IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-4 E-ISSN: 2347-2693

Algorithmic Approach To Cloud Data Security

G. Shukla[1*], P. Srivastava[2], R. Kesarwani[3], H. Neyaz[4]

[1]Dept.CSE, Shambhunath Institute of Engineering and Technology, APJAKTU, Allahabad, India
[2]Dept.CSE, Shambhunath Institute of Engineering and Technology, APJAKTU, Allahabad, India
[3]Dept.CSE, Shambhunath Institute of Engineering and Technology, APJAKTU, Allahabad, India
[4]Dept.CSE, Shambhunath Institute of Engineering and Technology, APJAKTU, Allahabad, India

[*]*Corresponding Author: shukla2103@gmail.com, Tel.: +91 9918874011*

Available online at: www.ijcseonline.org

Received: 10/Mar/2018, Revised: 17/Mar/2018, Accepted: 29/Mar/2018, Published: 30/Apr/2018

***Abstract*—** Cloud Computing is taking popularity day by day in a various organization as it provides giant and scalable space for public and private use. Cloud computing is now widely used by many of the organization as a service. With the increase in the usage of the cloud, there also increases the concerns of cloud security. Somehow many organizations are hesitating to keep their data in the cloud due to security concerns. This paper understands various security issues related to cloud and resolves the data security issues, based on our proposed framework. Proposed framework is based on securing the various types of data like text, image and videos by applying Encryption Algorithms which reduces the various security issues and loopholes and thus making it more secure. It prevents the data from unauthorized access and also maintains the CIA (Confindentiality , Integrity, Availability). The paper proves to be providing the security in least time.

***Keywords*—** Cloud Computing, Data Security, CSP(Cloud Service Provider), AES(Advanced Encryption Standard),Data theft, Breach level index,DoS,DDos,CIA(Confidentiality, Integrity, Availability)

I. INTRODUCTION

The term cloud refers to a large area that has the capability to store a lot of data, create a backup of your important files that helps users to manage their space locally as well as remotely [1,2]. Users can store and access data by using internet from any place via Mobiles, Tablets, Laptops, PC's etc. According to a Forbes' report published in 2015, cloud-based security spending is expected to increase by 42%. Nowadays there are many organizations that are moving towards the cloud storage. It is gaining popularity day by day due to a wide range of use in today's era of computation. Cloud storage also provides store huge amount of data that are secured, confidential and integral. Cloud provides Software as a service (SaaS), Infrastructure as a service (IaaS), Platform as a service (PaaS) which help individuals to choose amongst any of the above services according to their requirement.[15] Storage as a Service provides by OneDrive, Dropbox, Amazon S3, Google Drive etc. that allow the user to store their own private data in their Cloud space [3].
60% of IT Market Growth Is Being Driven by the Cloud. According to Wikibon's report, cloud spending is growing at a 16% Compound annual growth (CAGR) run rate between 2016 and 2026. According to another survey by Forbes, expenditure on the Cloud Computing is growing at 4.5 times the rate IT expenditure since 2009 and is expected to grow at through 2020. Platform-as-a-Service (PaaS) adoption is predicted to be the fastest-growing sector of cloud platforms according to KPMG, growing from 32% in 2017 to 56% adoption in 2020.

Nowadays data is usually referred to as the money. [14]With the increase in the usage of the cloud, there also raises a major concern regarding the security of data stored on the cloud because there are the chances that some data may get leaked and privacy may get compromised. Data on the cloud need to be secure, reliable and available when needed.

Some of the major issues of cloud security include:

1. DoS Attack: When data is made unavailable.
2. DDoS: Distributed Denial of Service
3. Malicious Insiders: Employee of an organization make use of his/her privileged position and may get compromised.

This paper overcomes the security issues of cloud data that helps users to feel secure while storing their private data in the cloud and also prevents it from unauthorized access.
This paper comprises of 5 sections. The section 1 is Introduction. The section 2 includes the literature review and the survey we performed to know the existing solutions to cloud data security. The section 3 is all about our proposed

framework. Section 4 is the conclusion and future scope. The section 5 includes the references.

