A Crossbreed approach to Enhanced Security of Multimedia Data using SKIP JACK and Elgamal Algorithm

Gemini Garg
Chandigarh Engineering College
Landran

Jaspreet Kaur
Chandigarh Engineering College
Landran

ABSTRACT

Due to the new development in computer networking expertise, delivery of the digital multimedia content through the internet is huge. However, the increase number of the digital credentials, all inclusive availability, and the multimedia dispensation tools of Internet entrance has created a very easy medium for exclusive rights trickery and out of manage distribution of multimedia contented. A most important constraint now is to protect the thinker property of multimedia content in multimedia organization. So, in this document multimedia protection will be providing using SKIP JACK and Elgamal algorithm. The full implementation is done in .NET structure.

Keywords

Multimedia cloud security, SKIPJACK, Elgamal, Cloud Computing, Video, Text.

1. INTRODUCTION

Cloud computing is a service dispense over the internet for computing, data entrance and cloud storage by generate scalability, flexibility and fewer cost. Examine needs gracefully [1].They is number of data format that can be characterized as multimedia data types. These are generally the elements which are the construction blocks of general multimedia platform, situation, or integrating tools. They describe the necessary type as auditory, text, imagery, graphic objects and the video [2].The main difficulty revolves around the Cloud security and the suitable execution of cloud over the network [3]. To keep user's data secure on cloud, data encryption using Advanced Encryption Standard algorithm and Elgamal algorithm has been planned in this work. The prototype of the model carry out the relation $m \leftrightarrow 1 \leftrightarrow n$ .The below figure shows the cloud computing organization arrangement [4,5].

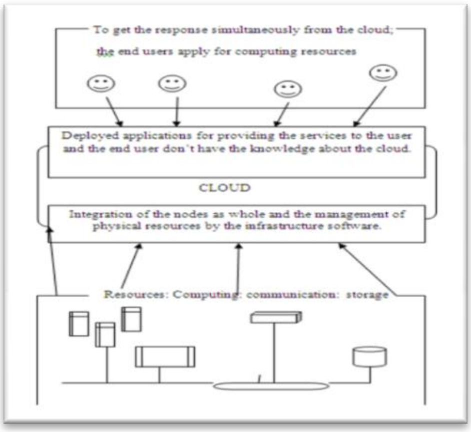

To get the response simultaneously from the cloud;
the end users apply for computing resources
Deployed applications for providing the services to the user and the end user don't have the knowledge about the cloud.
CLOUD
Integration of the nodes as whole and the management of physical resources by the infrastructure software.
Resources: Computing: communication: storage

Figure 1: Cloud computing pattern

1.2 Cloud Models

An essentially cloud models are two types: deployment model and Service model Cloud computing [6].

Deployment Model: Cloud deployment models communicate to a specific type of cloudy environment, primarily divided by size and access. Deployment model are three types [7].

Public cloud computing: It is chiefly depends on third person to suggest services by paying them on monthly basis according to the procedure. Public Cloud environment is made reachable to all unrestricted users who can promise the needed services [8]. The security issues will be decided by the service supplier and so it is very vital to choose the provider.

Private Cloud Computing: The association itself has control over the services. Usually organizations go for private cloud only in the case of association of sensible data. Scaling can be done very efficiently by adding hardware and thus the surroundings can be expanded. The security will be more due to the control of restricted by internal structure and therefore data will be secure [9].

Hybrid Cloud Computing: It is the mixture of both public and private cloud computing. A less sensible data will be storing in public and all others in Private Cloud.

Service Models: A cloud is a computing process in which services are distributing over network using computation process. The cloud character the hiding for complex environment it contains in system structure. Service models are three main categories: SaaS, IaaS, and PaaS [10].

Software-as-a-Service: The Software as services is high producing of a quality model. Where software hosted by the cloud venders are rented to the end client. They are substituting of the application running on pc. In 1960s with ASPs (Application Service

Providers) who managed and hosted dedicated business applications. Follow pay- per- use of prototype. Central organization is reduced cost. In this, the sales force, Microsoft, yahoo, Google is offered by company [11]. Example: They include customer relationship management (CRM) as a service; email; logistics software; order management software; payroll software and any other software are not installed and which is hosted on the internet on your computer [12].

