Comparison for Confidential Cryptography in Multimedia Cloud Environment

Shilpi Harnal
Research Scholar, Department of Computer Science and Application
Kurukshetra University
Kurukshetra, India
shilpi13n@gmail.com

R.K. Chauhan
Professor, Department of Computer Science and Application
Kurukshetra University
Kurukshetra, India
rkchauhandcsakuk@gmail.com

***Abstract*— The working pattern and lifestyle of people has been changed due to wide adoption of cloud computing in daily life. Cloud is a perfect match for the low configured mobile devices. However, security of crucial data at cloud is always an issue of concern for its widespread applications. In this paper we have discussed the existing cloud security concerns for such crucial media data, along with that we have also reviewed our earlier proposed integrated algorithm for performing encryption and decryption while retrieving and storing multimedia data (images, audio and video files) to/from the cloud. As security of sensitive private media data of a client at cloud server is a big question and multimedia data handling always requires special attention. This proposed integrated security algorithm works in contribution towards this. In this paper we have made a detailed analysis of this algorithm and also compared it with some other proposed hybrid algorithms for a secure multimedia cloud computing environment.**

Keywords: Multimedia, cloud, AES, Blowfish, security, cryptography, confidentiality.

I. INTRODUCTION

The cloud computing creates a centralized virtual computing pool of resources connected with network to deliver software, hardware and platform services [1]. Cloud is an advancement of parallel computing, utility computing, distributed computing and grid computing [2]. Through cloud users can dynamically share high cost hardware and software from anywhere anytime and charges based on their actual usage [3]. In this way cloud helps to reduce burden and cost of huge storage, software's licensing, computing powers and cost of application deployment etc. [4] [5] [6]. As these services are accessed virtually through the dynamically configurable pool of scalable resources through private or public cloud networks [7].

But in current scenario, multimedia computing has become the lifeline for everyone, as today 90% of data generated, searched, processed, stored, reviewed, edited, shared and transferred is of media type. So smart mobile devices with limited storage, computing power and limited battery can easily manage storing, processing and editing of these rich media data and applications through cloud servers in distributed manner. Multimedia cloud relaxes the users from the burden of purchasing, licensing, installation and continual upgrades of heavy and expensive multimedia software. So cloud is acting as a boon for the mobile users to maintain the tradeoff between the communication and computational capability [8]. The access of these types of rich media data by millions of users simultaneously have rigid quality of service (QoS) and quality of experience (QoE) requirements in terms of delay, bandwidth and jitter that may leads to unsatisfied users [9] [10]. The ordinary cloud providers are providing media services but still its full adoption has to face various challenges like inside attacks, power consumption, migration, privacy, legal difficulties, heterogeneity of data, heterogeneity of networks, heterogeneity of devices, heterogeneity of type and quality of media services required [11][12]. In order to counter these requirements multimedia cloud providers need huge storage capacity, faster central processing units (CPUs), graphical processing units (GPUs), separate security aids and high speed internet connectivity unlike content delivery network like YouTube etc.

Media cloud providers needs to take care of various security and services issues as they has to deal with highly sensitive and crucial data like personal videos, photos, medical records, satellite data, sensors networks etc. [13]. According to [14] the five major security categories are: authentication, access control, integrity, confidentiality and non-repudiation. But integrity of data is a challenging concern while transferring data over wireless channels as mobile users are increasing day by day. Integrity issue can be managed efficiently with the help of cryptography [15]. Strong and complex cryptography techniques can provide a more secure transmission channel for communication [16]. Several such methods and algorithms for multimedia data are proposed by several researchers. Abdel-Karim [17] has proved that the Blowfish performs better than other encryption algorithms after performing a detailed comparison amongst most common encryption algorithms like AES, DES, triple-DES and Blowfish for data blocks of different sizes in C#. Blowfish is not having any known weak points so far so it is a better candidate for cryptography. We have applied both symmetric key algorithms i.e. blowfish algorithm and highly secure advanced encryption standard (AES) algorithm with random generation of secret keys and proposed an integrated algorithm to improve security while storing text and media files like images, video, audio etc. onto the cloud server [18]. The complexity of cryptographic algorithm is improved as private keys are generated randomly. In the next section we will discuss about the working of the earlier proposed integrated algorithm in brief along with the detailed analysis on different platforms. In further section we will compare its performance with other algorithms proposed by different researchers for multimedia files with the help of tables. The last section projects the future scope and conclusion.

