next step. Eventhough,full image couldn't retrieved because of unknown header file in mobile.

6.Conclusion

We conclude than an PLIE method used different processes(SDS) for maintaining privacy and store it in the cloud. An PLIE method is well suitable for image encryption in mobile by reducing resource usage, throughput, speed-up the processing time and less complexity. We have proved with different performance measurement to maintain user's privacy in mobile and to reduce nearly 50% of the encryption time compared to existing method like AES. For future direction,it will be tested with other image formats like gif,png to express the level of security.

References

[1] Bahrami, M.; Singhal, M.(2015) "*A Light Weight Permutation Based Method for Data Privacy in Mobile CloudComputing* " 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud).
[2] B. Schneier, Applied cryptography, protocols, algorithms, and source code in C, John
[3] C.E. Shannon, A Mathematical Theory of Communication, The Bell System Technical Journal, vol. 27, no. 3, pp.379-423, 1948.
[4] Dudhatra nilesh;MaltiNagle(2014),"The new cryptography algorithm with throughput", International Conference on Computer Communication and InformaticsPages: 1 - 5
[5] Hong, J., Seo, S., Kim, N., & Lee, B. (2013)." *A study of secure data transmissions in mobile cloud computing from the energy consumption side"*. 2013 International Conference on Information Networking (ICOIN).
[6] H.C.A. Tilborg and S. Jajodia (eds.), *Encyclopedia of Cryptography and Security*, Springer, USA,2011.
[7] https://www.computerworld.com/article/3150992/wireless-carriers/the-votes-are-in-which-mo bile- data-provider-is-be
[8] D.Lohit Kumar;Dr. A.R.Reddy;Dr.S.A.K.Jilani;(2016)"*Implementation of 128-bit AES algorithm in MATLAB* ",International Journal of Engineering Trends and Technology (IJETT) – Volume 33 Number 3- March 2016

[9] Mehdi Bahrami;Dong Li;Mukesh Singhal;Ashish Kundu(2016)" *An Efficient Parallel Implementation of a Light-weight Data PrivacyMethod for Mobile Cloud Users*" 2016 Seventh International Workshop on Data-Intensive Computing in the Clouds (DataCloud),pg.no.51-58.

[10] Mehdi Bahrami; Mukesh Singhal(2016);" cloudPDB:*A light-weight data privacy schema for cloud-based databases*", 2016 International Conference on Computing, Networking and Communications, Cloud Computing and Big Data.

[11] Mehdi Bahrami; Arshia Khan; Mukesh Singhal(2016) "*An Energy Efficient Data Privacy Scheme for IoT Devices in Mobile Cloud Computing*" 2016 IEEE International Conference on Mobile Services.

[12] Prarthana Madan Modak; Dr. Vijaykumar Pawar(2015);"A Comprehensive Survey on Image Scrambling Techniques",International Journal of Science and Research (IJSR)Volume 4 Issue Xing Zhang;Seung-Hyun Seo;Changda Wang(2018);"*A Lightweight Encryption Method for Privacy Protection in SurveillanceVideos"*,IEEE Journals & Magazines,Volume: 6 Pages:18074-87.

[13] Zaheer Abbas Balouch;Muhammad Imran Aslam;Irfan ahmed(2017) " *Energy efficient image encryption algorithm*"2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT).

[14] Zhan Qin, Jian Weng, Yong Cui, Kui RenZen; Jian(2018) "Privacy-preserving Image Processing in the Cloud"IEEE Journals & MagazinesVolume: 5,Issue 2 Pages:48-57