International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Hybrid Cryptography based E2EE for Integrity & Confidentiality in Multimedia Cloud Computing

Shilpi Harnal, R.K. Chauhan

Abstract- Cloud Computing has become a desirable state for the mobile users by providing anytime and anywhere access to various services and resources. Likewisemultimedia data such as audio, images, video and gif files covers the maximum part of the network traffic, as most of the data shared, produced, processed and stored through numerous sources such as smart phones, computers, sensor networks, satellites, medical records etc. is of multimedia type. Such form of data requires huge computing power and storage capacities along with the major security constraints. Mobile devices with limited configuration and low computing powers are not able to match with the high level computing and manipulations required by costly multimedia softwares. That's why demand for the Multimedia Cloud Computing came into frames. As multimedia data has distinct computing, storage and security constraints, this field has become anemerging and latest area of research. Many researches have also proposed separate architectures for Multimedia Cloud Computing. Security, integrity and confidentiality of private and secret media files is always a matter of stake for cloud users as well as for cloud providers. For multimedia cloud security concerns, cryptography is a guaranteed solution.This paper has discussed about the various needs and challenges faced by the multimedia cloud providers. This work has also proposed a hybrid cryptography algorithm based end-to-end encryption (E2EE) approach to maintain integrity and confidentiality in multimedia cloud computing environment. The second last section provides a performance analysis for the algorithm in terms of tables and graphs to justify the results.

Keywords- Multimedia Cloud, Encryption algorithm, Integrity, Confidentiality, Security, Multimedia data, End-to-end encryption.

I. INTRODUCTION

Cloud computing is a complete Internet based architecture[1]. According to NIST i.e. National Institute of Standards and Technology[2], cloud computing allows convenient and demand basedaccess to configurable and scalable computing resources (e.g., storage, servers, networks, softwares and other services). In other words, several computing and storage services are provided by the emerging cloud technology through internet based on the Service Level Agreements (SLAs) [3][4]. As a result the organizations are relaxed from the burden of purchasing expensive hardware devices, computational devices, softwares and licenses.Now they can outsource all resources and services from third party cloud providers with the facility of anytime and anywhere access on pay per usage basis at high speed [5].

Manuscript published on 30 August 2019.
***Correspondence Author(s)**
Er. Shilpi Harnal, (Research Scholar), Department of Computer Science and Application, Kurukshetra University, Kurukshetra, India
Dr. R.K. Chauhan, (Professor), Department of Computer Science and Application, Kurukshetra University, Kurukshetra, India

Thus, even small organizations can have a good start-up with minimum expenditure. Some of the examples of important cloud service models are Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Some of the famous cloud service providers (CSPs) are Google Apps, Salesforce, AmazonEC2, Amazon's S3, Windows Azure etc.[6]. In current scenario most of the network traffic comprises of multimedia data, as maximum of generated, edited, stored and shared data via various smart devices (e.g. laptops, smart mobiles, cameras, tablets etc.) is of multimedia type (e.g. audio, images, gifs and video files etc.). But all types of smart devices are provided with limited storage, battery life and computing capacities. Thus, only option left with these limited smart devices is to adopt cloud services for heavy and expensive media applications, media editing and storage services [7]. Next these requirements of accessing, storing, sharing, editing, computing and transmitting media data over internet by billions of users raises Quality of service (QoS) and Quality of experience (QoE) issues in terms of bandwidth, throughput, jitter and delay. Also the security of private media data of clients in terms of confidentiality and integrity is a major concern of stake. These requirements would be a bottleneck for an ordinary cloud service providers and can leads to unsatisfied experience for clients[8] [9]. For better user's experience and in order to scale up to these requirements separate setup is required with huge storage capacity, fastest graphical processing units (GPUs), faster network connectivity and classic security aids are mandatory unlike ordinary cloud providers and content delivery networks (CDN) like Dailymotion, YouTube etc. Thus multimedia cloud can frees the user from the processes like installation, purchasing, maintenance, licensing and continual upgrades of heavy and expensive multimedia softwares. Above this, multimedia cloud service also saves battery life of mobile devices by transferring all heavy editing and computation at remote servers. Some examples of rich multimedia applications includes face recognition system, speech recognition system, physical simulation, mobile augmented reality, object and pose identification system etc.

A. Need of Multimedia Cloud Computing

Opting for media cloud can result in 85 percent savings of I.T energy. Moreover, cloud computing is in huge demand for providing various rich multimedia applications and services through the internet and wireless mobile networks. In nutshell, following are the key reasons for high demand of cloud resources:

- *Limited Hardware:* As discussed earlier, mobile devices cannot match the high resource requirements of multimedia files with their limited resource constraints. Thus, it raises the need of media cloud servers for media files handling[10].