II. LITERATURE REVIEW

M. Rajasekhar Reddy, Akilandeswari R, S. Priyadarshini, B. Karthikeyan, E.Ponmani et al. prevent the cloud from the attacks and intruders by using the combination of RSA and Diffie Hellman Key Exchange but in this MITM(Man In The Middle attack) can be performed also decryption time for the RSA is very long. This paper only provide the security of text data and assumes that data is safe from insiders [4]. Akanksha Bansal , Arun Agrawal et al. in their proposed framework do not encrypt the whole file they just encrypt few bits and used the ECC algorithm to provide more security. Their system is efficient in such a way that it uses less CPU power and execution time [5]. Dr. P. Raviraj, Angeline Lydia, Dr. M.Y. Sanavullah et al. split the data recursively until all pixel doesn't get the same value if all pixel haven't the same value it will split an image until image split in 1 pixel [6].Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas, Aniket More et al. the proposed approach of authors are too much time taking to process a video data [7]. Anju Bala, Dr. Aman Kumar Sharma et. al. describes the region splitting algorithm but there is no practical implementation of algorithm and encryption is also not used[11]. Yunchuan Sun, Junsheng Zhang, Yongplng Xlong, Guangyu Zhu et. al. describes the CIA (Confidentiality, Integrity, Availability) properties & privacy issues but they didn't classify the data and treated all type of data is same[12]. S. Arul Oli and Dr. L. Arockiam et al. proposed a solution to obfuscate only the numerical data, to enhance security in public cloud storage. In the proposed technique, two keys are generated from the cloud for the confidentiality of numerical data and to enhance security in CS. This focusses only on the confidentiality of numerical data whereas other properties like integrity is not met.[13]

III. PROPOSED SOLUTION

The proposed framework consists of three section. First Section depicts about the identifying the various cloud security issues and what can be done to resolve that issue.
The second section is all about our proposed solution to resolve Data Security issues and the third section is its implementation and finally analysis and results that had been drawn from it.

1. CLOUD SECURITY ISSUES AND COUNTERMEASURES

According to the Privacy Rights Clearinghouse report, data based on the amount of data lost, databases are the major source (64%) of data loss. Interest in the cloud is increasing day by day. IT Corporates are moving from the conventional method of storing data to Non-Conventional Method.

Using the cloud as a Non-Conventional Method on the large scale had demanded to secure the cloud data and assessing its various security parameters in depth.

Breach level index also reports that out of the 5.9 billion records that have been lost or stolen since 2013 only 4% consisted of encrypted data which is useless to any hacker.
Here is a snapshot of issues and countermeasures of cloud data Security in figure 1:

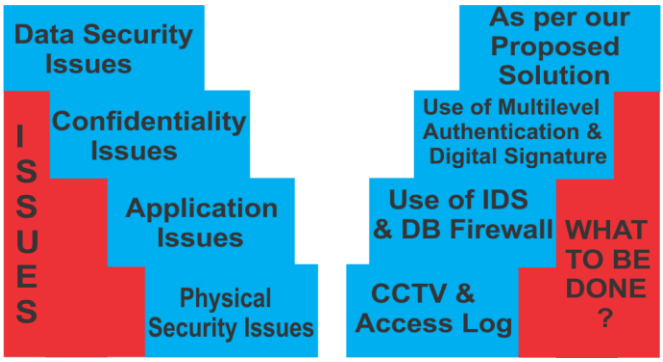


Figure 1: Cloud Security issues & their countermeasures

A. DATA SECURITY ISSUES:

Data at Rest & Data Theft are the major Data Security Issues and these can be resolved by our proposed solution given in table l. Encryption of data will be done using specific algorithm so in case if data is gathered, it is of no use to the attackers. This also ensures the Integrity of the data.

B. CONFIDENTIALITY ISSUES:

We can use multilevel Authentication & Digital Signature for the purpose of maintaining confidentiality. Biometric Authentication can also be introduced.

C. APPLICATION ISSUES:

A malicious piece of code can be injected into cloud database by Hackers or Attackers. For avoiding this IDS (Intrusion Detection System) can be used. Database Firewall can be installed. Regular Monitoring and auditing of data can be done.

D. PHYSICAL SECURITY ISSUES

So far we are talking about the Security of the data at the browser end but what will happen if the Physical Security of Data is being compromised and someone physically acquires the machine, for this issue, we can use CCTV and Access log.