II. THE ALGORITHM USED

We have performed a survey to find effective algorithm that can have wide acceptability against the side channel attacks for media contents in terms of cloud security. Side channel attacks are not so easy to track, so double level encryption and double level decryption can be an effective solution. The ordinary cloud providers perform single level of encryption/decryption. We have proposed a more secure integrated algorithm in earlier paper [18] with the combination of AES and blowfish with randomized 128-bits secret keys over different types and sizes of data for secure storage and retrieval of media data over cloud servers. For large amount of data symmetric cryptography is much better than asymmetric cryptography in terms of complexity and time. U.S. government was using the DES algorithm since 1977 [16]. However, this algorithm is not much secure as quick and inexpensive cryptanalysis exist for it. In 2000 the AES algorithm replaces the DES algorithm to overcome these vulnerabilities. But AES algorithm has the limitation of dealing with the text input only. So it is a challenging task to apply AES for different types of media data as input.

Blowfish is also a fast and free alternative to various existing cryptography algorithms. Like AES it is also a symmetric-key block cipher algorithm and also included in various cryptography algorithms. There is no effective cryptanalysis has been proved against it till now. AES is used by various big cloud providers but there are some known side channel attacks on various implementations of AES. Md. Asif [19] has also performed a detailed comparison of all symmetric cipher algorithms and proved that AES and Blowfish has better performance than others. So in the earlier proposed work [18] we have implemented a 128-bit AES algorithm along the with Blowfish algorithm using JAVA and tested for different types of multimedia input such as image, video and audio file on various platforms.

A. Implementation Details:

As cloud is a server-client model, the server end comprises of databases, security module, agent module and analysis module as described in figure 1. The client side consist only of security module and the contents player. The algorithm work under the security module to perform double encryption and decryption unlike the conventional cloud model as shown in figure 2. First level of encryption is provided with the secure and fast Blowfish algorithm and the resultant file is named as CipherText-1 that goes as input to the highly secure AES algorithm to generate the final cipher text file corresponding to the input media file to be stored over the cloud. Both the algorithms work with randomly generated secret keys. Same way double decryption is applied over the stored cipher file in reverse order while retrieving the media content from the cloud. The AES decryption module is applied over the stored cipher file in first step to generate the file named as CipherText-1. Then the second decryption module of Blowfish algorithm is applied to generate the corresponding media content file. The size and resolution of the retrieved media file is same as the original one that was encrypted. We have tested this over the google cloud server too. The model proposed for media cloud is shown in figure 1 and the complete procedure of the integrated algorithm with two levels of encryption/decryption phases is depicted in figure 2.

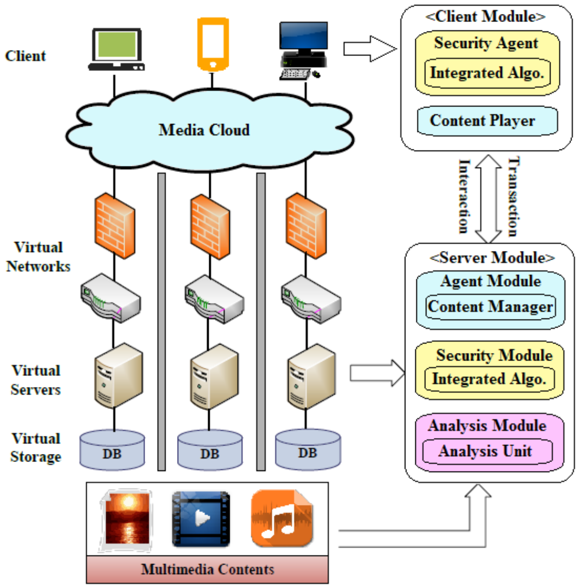

Figure 1: Proposed Model for Media Cloud [18]

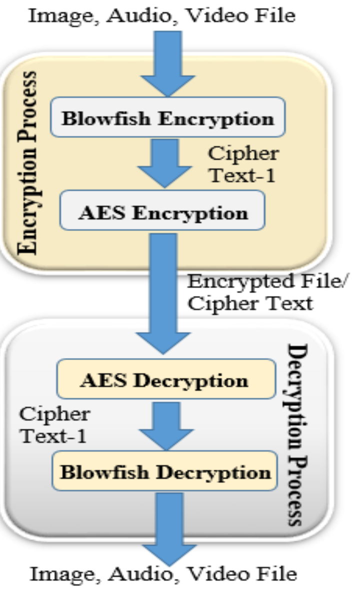

Figure 2: Proposed Integrated Algorithm [18]

B. Implementation Analysis on different Platforms:

In the earlier paper we had analyzed the performance of proposed integrated algorithm over different sizes and types of multimedia data such as images, video and audio files and it gives hopeful results for each input of such type. In this paper we have extended the analysis by performing the encryption and decryption over different platforms like Intel Pentium dual core (with 2GB RAM and 32-bit OS), core i3 (4GB RAM, 32-bit OS) and core i5 (4GB RAM, 32-bit OS) processors. We have run the algorithm on these platforms for the same multimedia files to analyze the performance for the real application.