- *Huge Demand of Media Resources:* The demand of media contents such as images, gifs, audio files, videos files, internet gaming, presentations, sensor networks, multimedia mails and medical data etc. are already dominating internet traffic and this trend is going to raise rapidly in future [11].
- *Enhancement through Cloud:* It is only the cloud that can provide distributed access on pay as you go basis, side by reducing burden of owning the heavy multimedia applications and resources for the user.

Thus, Multimedia is indulged as a crucial service in cloud computing to provide a better experience through high quality media services.Figure 1 is depicting a general idea for multimedia cloud computing.

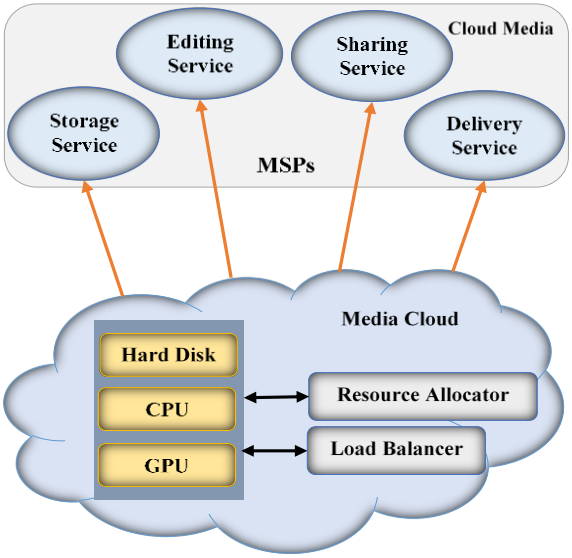

Figure 1: General framework for Multimedia Cloud

B. Challenges for Multimedia Cloud Computing

Multimedia cloud incorporates a major issue of security, with the extension of cloud storage for storing multimedia files such as user's personal photographs, videos and other media files[12]. Multimedia cloud has turned into a major research problem. Several researches have proposed many solutions for enhancement of storage security of multimedia cloud computing by the usage of authentication checks, certifications and encryption algorithms etc. in last few years. Intensive multimedia data accessing, storing and processing is a great challenge for cloud service providers in terms of data integrity, confidentiality, authentication, access control and non-repudiation. Main challenges for computation and storage of multimedia data are mentioned as follows:

- *Multimedia contents and services heterogeneity:* The cloud has to deal with the heterogeneity of various multimedia contents and services required by the users such as photo/video editing and sharing, video conferencing, multimedia streaming, video transcoding etc. The providers have to support all distinct services while maintaining good QoS and QoE for each user.
- *QoS heterogeneity:* Each cloud service provider have to deal with the various types of QoS requirements depending on the different types of multimedia services required by the cloud client.
- *Networks & Devices heterogeneity:*The media cloud provider shall manage efficient service delivery to various types of devices (e.g. smart phones, laptops, TVs, kindle etc.) connected through different types of networks (e.g. Internet, wireless local area network (WLAN) and wireless network) and having distinct network features (e.g. bandwidth, delay and jitter).
- *Security Concern:* It's the first thing that gains everyuser's attention as they have their personal and crucial media data stored over a third party cloud provider. This enhancement is possible only with the help employing strong authentication policy, better access control policies and proper encryption techniques.
- *Energy Consumption: P*ower consumption has become a serious burden over energy resources with increased media network traffic.

For an ordinary cloud provider media data handling is always a bottleneck due to rigid QoS and QoE requirements for multimedia traffic. The developed I.T strategies believes that secure communication can be provided with the cryptography strategy. There are 2 types of cryptography systems, i.e. Symmetric (Secret/Private key) and Asymmetric (Public key).A single shared secret/private key is used by both sender and receiver for symmetric key encryption scheme. And a pair of keys (Private and Public keys) are maintained by both parties in case asymmetric encryption technique. For asymmetric encryption technique each user also manages public keys of all other parties along with its own public and private key pair. But symmetric cryptography technique is 1000 times faster than asymmetric technique as it comprises of more computations than symmetric process. Also asymmetric technique is more prone to attacksand perform better for small size messages only [13] [14]. Generally a combination of both techniques is always preferable, in which asymmetricencryption is used for sharing of secret/private key only and symmetricencryption is applied to over data.