2. PROPOSED FRAMEWORK

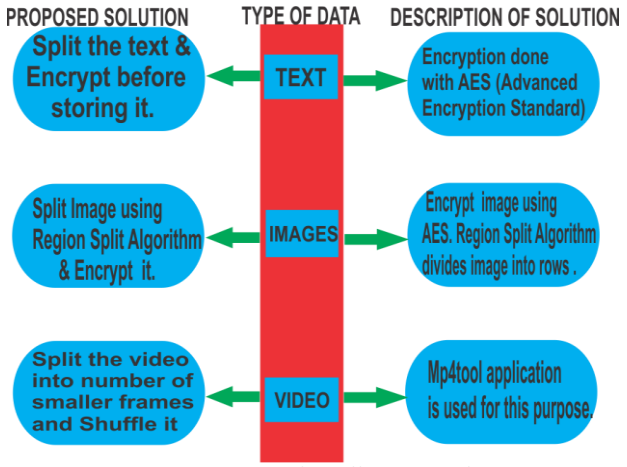


Figure 2: Proposed Solution for Different type of Data

We are proposing an approach that store text data in the cloud by splitting and encrypting before storing in the cloud. The breaking of data prevents leakage of confidential information and encryption method guarantees security which ensures that the Cloud Service Provider (CSP) is also unable to access the user data. We are also proposing an approach for image and video data also where we split the image and video using the splitting algorithm and also encrypting, before storing it in the cloud. While splitting the data we are also ensuring that integrity of data will remain to maintain when we fetch it back from the cloud.

The breaking of data (text & image) is done through the *splitting* algorithm that splits the data and the encryption is done [9] using the most secured algorithm called as AES (Advanced Encryption Standard). The text & image data can also be decrypted in the reverse order of both algorithms while we fetch it from the cloud. The image data will be split by the region splitting algorithm in which image is broken into a predefined number of horizontal regions after the original image being encrypted by the AES algorithm. For the decryption, the horizontal split images are merged and then decrypted in the reverse manner of the same algorithm. The video data is split by an API called as MP4Tool which split the large video clip into a number of smaller frames. These video frames are shuffled in a random order before being uploaded to the cloud storage [8].

Table 1. Approaches used for Different Data

Text Data	Split the text and Encrypt before storing in the cloud.	Split the text and encrypt it by using AES (Advanced Encryption Standard) and decrypt the text with the same algorithm in reverse order.
Image Data	Encrypt& Split images before storing into the cloud.	The selected image is encrypted by AES (Advanced Encryption Standard) algorithm & then split by region splitting algorithm. Decryption is done in reverse manner of algorithm after merging the split image.
Video Data	The video clip is split into a number of small video frames. These frames are then shuffled.	The video is split into several small video frames by using MP4Tool application. These frames are then shuffled randomly.