The table 1 given below shows the different types of sampled multimedia data used and the time it takes for encryption and decryption process. The sizes of sampled inputs files are taken in kilo bytes (KB) units and times taken to perform encryption/decryption are measured in milliseconds (ms). For this we have not considered the time taken for the Blowfish key generation as it is a little complex process of generating the key array from the private key but once calculated it can be applied any number of times until the key is changed. So we can ignore it for the once. The algorithm is showing hopeful results for different media inputs.

TABLE 1: IMPLEMENTATION ANALYSIS ON DIFFERENT PLATFORMS

Machine type (on Right)	**Dual Core (2GB RAM, 32-bit OS)**		**Pentium Core i3 (4GB RAM, 32-bit OS)**		**Pentium Core i5 (4GB RAM, 32-bit OS)**	
Media File Type and Size (Below)	*Encryption Time in milliseconds*	*Decryption Time in milliseconds*	*Encryption Time in milliseconds*	*Decryption Time in milliseconds*	*Encryption Time in milliseconds*	*Decryption Time in milliseconds*
Image (3236 KBs)	955 ms	315 ms	646 ms	246 ms	582 ms	200 ms
Audio (4212 KBs)	1029 ms	383 ms	745 ms	353 ms	642 ms	245 ms
Video (7292 KBs)	1290 ms	627 ms	1040 ms	552 ms	802 ms	405 ms

III. COMPARISON WORK

The most commonly used symmetric key encryption algorithms are DES, triple DES, Blowfish and AES. DES is widely used in number of applications but now quick and easy cryptanalysis exist against the DES algorithm. So now triple DES with three cycles of DES algorithm is much more secure than DES. Sandhu et al. [20] have applied the DES cryptographic algorithm along with the MD5 digital signature algorithm for security. Except this the most widely used algorithm in most security applications and by the big cloud providers is AES. In this section we have performed a comparison of our proposed integrated algorithm (discussed above) with the existing AES and DES algorithms for performing encryption and decryption of an image file over Pentium dual core with 2GB RAM and Intel core i5 with 4GB RAM. The results are shown in table 2 given below. It is clear from the results that there is slight difference between the encryption/decryption time taken by the AES and proposed algorithm. The proposed algorithm is taking only few milliseconds extra for this operation but it is much more secure and confidential than the AES algorithm alone. The ordinary cloud providers are using AES algorithm with any of digital signature algorithm like MD5 to maintain integrity of data. This type of digital signature algorithm can also be applied with the proposed algorithm for integrity of data. But DES algorithm is taking much longer time for encryption and decryption processes. So it is obviously an out dated candidate for use. Also triple DES will take even more extra time than DES algorithm so it is not useful to work with it. The proposed algorithm is performing well in less time.

TABLE 2: COMPARISON FOR AES AND DES

Algorithm Applied over image of size 3236 KBs	**Dual Core (2GB RAM, 32-bit OS)**		**Intel Core i5 (4GB RAM, 32-bit OS)**	
	Encryption Time in milliseconds	*Decryption Time in milliseconds*	*Encryption Time in milliseconds*	*Decryption Time in milliseconds*
AES (Advanced Encryption Standard)	900 ms	222 ms	579 ms	92 ms
Blowfish with AES (Our Proposed Integrated Algorithm [18])	955 ms	315 ms	582 ms	200 ms
DES (Data Encryption Standard) [20]	1028 ms	332 ms	639 ms	157 ms

In this section we have compared the proposed integrated algorithm with some other algorithms proposed by some other researchers for multimedia data security over cloud server. Most of them have used asymmetric cryptography RSA (Rivest Shamir Adleman) at the first level to encrypt the public key for transfer to other nodes. As asymmetric algorithms are slow they cannot be applied to larger and multimedia data. According to Nithyabharathi et al. [21] by applying encryption before storing the data and checking authentication before every access, a secure channel can be formed for data transmission. They have applied two famous cryptographic algorithms (RSA and AES) for this purpose. Sharma et al. [22] has implemented a technique with DES and RSA algorithms along with some private keys based authentication mechanism. Guleria et al. [23] have also applied RSA and DES cryptographic algorithms with some access control mechanism for data security and optimization.