C. Need of End-to-End Encryption (E2EE) Technique

However, even the servers of most popular cloud service providers (including Google, Yahoo, Amazon, Dropbox and Microsoft Outlook 365) are vulnerable to attacks because they operate on unencrypted data[15]. No doubt, cloud provides enormous benefits but they are always tempting target of attackers being a centralized repository of information. E.g. recently a billion user accounts were compromised from the Yahoo server. In order to address this issue some cloud providers started using encryption for the data stored in the storage media when not in use this phenomenon is known as encryption-at-rest. This reduces the risk of data breaches at server storage. Even Google follows multi-layer AES (256 bits) encryption policy for encryption-at-rest. But still attackers can steal the data in transit. These types of attacks are well known as Man-in-the-Middle attacks. To prevent this only End-to-End Encryption (E2EE)can be a solution. Now some application providers have started providing E2EE like WhatsApp, TextSecureand Gmail etc.

Like other email providers Gmail support only Transport Level Security (TLS) end-to-end encryption, where data is not accessible during transmission but still it is visible to the server. Because of this now many cloud users have started using third party apps to encrypt their private and crucial data before storing it over the cloud. Such type of applications are known as domain client (DC) applications. Y. Song and H. Kim in [16] have proposed anEncrypted Cloud (EnCloud), that is a system for providing end-to-end encryption between the cloud users and application providers to facilitate their tasks and to maintain enable user's trust. Thus, it is clear from the above discussion that cloud services and applications are vulnerable without end-to-end encryption.Numerous researchers have proposed several architectures, cryptography methods and algorithms for multimedia data security. Wenwu Zhu et al. [17] has presented multimedia cloud computing in terms of cloud media and media cloud as shown in figure 1. Abdel-Karim[18] has implemented and performed a comparison for different sizes of data blocks in C# among most common symmetric encryption algorithms like AES, Blowfish, DES, 3DES. Based on comparison results he has concluded that Blowfish algorithm has performed better than others. Also blowfish is a better candidate to be used for media data encryption/decryption as it faster and has not proved against any cryptanalysis till now. This work has proposed a secure hybrid symmetric algorithm with random generation of secret key for multimedia data cryptography that is an improvement of blowfish algorithm to enhance security while storing/retrieving text and other media files (e.g.images, audio, gifs, video files) to/from the cloud server. Earlier blowfish was meant to be used for text files only. This proposed approach is based on end-to-end encryption (E2EE) as the data is encrypted at client end before transmitting to server and also decrypted at client site after retrieving from cloud server.This hybrid approach can work for any type of media files and provides high level of security for personal multimedia files of users. The followed section presents the approach and methodology of proposed algorithm. The third section will projects the performance and results in the form of graphs. The last section presents the future aspects and conclusion of work.

II. PROPOSED APPROACH

The survey is performed to select effective algorithm having wide acceptability, good performance and moderate complexity level to provide protection against various side channel attacks and data security for multimedia cloud environment. As it is difficult to track side channel attacks, a hybrid cryptography algorithm proposed here can be an effective solution. This proposed work is an improvement of blowfish algorithm for an effective solution. Blowfish was invented by Bruce Schneier in 1993. He is president of an organization specialized in computer security and cryptography and also one of the leading cryptologist. It's an unpatented symmetric key algorithm with a key multiple of 32 bits. This algorithm is not vulnerable to any proved attacks and no effective cryptanalysis has proved for it till now[19] [20].This work is based on the symmetric/private key encryption algorithm as symmetric cryptography is far suitable than asymmetric cryptography for large amount of data. Well known symmetric algorithms such as Data Encryption Standard (DES) or Advanced Encryption Standard (AES) can also be an option for multimedia data by converting data bit stream as a binary sequence. DES is used by Advanced Encryption Standard (AES) since 1977 [21]. Although DES is not much secure as inexpensive and quick cryptanalysis already exist for this algorithm.Later in the year 2000, to match the security requirements of network the DES was replaced by AES. AES was defined by the National Institute of Standards and Technology (NIST) of the United States and was the better alternative. But AES has some vulnerabilities and time constraints associated while dealing with files other than the text format like multimedia files. Being a symmetric-key block cipher algorithm blowfish is proved as fast, secure and free alternative for various cryptography problems.

A. Proposed Framework

In this proposed work we have implement a secure hybrid symmetric key algorithm that is an improved blowfish algorithm for multimedia cloud computing to maintain integrity of the data.Also asymmetric/public key algorithm is applied over the symmetric secret key with the help of public and private key pairs to maintain the confidentiality and authentication between two parties. The cloud is a client-server based architecture. The general model of proposed framework for multimedia cloud computing is depicted in figure 2, where server side consists of huge databases, virtual servers, content manager for application of various constraints, analysis module and security module that implements the hybrid algorithm along with an asymmetric key algorithm. The client side comprises of only media content player and security module like in server side. In proposed framework we have E2EE to preserve integrity and confidentiality of data during transmission over unsafe networks. That's why we have deployed hybrid algorithm at both server and client end. For pure E2EE system encryption/decryption is done at client end only. Pure E2EE is suitable for media cloud storage services only. But cloud server need to access stored media files as per requirements of client in multimedia cloud computing to access rich multimedia applications and media editing softwares for stored media files. If a client raises a request for any multimedia data access, the following steps are performed in order:

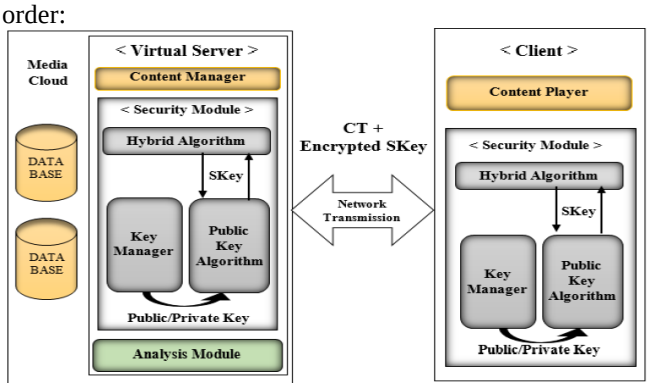

Figure 2: Proposed framework for multimedia cloud with E2EE

Note: encryption/decryption algorithm have two parameters: first is the key and second is data.

- Client made a request for any media data.
- The content manager matches the request for various constraints. If satisfied then proceed further.
- Analysis module analysis the availability of servers and other parameters.
- The key management module make a set keys available such as secret key for hybrid algorithm (SKey), public key of server (PUs), private key of server (PKs) and public key of client (PUc).
- Then the security module fetches the required data (PT) from the database and
  encrypt it with the secure hybrid algorithm following symmetric key cryptography with the
- help of SKey provided to generate cipher text (CT), i.e. CT=Hy.En(SKey, PT). This will ensure integrity of data for both sender and receiver.
- The asymmetric/public key algorithm is used to encrypt the secret key (SKey) with the public and private keys, such as:
  - For confidentiality, firstly SKey is encrypted with the public key of client (PUc), i.e En(PUc, SKey). So that only the client will be able to decrypt it with the matching private key (PRc).
  - For authentication, the SKey is again encrypted with the private key of server (PKs), to prove that the message has come from an authentic source, i.e. En(PRs, En(PUc, SKey)). The client can decrypt it with the available public key of server (PUs). This private key encrypted SKey also serves the purpose of server's digital signature for client.
- The hybrid encrypted data and encrypted SKey is sent to client, such as:

CT= Hy.En(SKey, PT) and En(PRs, En(PUc, SKey)).

- The reverse process or decryption is performed at the client end. The secret key (SKey) is recovered firstly using asymmetric algorithm and then the required data (PT) is decrypted using hybrid algorithm,

  i.e. SKey = Dn(PUs, Dn(PRc, SKey)) and then PT=Hy.Dn(SKey, CT).

For hybrid algorithm randomly generated secret key is applied always for security reasons. The above process shows that data is transmitted in encrypted form (CT) and can only be decrypted by other party. This approach provides high level security for stored as well as transmitted media files from one end to another end, while preserving confidentiality, integrity and authentication at both ends. The detailed process of applied encryption and decryption of hybrid algorithm is discussed in further sections.

B. Implementation Methodology

To implement the proposed hybrid algorithm C#, JAVA and C++ are the most suitable languages and corresponding compilers canbe Eclipse, Code Blocks or NetBeans. The proposed hybrid cryptography algorithm isimplemented using JAVA and run using the Eclipse and command line interface over Intel Core dual core based workstation with 2GB of RAM. The setup is implementedand tested for various types and sizes of multimedia files.

C. Proposed Algorithm

The hybrid algorithm mentioned in proposed framework is an improvement of blowfish algorithm anda symmetric/private key based approach. This improved blowfish algorithm is more complex and also it can work with any type of files such as text, audio, images and video etc. for media cloud. The proposed algorithm for multimedia cloud computing operates with randomly generated 128 bits secret key (SKey) and it includes 16 rounds. The key can also be provided manually but that will not be of much use. The algorithm is based on the 64-bit block cipher model[6] except for the first and last steps.

The initial setup of the algorithm comprises of following steps:

- *Byte Streaming:* The input media files is streamed into array of bits.
- *K-Array initialization:*The 128 bits SKey is expanded to 18 keys each of 32-bits in size, out of these 16 keys goes as input to each round and 2 keys are used for the lasttwo XOR operations performed after all the rounds. This expanded key bits are stored in a K-Array (K1, K2,…,K18).
- *The S-Box transformation:*This function uses four two-dimensional (4 X 64) pre-initialized S-Boxes as shown in figure 4. Each S-Box takes 8-bits (b1, b2, …, b8) as input to generate 32 bits of output. From these 8-bits, combination of first and last bit that is b1 and b8 is used to select the row index and combination of remaining six bits b2, b3, .., b7 is used to mark the column index from 64 available columns. The intersection of these indexed row and column represent the 32-bits of output.
- *R*-Array *initialization:*A random array named as R-Array in the algorithm, is pre-initialized for the last XOR operation performed with the final streamed byte array of complete media file generated after all the rounds.