Platform-as-a-service: The platform as services are refers to the software deployment framework, runtime atmosphere and the element on pay to alter the direct ready of application level assets or internet application [13]. It is a platform wherever put together will be deployed, tested and developed. They are resources of entire life cycle are software can be operated on a PAAS. For example: IBM Smart cloud, Microsoft Azure, Google app engine, and

Amazon EC2etc. Other word the platform as a service is allowing the customer to create their own request. The cloud application is supports a set of applications program interface. It is the middle connection between application and hardware.

Infrastructure as a service: The hardware as services are also called the infrastructure as a service. They are provides computing capabilities as standardized services and basic storage over the network. Pooled and made available to handle workloads are services, storage systems, networking tools, data center space etc [13]. Example: storage services provided by Amazon S3, Amazon EBS etc. Where users have consumes the property and virtual desktop like

network, virtualized services, routers and storage etc. are main idea of this model.

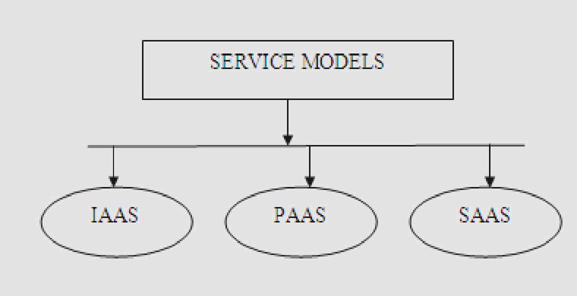


Figure 2: Service Model

1.3 Multimedia Data Security

Web of advance, Internet multi-media are emerging as a check. They are used the loaded medium services, process, they has emerge as a important technology to edit, produce and search media filling, such as video, graphics, images, audio, and so on. For cloud computing multimedia application are strong difficulties because of the important amount of totaling required for serving millions of Internet or mobile users at the same time?

1.3.1 Availability

The objective of availability for Cloud Computing system is on the technique to ensure its users can use them at any position, at any time. As its web native character, Cloud computing system permit its users to access the system from anywhere. For example request, services [14].

1.3.2 Confidentiality

Confidentiality means in cloud system is observance user's data clandestine. Cloud computing system aid are in essence public networks for example applications and its infrastructures Therefore, keeping all classified data of users secret in the Cloud is a elemental requirement which will draw even more users accordingly [15].

2 SYSTEM MODEL

Data reliability and privacy are the main issue in cloud storage surroundings. The requested multimedia data is transfer securely from cloud server to consumer. Here the Security is providing with combination of cryptographic algorithms.

1) Skipjack algorithm: Skipjack is a block cipher. Originally classified, it was initially intended for use in the contentious Clipper chip. Consequently, the algorithm was de-classified and now provides a exceptional insight into the cipher designs of a supervision intelligence agency. Skipjack uses an 80-bit key to encrypt and decrypt 64-bit data blocks. It is an unbalanced Festal network with 32 rounds. It was calculated to be used in tenable phones.

2). Elgamal algorithm: The Elgamal encryption system is an asymmetric key encryption algorithm for public key cryptography which is based on the Diffie Hellman key exchange. Elgamal encryption can be defined over any cyclic group.