Kaur et al. [24] have proposed to implement Elgamal algorithm with Advanced Encryption Standard (AES) algorithm for protecting intellectual property of media contents. Elgamal, as an asymmetric encryption algorithm is not good in performance than RSA. Gupta et al. [25] have proposed an integrated encryption algorithm that is a combination of RSA and Tow-Fish algorithms and a signature verification scheme to enhance security. But Two-Fish is not the encryption standard because it is relatively too slow so we have not considered it. For comparison we have implemented the other proposed algorithms for performing encryption and decryption of an image file over Pentium dual core platform with 2GB RAM and Intel core i5 with 4GB RAM. The corresponding results are shown in table 3 given below. The comparison results shows that the proposed algorithm is performing well than other proposed algorithms. The proposed integrated algorithm can also be implement with RSA algorithm for secure transfer of key. Some other parameters are also covered for the comparison of these algorithms with the proposed algorithm on the scale of good, above average, average, below average and low. The results are displayed in the table 4 given below.

TABLE 3: COMPARISON FOR OTHER PROPOSED

Algorithm Applied over image of size 3236 KBs	**Dual Core (2GB RAM, 32-bit OS)**		**Intel Core i5 (4GB RAM, 32-bit OS)**	
	Encryption Time in milliseconds	*Encryption Time in milliseconds*	*Encryption Time in milliseconds*	*Decryption Time in milliseconds*
Blowfish with AES (Our Proposed Integrated Algorithm [18])	955 ms	579 ms	582 ms	200 ms
RSA (Rivest Shamir Adleman) with AES [21]	1144 ms	582 ms	648 ms	222 ms
RSA with DES [22][23]	1074 ms	639 ms	624 ms	196 ms

TABLE 4: COMPARISON ON THE BASIS OF OTHER PARAMETERS

Algorithms	**Confidentiality**	**Side channel attacks prevention**	**Speed**	**Data integrity**	**Memory usage**	**Performance**
AES	above average	average	good	average	above average	above average
DES	below average	low	below average	low	above average	below average
Triple DES	above average	above average	low	above average	low	below average
RSA with AES	above average	above average	average	above average	average	above average
RSA with DES	above average	above average	average	above average	average	average
RSA with Two-Fish	above average	above average	low	above average	average	average
Elgamal with AES	above average	above average	average	above average	average	above average
Blowfish with AES	good	good	above average	good	average	good

The client's personal media data is always a matter of stake for cloud providers. Thus proposed solution can be implemented for real applications as it is providing a secure channel for transmission while maintaining confidentiality and integrity of crucial multimedia data over the cloud servers. It is having good performance with average memory usage. This solution can also provide prevention from side channel attacks in a better way than AES algorithm alone.

IV. CONCLUSION AND FUTURE SCOPE

Because of limited processing power, limited memory and battery constraints of mobile devices, future requirements of accessing all multimedia data will going to be totally based on cloud computing. Although ordinary cloud providers have to solve many practical issues related to security and confidentiality before its full adoption. As security, integrity and confidentiality are the major factors while storing private media data over the cloud. So to counter these factors the dual level integrated cryptography algorithm is implemented and tested in the proposed work. The implemented scenario performs two levels of encryption/decryption before storing/retrieving media files to/from the cloud server. The proposed solution is implemented and tested for different platforms. Also it is compared for performance and speed with the other proposed solutions. After comparison, it is proved that the proposed solution can be successfully adopted for multimedia cloud environment. Besides securing confidentiality and integrity of data, it also protects against the side channel attacks as input files are not stored in the readable formats over the cloud. Further the work can be extended by adding some authentication mechanisms to it.

REFERENCES

[1] G. Boss, P. Malladi et al., “Cloud computing, 2009”, http://www.ibm.com/developerswork/websphere/zones/hipods/ library.html

[2] L.M. Vaquero, L. Rodero, J. Caceres, M. Lindner, “A break in the clouds: towards a cloud definition”, In: ACM SIGCOMM, editor, Computer communication review 2009, New York: ACM Press, 2009, pp. 50–55

[3] J. Chea, Y. Duanb et al., “Study on the security models and strategies of cloud computing”, 2011 International Conference on Power Electronics and Engineering Application, Elsevier, Procedia Engineering 23, 2011, pp. 586 – 593

[4] R. Buyya, C. S. Yeo, and S. Venugopal, “Market-oriented cloud computing: Vision, hype, and reality for delivering its services as computing utilities”, in Proc.10th IEEE, Int. Conf. High Performance Computing and Communications, 2008, pp. 5-13