Steps of the proposed hybrid algorithm for encryption process Hy.En (SKey, PT) are as follows (also presented in figure-3):

- Input media files is streamed into bits.
- Initialize all the arrays as mentioned above: 18 K-Arrays from 128-bits SKey, 1 R-Array and 4 S-Boxes.
- The initialization phase comprises of N left shift operations for encryption and N right shift operations during decryption.
- After this the algorithm has 16 rounds for each 64 bits block to pass throughsimple encryption process that includes XOR operations and S-Box transformation function for each round as shown in figure 3.
- Each block X of 64 bits is divided into two 32-bits blocks say XL (left 32 bits) and XR (right 32 bits) and passed as input to round 1. The following 4 steps are repeated for each i^{th} round of total 15 rounds:
  - XLi XOR Ki : XLi is XORed with expanded 32-bits key Ki (round specific).
  - S-Box (XLi XOR Ki) : The XoRed 32-bits are passed through the S-Box transformation function.
  - (S-Box (XLi XOR Ki)) XoR XRi : The resulting 32-bits from S-Box transformationare XoRed with XRi.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- XLi+1 = XRi and XRi+1= XLi : Initialization of XLi+1 and XRi+1 for next (i+1)th round.

- For the last 16th round first 3 steps are processed in order and then XL16 is XoRed with K17 i.e. (XL = XL16 XoR K17) and XR16 is XoRed with K18 i.e. (XR = XR16 XoR K18).

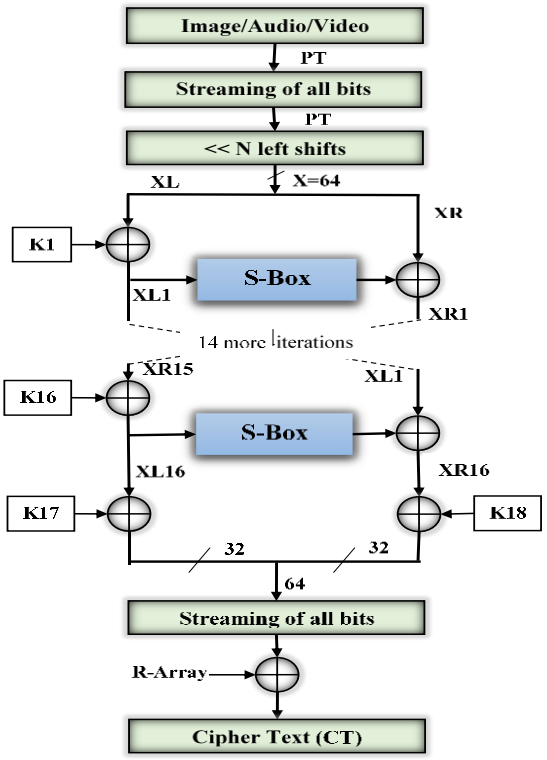

Figure 3: Proposed Hybrid Algorithm

- After these rounds all the blocks of 64-bits are streamed together and XoRed with the pre-initialized R-Array to generate the final cipher text (CT).

The decryption algorithm PT = (Hy.Dn(SKey, CT)) is exactly the reverse of encryptionwith secret key (SKey) and cipher text (CT) as input. Such as N right shifts operations are performed instead of N left shifts and Expanded key arrays (K1, K2, … , K18) are applied in thereverse order of encryption.

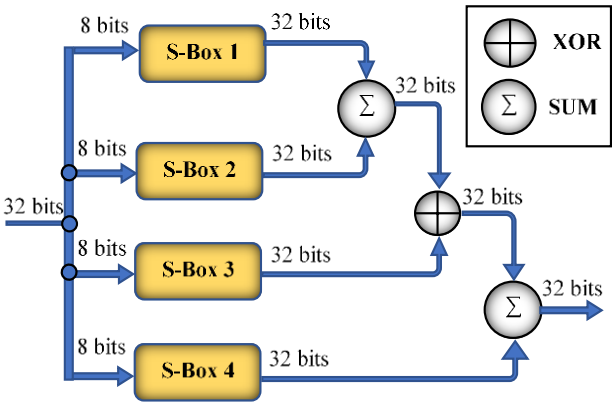

Figure 4: S-Box Transformation Function

III. RESULTS, ANALYSIS AND BENEFITS

A. Results&Analysis

This section analyze the time taken by the proposed algorithm to encrypt and decrypt multimedia data of different types and sizes. Thus, the algorithm can work with variety of files of different sizes such as images, audio or video files. For each such input the algorithm is showing hopeful results. The table 1 here, represents time taken by the algorithm for encryption and decryption of various types and sizes of sample media files provided as input. The size of the input files are measured in kilobytes (KBs) units and corresponding encryption and decryption time taken is measured in milliseconds (MS). As stated, this implementation is performed over Pentium dual core workstation with 2GB of RAM, the results will be more improved for advanced processors.