2.1 Working Steps

- **Start**: It is the first step that initializes whole process. When program starts it loads pages of system into memory to start process of encryption and call next step for uploading file into system.
- **Upload file:**Here user can upload files for encryption.
- **Text, Audio, Video and Image**: There are four types of files Text format, audio, video and Image. These files are used for encryption.
- **Apply Elgamal:** It used to generate key for encryption of data file. System configures it and uses their key for SKIPJACK for encryption.
- **Cipher Block:** In this step cipher block of SKIPJACK is generated with Elgamal key. And transfer control in two separate blocks of code 1. Mail system and 2. Encryption blocks Skipjack.
- **Mail Services:** It is provided by gmail.com with SMTP protocols to attach system with Gmail server. It uses simple mail transfer protocol. After connecting system with Gmail, mail is sent to user with content as key.
- **Encryption with SKIPJACK:** In this step Skipjack encryption technique is applied on data with key and encrypts it for storing in database.
- **Generate data:** After applying both encryption algorithms, data is generated. It is encrypted data that is ready to store in database. All encrypted bytes are combined with each other to generate single file.
- **Signature:** Now add signature in the data to make it secure from external misuses. It is a digital signature that is used to upgrade the security content.
- **Upload:** Here whole encrypted data is uploaded in database for further use.
- **User:** User can select file and can download file from the system. For this user requires key and signature to decrypt the file.
- **Key+ Signature:** User enters the key that he has fetched from mail and signature that is entered at the time of uploading file.
- **Download:** If the key and signature are same than it will decrypt file, else the process of download is rejected by the system and ask from user to try again with other correct key and signature.

2.2 Flowchart

Below flowchart describes the working model of proposed work.

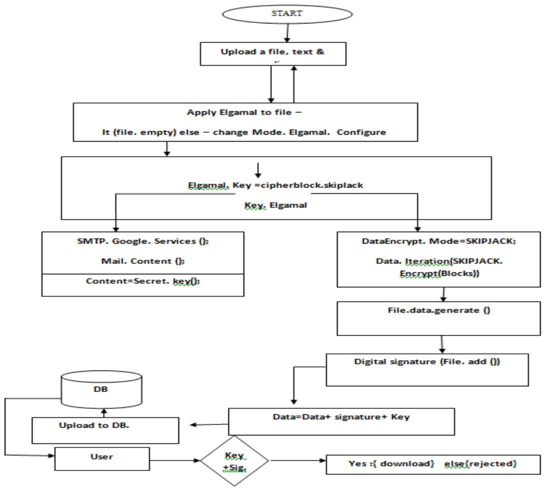

START
Upload a file, text &
Apply Elgamal to file –
It (file. empty) else – change Mode. Elgamal. Configure
Elgamal. Key =cipherblock.skiplack
Key. Elgamal
SMTP. Google. Services ();
Mail. Content ();
Content=Secret. key();
DataEncrypt. Mode=SKIPJACK;
Data. Iteration(SKIPJACK. Encrypt(Blocks))
File.data.generate ()
Digital signature (File. add ())
DB
Upload to DB.
Data=Data+ signature+ Key
User
Key +Sig.
Yes :{ download} else{rejected}

Figure no: 3 Simulation Model

2.3 Algorithm Steps

Step1. System.file.Upload(Image,Audio,Text,Video)

This is the first step which used to get input starting user. The input should be any kind of file which is as text file, audio file, video file or any image.

Step2. System.check(file.status)

System checks file status that file present or not. If it uploaded it shows status as true.

Step3. If (file.status.exist==false) It compare system's file status that status true or false. If file present its status true otherwise it will false.

Step4. Repeat step (file. Upload)

Its transfer control for first step if the file status would be false. It shows that file not present. So it needs to show message for upload a file for further operations.

Step5. else { Data.mode.set==cipher }

Step6. algo. Elgamal.prepare=true.

This step allows code to change working mode to cipher mode to apply encryption scheme. It used to initialize encryption on file.

Step7. Elgamal.generate.key=true.

First step to initialize Elgamal algorithm for key generation which require for encryption and decryption.

Step8. Cipher. Block =Elgamal. Key

Next step is also used to define blocks of data to be encrypts. It used to Encrypts key in data with using SKIP JACK algorithm.

Step9. SMTP. Google. Services();

Step ninth are used to configure Gmail with our system. This process use SMTP protocol for configuration.

Step10. Mail. Content (Key. Elgamal. Key());

Step tenth are used to configure gmail with our system. Here system uses this service for mail key to user for security purpose.

System accepts digital signature for enhance security. It would be as image file for data security.

Step11. System. Encryption. Mode=Mode.skipjack;

Next three steps used to encrypt data block by block with using key. It generates encrypted data and embed key block wise.

