International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 6 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/IJSRCSEIT

Multimedia Data Encryption Technique for Mobile Cloud Computing

Rishabh Shende[1], Dr. R. B. Ingle[2]
PG Student[1], PG Scholar, Professor[2],
Department of Computer Engineering, Pune Institute of Computer Technology, Pune, Maharashtra, India

ABSTRACT

Mobile devices and its applications make a new era for storing important data with in mobile device as well as on a cloud; it can be easily to share data, with others. Mobile Cloud computing paradigm is being used because of its low up-front cost. In recent years, even personal computer user, mobile phone users are storing their data at Cloud. Most of the mobile user stored there important information into their personal Mobile Devices. The securities of such a system against potential intruders as well as cloud service provider are the major target for most of the attackers. There is threat to the data in transit and data at cloud due to different possible attacks. By designing a provision which help to those mobile user to secure their data at transit as well as stored at locally on the same device by using Cryptography Encryption Technique, which helps to Store and Backup their personal data in secure Encrypted form with the help of Mobile Cloud Computing Mechanism.

Keywords : Cloud Computing, Mobile Cloud Computing, Mobile Device, Security, Encryption, Decryption, Key Management.

I. INTRODUCTION

Advancements in mobile system with Innovative Application and Decreasing prices of Smartphone devices, with high amount of storage space which make the people to use their local devices for storing their personal information. Most of the time people will even not able to transfer their multimedia information through mail system or Any other messengers application, due to which most of the time people need to Register their Devices with Cloud services provides for Storage Purpose, which is some time not even possible to Purchasing such Application. Our Application helps those users for storage and computational facility to shear their multimedia data with others, and helps to give external facility to store information in cloud account when their system not having sufficient storage. Mobile Cloud Computing becomes Major Trend which is used by most of the organization as well as those people who rely on Mobile Devices. In this era of Mobile Computing, people use their mobile as secondary source to store, sheared there data with other by using the Communication Mechanisms of wireless data Shearing system such as Wi-Fi or through Messengers. Most of the time people use their Mobile Device for Personal usage; it's often used as a repository for Storing and Backup user's personal information, such as User Passwords, Bank Account Information and Medical Records. The storage and computational requirement of mobile device by utilizing Cloud Infrastructure by interacting with cloud, Mobile Device can deliver various services to the user, such as healthcare, mobile commerce and online education. Users can upload and store data (photos, medical records) from their mobile device to the Cloud Storage and She a r with others, also Mobile Device can offload Computation Intensive tasks to the cloud to overcome its resources limitation and for saving storage

space as well as battery. Main focused on this project is to develop such encryption and decrypting algorithm to make a file with in the Mobile Device truly secure with the help of AES-128 bit encryption standard. Our major roll for development this mechanism is that to secure personal Information stored in Mobile Device as well as Backup Data like (images, pdf, doc), of size in the range of 10- more MBs. Also design such a light weighted encryption protocol which must be handling such a files on mobile device that are currently available in the market. Also the algorithm must be complete their task with in the Acceptable time frame due to which it is called as Light Weighted Application.

II. LITERATURE SURVEY

Existing work is based on Cloak stream cypher based encryption technique which is conducted to secure the communication channel of data transfer from mobile to cloud server. [1] Suggested that three versions of the protocol referred as s- CLOAK, r-CLOAK and d-CLOAK, the CLOAK is a light weight stream cipher based encryption protocol for secure data communication between two mobile de- vices. Basically this method is used for the generation of key or XORing. This is the fundamental idea of CLOAK which generation operation can be performed in an External server and the XORing operation performed on mobile device to generate cipher text. In previous paper [2] Suggested the basic working of mobile cloud computing and storage and computational requirement of mobile device by utilization of cloud infrastructure. Reference [3] talk about Users can upload and store data (photos, medical records) from their mobile device to the cloud and can share them with others. Mobile Cloud Computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smartphone users but a much broader range of mobile subscribers. Reference [4] talk about the key management facility which is required to shear on the time of message delivery and when the system checks the consistency of that key, also this paper covers the major facility of various key management mechanisms which is better with the various cloud services. Reference [5] talk about, security is a major concern in mobile cloud computing, particularly for mobile applications sending unencrypted personal information over insecure wire- less medium to the cloud. Data encryption is also required for protecting user's data against external and internal attacks within the cloud environment. Reference [6] talk about, the Encryption/decryption algorithms are commonly used for providing security to user's personal information using stream cipher and AES algorithm, is proposed in this paper an encryption system based on the algorithm on ARM(S3C6410), which can encrypt and decrypt the information in many kinds of memorizers, such as U-Disk, SD card and mobile HDD.

III. Comparative Study

NO.	Title.	Author.	Publication and Year.	Technique and Algorithm used.	Strength.	Weakness.

1.	CLOAK: A Stream Cipher Based Encryption Protocol for Mobile Cloud Computing.	Amit Banerjee, Mahamudul Hasan, Md. Auhidur Rahman, And Rajesh Chapagain.	IEEE Access, Year: 2017.	Developing CLOAK Mechanism for Encryption/ Decryption on mobile cloud computing.	1.Provide strategy of develop light weight secure application software 2. The whole mechanisms based on Light weight encryption technique which apply 128bit AES technique.	Lack details of actual security algorithm.
2.	Heterogeneity in mobile cloud computing: Taxonomy and open challenges.	Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya.	IEEE Communication Surveys, Year: 2014.	Detailed Analysis of Open Challenges.	1. The application developed for an OS version and Deployed in one Specific Product having less configuration and modification facility.	Problem on heterogeneity mobile cloud computing.
3.	A survey of mobile cloud computing: Architecture, Applications, and Approaches.	H.T.Dinh, C. Lee, D. Niyato, and P.Wang.	Wireless Communication and Mobile Computer, Year: 2013.	Mobile computing and Cloud Computing, Providing optimal services to mobile users.	1. Extending battery life. 2. Improving data processing power. 3. Improving reliability.	Problem on battery, data storage, processing power and reliability.
4.	Key Management for Cloud Data Storage:	A. R. Buchade, R. B. Ingle.	IEEE Conference on Advanced Computing Communicat	Symmetric key algorithm is faster than Asymmetric key.	Key management method with various cloud environments	Lack details of actual key management methods and