Table 1: Time taken for Encryption/Decryption

Sr. No.	File Type	File Size in KBs	Encryption Time (MS)	Decryption Time (MS)
1	Image	3233	208	165
2	Image	4830	295	235
3	Image	6308	383	287
4	Audio	4209	264	193
5	Audio	6374	392	291
6	Video	7289	419	320
7	Video	9171	524	401
8	Video	11305	662	516

The algorithm is giving hopeful results for each type and size of media files. The encrypted files are successfully tested to be stored over the cloud server. The column/bar graphs shown in figure 5 here are presenting the encryption and decryption time taken by the algorithm over different types and sizes of media files (audio, image and video files). The x-axis represents range for time and y-axis represent the type & size of media file input. Here the orangebars represents the encryption timetaken and green bars shows the decryption time taken for different input files with hybrid algorithm.

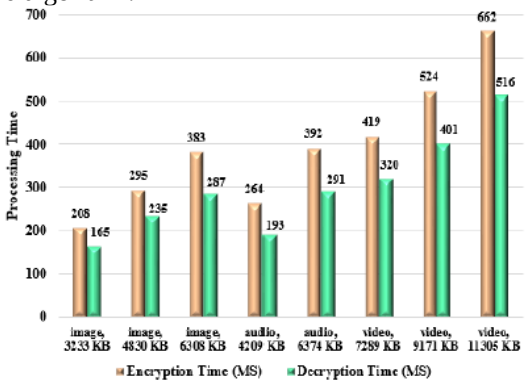

Figure 5: Time taken for Encryption/Decryption

B. Comparison with other Algorithms

AES, DES, triple DES and Blowfish are the most commonly used and popular and private/symmetric key algorithms. As discussed, easy cryptanalysis exist against DES.

But triple-DES with three cycles is very secure and used in some applications. The most popular among cloud service providers is AES algorithm and used in many security applications. Blowfish is faster than others but it is not an algorithmic standard. Many authors have proposed to apply double level of encryption using Blowfish and AES algorithms in integrated manner [6]. As per requirement of E2EE for multimedia cloud computing it is clear that, only a faster algorithm can serve
the purpose for performing encryption/decryption at client/server end for large media files. In this section we have performed a comparison of our proposed hybrid algorithm with these algorithm for performance measurements.

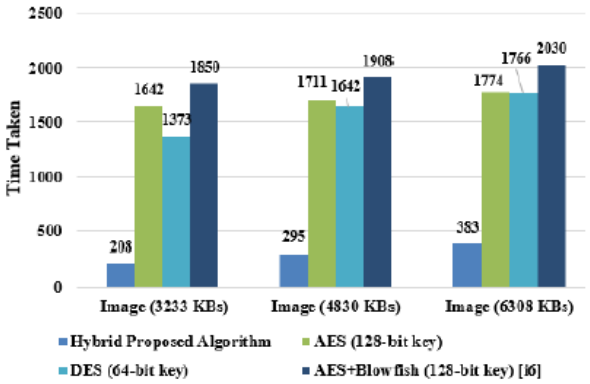

Figure 6: Comparison for Encryption Time in MS

The experiment is performed only for the image files of various sizes. The experiment results are very satisfactory for the proposed hybrid algorithm as depicted in Table-2 given below. The results are also presented separately in the form of column/bar graphs shown in figure 6 and figure 7.It is clear from table and graphs that the proposed hybrid algorithm is much faster and better alternative for encryption/decryption than other algorithms.