Step12. If (key. Elgamal. Key () !=null) { Skipjack.(Elgamal. Key. Content ()) };

Step13. Data.Bytes.Encrypt(Skipjack.Encryption)

Step14. Data(Add. Signature(Digital));

Data is combination of cipher bytes, Elgamal Key and digital signature. The whole bytes are combined and system generates output as encrypted data.

Step15. Data=Data()+Elgamal. Key ()+ Digital. Signature ();

Data is combination of cipher bytes, Elgamal Key and digital signature. The whole bytes are combined and system generates output as encrypted data.

Step16. Encrypted _output_ Data = Data.

Steps17. Stop

Stop save all the data object and render page for further process. It unloads objects after rendering process would be complete and give response to user accordingly.

3 RESULTS AND IMPLEMENTATION

The whole simulation has been done in .Net framework.

Its show the parameter values like time , accuracy, and error rate.

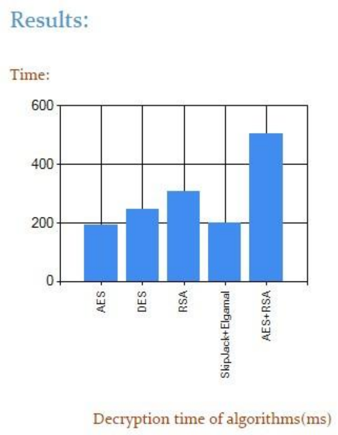


Figure.5 graph of time consume

The above figure shows the time consumer graph. In this graph is show the consumer time different algorithms like AES, DES, and RSA, skipjack + elgomal and RSA + AES.

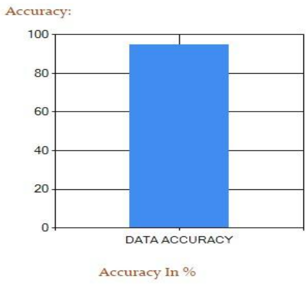


Figure.6 accuracy graph

The above figure shows the accuracy graph. In this graph are show the accuracy in skipjack+Elgamal algorithm.

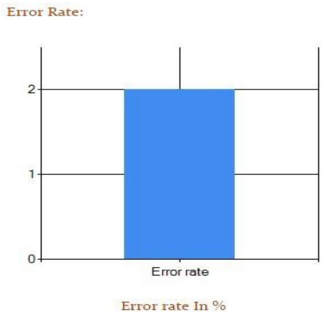


Figure.7 graph of error rate

The above figure shows the error rate. An error rate means the number of errors separated by the total number of moved bits during a studied time interval.

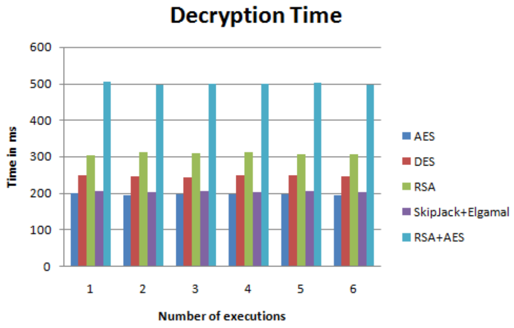
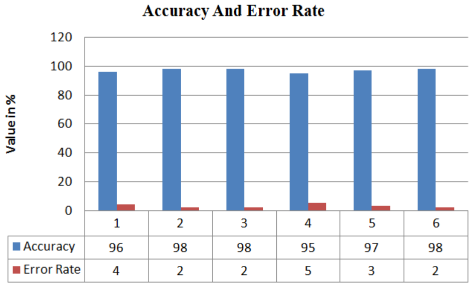


Figure no: 8 Decryption Time

The above figure shows the Decryption Time. To translate with or without before knowledge of its key. In this graph is showing the decryption time different algorithms like RSA, AES, DES, ELGOMAL+SKIPJACK and RSA+AES.



	1	2	3	4	5	6
Accuracy	96	98	98	95	97	98
Error Rate	4	2	2	5	3	2

Figure no: 9 Comparison between Accuracy and error rate

The above figure shows the Comparison between accuracy and error rate graph in purpose work.

4 CONCLUSION AND FUTURE SCOPE

In this paper, a variety of security concern of cloud computing has been systematically examined. All the primary concern of the data security explicitly privacy, validation and integrity have been address inside in a single environment. The proposed algorithm is, thus exclusive in its own way.