	Methods and Comparisons.		ion Technologies, Year: 2014.		, use of Symmetric key algorithms such as AES, DES, Blowfish and RC4.	Improved access security.
5.	A Practical implementation of transparent encryption and separation of duties in enterprise databases: Protection against external and internal attacks on databases.	U.T. Mattsson.	Proc. 7th IEEE Int. Conf. E-Commerce Technol. (CEC)	Encryption strategy and protection related to key management strategy and DBMS.	Authentication method.	Because of separation of duties encryption goes to week.
6.	ARM realization o storage devic encryption based on chao and AES algorithm	C. Wang, G. Wang, Y. Sun, and W. Chen	4th Int. Workshop Chaos-Fractals Theory. Appl. (IWCFTA)	Systems generate PIN sequence algorithms to encrypt source data	Improved security patterns.	Because of slow encryption process and weak key.

ALGORITHM

Algorithm CSPRN Generation

Function CSPRN_Gen (CSPRN, size: cs)

S ← random_num(); /*Key or seed*/

Sn← random_num(); /* Seq Num */

CSPRN ← NULL; /* Init. CSPRN */

N ← [cs/128];

While n > 0 do

CSPRN ← CSPRN + AES (s,sn);

Sn ← Sn + 1;

N ←n – 1;

return CSPRN;

MATHEMATICAL MODEL

Let S be a system
Such that S = {s, e, X, Y, V, fu, fm, Success}
in which,
s= Start state of system
e= End state of system
Input: X = { Upwd, pt }
Output: Y = { Eptf }
Functions: fm = { fAES, fSHA }
Fu = { Eptf }
Upwd = User Generated Password.
Pt = Plane text.
Eptf = Encrypted Plane text file.
fm= function of two main methods.
V = A set of classes implemented for an API.
Fu = {File not Encrypted or not Supported}
Success = {Encrypted file is Ready}

IV. EXPERIMENTAL ANALYSIS

The below analysis graph show that the encryption and decryption of our file data, where the size is not change with actual file size. To complete this analysis we perform execution on different symmetric key file algorithm of different key size. In this first size is of very small size till it taking same time as the file of size 128 bits is taking. This time taken is for the operations such as key generation, file encryption, file partition and file upload on a cloud. So analysis result shows that there is no much time variance even if file size increased.

As we know AES-128 is computationally secure against brute-force attack, most of the security organization and businesses places belief that AES is so secure and its key can never be broken.
In brute force attack longer keys exponentially more difficult than shorter ones.
In AES 128-bit required 3.4×10^{38} combination of keys which is not possible by attacker even the faster supercomputer 10.51 penta flops=10.51×10^{15} Flops.
[Flops= Floating point operations per second]

No. of Flops required pre combination checks: 1000.
No. of Seconds in one year = 365 x 24 x 60x 60 = 31536000.
No. of Years to crack AES with 128-bit key = $(3.4 \times 10^{38}) / [(10.51 \times 10^{12}) \times 31536000]$
$= (0.323 \times 10^{26}) / 31536000$
$= 1.02 \times 10^{18}$
= 1 billion billion years.
As the NIST survey they said that AES -128 bit key it takes same machine approximately 149 trillion years to crack a 128- bit AES key.in the end, AES has never been cracked yet and is safe against any brute force.

V. CONCLUSION

The Proposed system used to AES-128 bit key with 10 rounds provide the better performance on the other algorithm due to which this algorithm we used to do Encryption/Decryption mechanisms or for User generation Password increase the security and Speed of algorithm.

VI. REFERENCES

[1]. Amit Banerjee, Mahamudul Hasan, Md. Auhidur Rahman, and Rajesh Chapagain, "CLOAK: A Stream Cipher Based Encryption Protocol for Mobile Cloud Computing", IEEE Access, Volume: 5, Pages: 17678-17691, Year: 2017.
[2]. Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, "Heterogeneity in mobile cloud computing: Taxonomy and open challenges", IEEE Communication surveys, Volume: 16, Issue: 1, Pages: 369-392, Year: 2014.
[3]. H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches", Wireless Communication and Mobile Computer, Volume: 13, Issue: 18, Pages: 1587-1611, Year: 2013.

[4]. Amar.R.Buchade, Rajesh Ingle, "Key Management for Cloud Data Storage: Methods and Comparisons" 2014 Fourth International Conference on Advanced Computing Communication Technologies, Pages: 263 - 270, Cited by: Papers (2), Year: 2014.

[5]. U. T. Mattsson, "A practical implementation of transparent encryption and Separation of duties in enterprise databases: Protection against external and Internal attacks on databases," in Proc. 7th IEEE Int. Conf. E-Commerce Technol. (CEC), Pages: 559-565, Year: Jul. 2005.

[6]. C. Wang, G. Wang, Y. Sun, and W. Chen, "ARM realization of storage device encryption based on chaos and AES algorithm," in Proc. 4th Int. Workshop Chaos-Fractals Theory. Appl. (IWCFTA), Pages: 183-187, Year: 2011.

Cite this article as :

Rishabh Shende, Dr. R. B. Ingle, "Multimedia Data Encryption Technique for Mobile Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 6, pp. 42-47, November-December 2019.
Journal URL : http://ijsrcseit.com/CSEIT195619