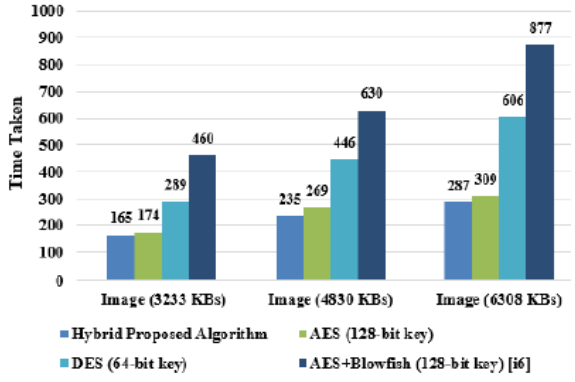

Figure 7: Comparison for Decryption Time in MS

Table 2: Results of Comparison with different algorithms for image files

Image File Size in KBs	Encryption time in Milliseconds (MS)				Decryption Time in Milliseconds (MS)			
	AES (128-bit key)	DES (64-bit key)	AES+Blowfish (128-bit key) [i6]	Hybrid Proposed Algorithm	AES (128-bit key)	DES (64-bit key)	AES+Blowfish (128-bit key) [i6]	Hybrid Proposed Algorithm
3233	1642	1373	1850	208	174	289	460	165
4830	1711	1642	1908	295	269	446	630	235
6308	1774	1766	2030	383	309	606	877	287
Average Time	1709	1593.67	1929.33	295.33	250.67	447	655.67	229
Throughput	2.8	3.01	2.48	16.22	19.11	10.72	7.31	20.92

Also the proposed hybrid algorithm outperforms in terms of throughput comparison for both encryption and decryption. The throughput (file size in KB/Time in MS) results are presented through the line graphs in figure 8.

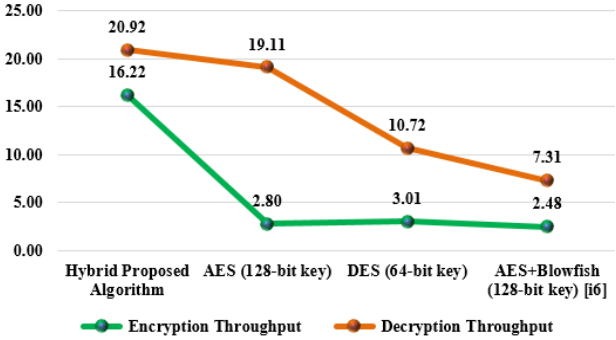

Figure 8: Throughput Comparison for encrypt/decrypt

Comparison can also be extended for some other parameters in terms of security and maintaining client's trust for cloud. The comparison results are demonstrated in Table-3 given below and the algorithms are scaled for low, good, average etc. on the basis of results of experiment performed and the results of other researchers.

C. Benefits

The approach is proposed for multimedia cloud computing is providing E2EE for end users. If implemented it can provide the following benefits for the end users:

- *Authentication:* The proposed scheme guarantees complete authentication for both parties as only authorized party can decrypt the secret key (SKey) using their own private key. Further SKey can be used to encrypt the data. This acts as Digital Signature.
- *Confidentiality and Integrity:* The proposed algorithm is also securing most required and critical issues for every cloud providers i.e. confidentiality and integrity. The data is viewed by authorized user only for confidentiality and no tempering of is possible during transmission to maintain integrity.
- *Scalability and Availability:*The approach is flexible and scalable enough according to customer's requirements on pay per usage basis.
- *Prevention from attacks:* The proposed scheme can be implemented for multimedia cloud environment to provide protection against many attacks like man-in-middle attack, non-repudiation, side channel attacks, brute force attack etc.
- End-to-End Encryption: The main feature of the proposed system is E2EE for securing the private and personal media data of users during transmission.
- *High Performance:* The results presented in earlier section proves that the proposed algorithm has performed better than other algorithms discussed over here.

IV. CONCLUSION AND FUTURE ASPECTS

Only cloud can handle the future requirements of accessing multimedia files because of limited capabilities of low configured mobile devices.

But cloud and user has many privacy and security related aspects that requires special attention. Here the work has discussed the challenges faced by ordinary cloud provider to handle multimedia files. Although, ordinarycloud providers need to manage many practical issues related to authentication,confidentiality, integrity and security before the full adoption of multimedia cloud. Also a framework is discussed on how multimedia data can be easily managed through media clouds. The security of stored personal media files is the highly demanding feature for every media cloud provider. The work has proposed a secure hybrid cryptography approach along with end-to-end encryption scenario to provide a safe storage and safe transmission for media files over the internet. The hybrid algorithm is tested and compared against the other proposed and existing algorithms. The results are satisfactory to many extends. If implemented the proposed approach can give fast and better results in terms of performance and security.