The main motivation behind this examine is to propose a solution to secure the disc data storage and organization since storage space over cloud takes place somewhere at a position which is beyond data owners' domain of control.

Apart from conniving the proposed result its achievement is also done using Dot Net framework over Microsoft Azure server. Moreover, in order to reproduce the optimal competence of this compound platform in evaluation to their individual counterpart, presentation analysis has been done on the basis of average finishing time, accuracy etc and the product is graphically reflected and systematically discussed. Thus, from the examination we terminate here that the proposed framework results in an optimal performance in terms of privacy, encryption and accuracy.

There are different ways to extend the research done in this study.

The future solution is implementing at a very smaller level where only a small amount of data is being outsourced to cloud. This could be unlimited for any huge data.

The projected framework may be unlimited to consist of many other organization or prepared controls.

5 REFERENCES

[1] Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. (2009, Feb. 10). Above the clouds: A Berkeley view of cloud computing. EECS Dept., Univ. California, Berkeley, No. UCB/EECS-2009-28[Online]. Available: http://radlab.cs.berkeley.edu/

[2] Vikas Goyal, Dr. Chander Kant, International Journal ofEngineering Sciences, ISSN : 2229-6913, September 2011,4, pp. 274-282. "Security Issues for Cloud Computing".

[3] Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. (2009, Feb. 10). Above the clouds: A Berkeley view of cloud computing. EECS Dept., Univ. California, Berkeley, No. UCB/EECS-2009-28[Online]. Available: http://radlab.cs.berkeley.edu/

[4] 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, 2008, pp. 5–13.

[5] Rajnish Choubey, Rajshree Dubey and Joy Bhattacharjee, "A Survey on Cloud Computing Security, Challenges and Threats", International Journal on Computer Science and Engineering (IJCSE), pp:1227 – 1231, Vol. 3 No. 3 Mar 2011, ISSN : 0975-3397

[6] B. Aljaber, T. Jacobs, K. Nadiminti, and R. Buyya, "Multimedia on global grids: A case study in distributed ray tracing," Malays. J. Comput. Sci., vol. 20, no. 1, pp. 1–11, June 2007.

[7] J. Nieh and S. J. Yang, "Measuring the multimedia performance of server based computing," in Proc. 10th Int. Workshop on Network and Operating System Support for Digital Audio and Video, 2000, pp. 55–64.

[8] Wenwu Zhu, Chong Luo, Jianfeng Wang, and Shipeng Li; "Multimedia Cloud Computing" Digital Object Identifier 10.1109/MSP.2011.940269 Date of publication: 19 April 2011.

[9] D.DanielM.Sona, , S.Vanitha"A Survey on Efficient Video Sharing and Streaming in Cloud Environment Using Video cloud"Vol. 1, Issue 8, October 2013.

[10] Douglas Selent, "Advanced Encryption Standard", Rivier Academic Journal, Volume 6, Number 2, 2010.

[11] Anna C.Squicciarini Dan Lin,Smitha Sundareswaran, “Ensuring Distributed Accountability for Data Sharing in the Cloud,” IEEE 2012.

[12] Boyang Wang, Jingbo Yan, Xuefeng Liu, YuqingZhang,”Mona: Secure Multi-Owner Data Sharin for Dynamic Groups in the Cloud,”IEEE 2013. [5] Larry A. Dunning and Ray Kresman,” Privacy Preserving Data Sharing With Anonymous ID Assignment,” IEEE 2013.

[13] KuiRen ,Ming Li, Shucheng Yu ,Yao ZhengWenjing Lou, , “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,” IEEE 2013.

[14] Sonal Guleria1, Dr. Sonia Vatta, “To Enhance Multimedia Security in Cloud Computing Environment Using Crossbreed Algorithm”, International Journal of Application or Innovation in Engineering and Management (IJAIEM), Volume 2, 2013.

[15] Cong Wang, KuiRen, Ning Cao,Qian Wang,Wenjing Lou, “Toward Secure and Dependable Storage Services in Cloud Computing,” IEEE 2012.