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph et al., “Above the clouds: A Berkeley view of cloud computing”, EECS Dept., Univ. California, Berkeley, No. UCB/EECS-2009-28, 10 Feb, 2009

[6] T Nagajyothi, S. Abdul Moeed, “An Automated Resource Allocation for QoS Provision in a Cloud-Based Multimedia Storage System”, International Journal of Research (IJR), Vol. 2, Issue 08, August 2015, pp. 69-74

[7] S. Harnal, R.K Chauhan, “Issues & Perspectives with Multimedia Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol. 6, Issue 11, November 2016, pp. 174-180

[8] ABI Research, Mobile cloud computing [Online]. Available: http://www.abiresearch.com/research/1003385-Mobile+Cloud+Computing, July 2009

[9] Q. Zhang, Z. Ji, W. Zhu, and Y.-Q. Zhang, “Power-minimized bit allocation for video communication over wireless channels”, IEEE Trans. Circuits Syst. Video Technol., Vol. 12, No. 6, June 2002, pp. 398–410

[10] K. Kilkki, “Quality of experience in communications ecosystem”, J. Universal Computer Sci., Vol. 14, No. 5, 2008, pp. 615–624

[11] S. Harnal, R.K Chauhan, “Multimedia Support from Cloud Computing: A Review”, International Conference on Microcom-2016, IEEE, 23-25 Jan, 2016

[12] P. Bindhu Shamily, S. Durga, “A Review on Multimedia Cloud Computing, its Advantages and Challenges”, Vol. 1, Issue 10, December 2012, pp. 130-133

[13] C.T. Huang, Z. Qin, C. J. Kuo, “Multimedia Storage Security in Cloud Computing: An Overview”, Multimedia Signal Processing (MMSP), IEEE 13th International Workshop, 17-19 Oct. 2011, pp. 1 - 6

[14] W. Stallings, “Cryptography and network security: principles and practice”, Prentice Hall, 2010

[15] V. B. Patil et. al. “Implementation of AES algorithm on ARM processor for wireless network”, International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 2, Issue 8, August 2013, pp. 3204-3209

[16] S. More, R. Bansode, “Implementation of AES with Time Complexity Measurement for Various Input”, Global Journal of Computer Science and Technology: E Network, Web & Security, Publisher: Global Journals Inc. (USA), Vol. 15, Issue 4, Version 1.0, 2015, ISSN: 0975-4172, pp. 11-20

[17] Q. Zhang, Z. Ji, W. Zhu and Y.-Q. Zhang, “Power-minimized bit allocation for video communication over wireless channels”, IEEE Trans. Circuits Syst. Video Technol., Vol. 12, No. 6, June 2002, pp. 398–410

[18] S. Harnal, R.K. Chauhan, “Hybrid Cryptography to Maintain Integrity of Data in Multimedia Cloud Environment”, International Journal of Emerging Technology and Advanced Engineering (IJETAE), Volume 7, Issue 9, September 2017, pp. 669-675

[19] M. A. Mushtaque, “Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security”, International Journal of Computer science & Engineering, Vol. 2, Issue 4, April 2014, pp. 76-82

[20] M. S. Sandhu, S. Singla, “An Approach to Enhanced Security of Multimedia Data Model Technology Based on Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 7, July 2013, pp.724-728

[21] P. V. Nithyabharathi, T. Kowsalya, V. Baskar, “To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES”, International Journal of Science, Engineering and Technology Research (IJSETR), Vol. 3, Issue 2, February 2014, pp. 341-345

[22] A. Sharma, V. Gupta, “Crossbreed Algorithm to Enhance Security for Multimedia Content: An Overview”, International Journal of Computer Science and Communication Engineering, Volume 2, Issue 2, May 2013, pp. 71-75

[23] S. Guleria, S. Vatta, “To Enhance Multimedia Security in Cloud Computing Environment using Crossbreed Algorithm”, International Journal of Application or Innovation in Engineering & Management, Vol. 2, Issue 6, June 2013, pp. 562-568

[24] R. Kaur, G. Kaur, “Multimedia Cloud Computing an Emerging Technology: Survey”, International Journal of Engineering And Computer Science, Volume 4, Issue 3, March 2015, pp. 11045-11049

[25] P. Gupta, A. Kaur, “An Enhanced Security Technique for Storage of Multimedia Content over Cloud Server”, International Journal of Engineering Research and Applications, Vol. 3, Issue 4, Jul-Aug 2013, pp.2273-227