Table 3: Comparison on the basis of other parameters

Algorithm	Confidentiality	Attacks Prevention	Speed	Data integrity	Memory usage	Performance
AES	above average	good	good	excellent	good	above average
DES	low	low	below average	low	below average	below average
Triple DES	above average	above average	low	good	average	average
Blowfish with AES	average	good	below average	good	average	average
Hybrid algorithm with Public key encryption	good	excellent	excellent	excellent	good	good

REFERENCES

1. Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, NIST Special Publication, September 2011.
2. Shilpi Harnal, R.K. Chauhan, “Multimedia Support from Cloud Computing: *A Review”, International Conference on Microcom-2016, IEEE*, NIT, Durgapur, Jan, 2016
3. R. Buyya, C. S. Yeo, and S. Venugopal, “Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities,” in Proc.10th IEEE Int. Conf. High Performance Computing and Communications, pp. 5–13, DOI: 10.1109/HPCC.2008.172, 2008.
4. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R.Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. EECS Dept., Univ. California, Berkeley, No. UCB/EECS-2009-28, 10 Feb, 2009 [Online]. Available: http://radlab.cs.berkeley.edu/
5. Sheetal Deshpande, Deepali D. Gatade, “A Survey and Analysis for Accountability and Privacy of Shared Data in the Cloud”, National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2013), International Journal of Computer Applications (IJCA), pp. 22-27, 2013.
6. Shilpi Harnal, R.K. Chauhan, “Hybrid Cryptography to Maintain Integrity of Data in Multimedia Cloud Environment”, International Journal of Emerging Technology and Advanced Engineering, Vol. 7(9), Sep. 2017, Pg 669-675.
7. ABI Research, Mobile cloud computing [Online]. Available: http://www.abiresearch.com/research/1003385-Mobile+Cloud+Computing, July, 2009.
8. 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, pp. 398–410, June 2002.
9. K. Kilkki, “Quality of experience in communications ecosystem”, J. Universal Computer Sci., Vol. 14, No. 5, pp. 615–624, 2008.
10. J. Flinn, Cyber Foraging: Bridging Mobile and Cloud Computing via Opportunistic Offload. Morgan & Claypool Publishers, 2012.
11. Reza Farahbakhsh, Angel Cuevas, Ruben Cuevas et al., “Understanding the evolution of multimedia content in the Internet through BitTorrent glasses”, IEEE Network, November-December 2013, Vol. 27, pp. 80-87, DOI: 10.1109/MNET.2013.6678931.
12. Chun-Ting Huang, Zhongyuan Qin, C.-C. Jay Kuo, “Multimedia Storage Security in Cloud Computing: An Overview”, Multimedia Signal Processing (MMSP), IEEE 13th International Workshop on multimedia signal procevving, pp. 1 - 6, DOI: 10.1109/MMSP.2011.6093775, 17-19 Oct. 2011.
13. Edney, “Real 802.11 Security: Wi-Fi Protected Access and 802.11i”, Addison Wesley, 2003.
14. Hardjono, “Security in Wireless LANS and MANS”, Artech House Publishers, 2005.
15. https://www.preveil.com/blog/cloud-services-vulnerable-without-end-end-encryption/
16. Youngbae Song, Hyoungshick Kim et al., “A PrivateWalk in the Clouds: Using End-to-EndEncryption between Cloud Applications in a Personal Domain”, C. Eckert et al. (Eds.): TrustBus 2014, LNCS 8647, pp. 72–82, Springer International Publishing Switzerland 2014.
17. Wenwu Zhu, Chong Luo, Jianfeng Wang, and Shipeng Li, “Multimedia cloud computing”, IEEE SIGNAL PROCESSING MAGAZINE, vol. 28, Issue. 3, pp. 59-69, DOI: 10.1109/MSP.2011.940269, MAY 2011
18. Abdel-Karim Al Tamimi, Yarmouk University, “Performance Analysis of Data Encryption Algorithms”,http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html
19. Bruce Schneier, "Applied Cryptography”, John Wiley & Sons, Inc 1996.
20. Aamer Nadeem et al., “A Performance Comparison of Data Encryption Algorithms”, IEEE, 2005.
21. Shraddha More & Rajesh 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.

AUTHORS PROFILE

Er. S. Harnal pursed Bachelor of Technology and Master of Technology from Kurukshetra University in year 2008 and 2012 respectively. She is currently pursuing Ph.D. and working as Assistant Professor in Computer Science and Engineering Department of Seth Jai Prakash Mukand Lal Institute of Engineering & Technology. She has published around 10 research papers in reputed international journals and conferences including IEEE. Her main research work focuses on Cryptography Algorithms, Network Security, multimedia cloud computing, Cloud Security and Privacy.

Dr. R.K. Chauhan is Professor in Department of Computer Science & Applications, Kurukshetra University, Kurukshetra since 1989. He has pursed Ph.D in the year 2000, Master of Science in year 1993 and Master of Computer Applications in year 1987. He has vast experience in research and teaching. He has guided many research scholars and also has published more than 200 research papers in various national/international journals and conferences of repute. His main research work focuses on Advance Database, Data Mining & Warehousing, Mobile Computing, Ad-hoc Networks, Software Engineering and Cloud Computing.