3. IMPLEMENTATION AND RESULTS

3.1. DATA FLOW DIAGRAM

Figure 3. Level-0 DFD

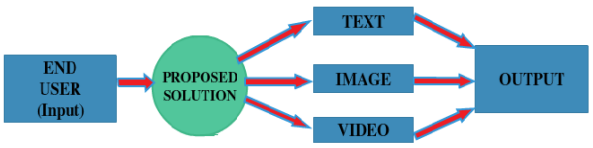


Figure 4. Level-1 DFD

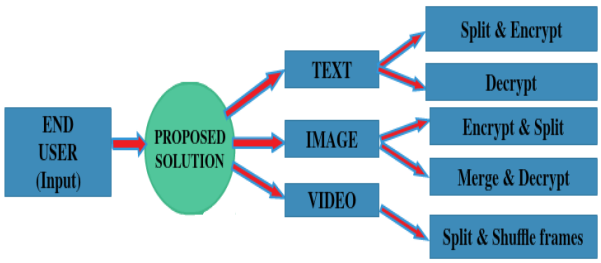


Figure 5. Level-2 DFD

3.2. SNAPSHOT OF THE DEVELOPED SOFTWARE FOR:

I) TEXT DATA

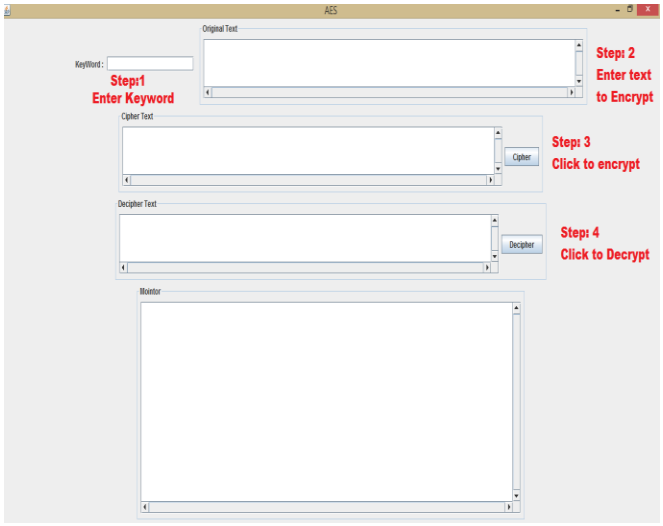


Figure 6. Software Window Before Encryption

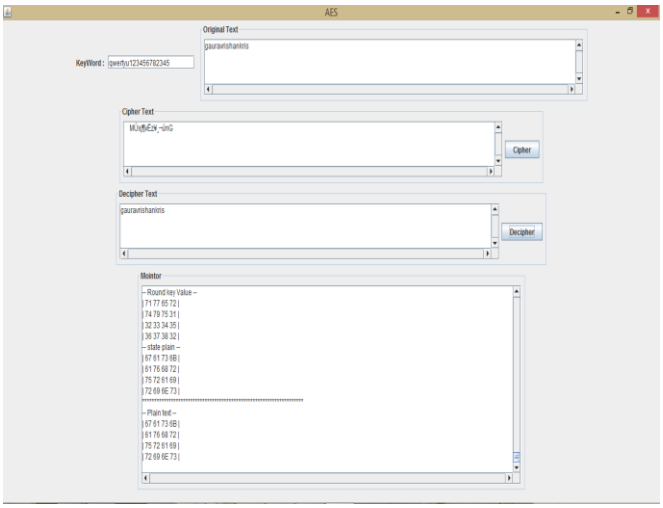


Figure 7. Software Window After Encryption

II) IMAGE DATA

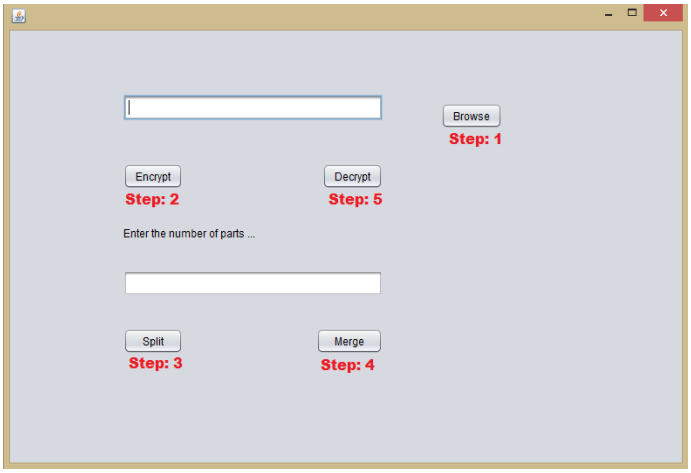
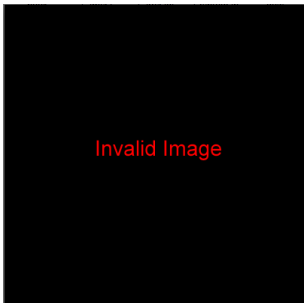


Figure 8. Software Window for Image Data

Table 2. Image Before and After Encryption

IMAGE BEFORE ENCRYPTION	IMAGE AFTER ENCRYPTION
	

III) VIDEO DATA

Figure 9. Splitting & Shuffling of Video frames

3.3. ANALYSIS & RESULT

Table 3. Analysis between RSA and AES Algorithm

Parameters	RSA	AES
Encryption	Slower	Faster
Decryption	Slower	Faster
Power Consumption	Low	High
Algorithm	Symmetric	Asymmetric
Security	Least Secured	Excellent Secured
Rounds	1	10/12/14
Hardware & Software Implementation	Not Efficient	Faster
Ciphering & Deciphering Algorithm	Different	Same

It is clear that from Table 3,AES algorithm performs better than RSA algorithm and showing the improvement in Encryption, Decryption, Security, Rounds etc. The security of Video data is also improved by applying AES on it as well.

IV. CONCLUSION AND FUTURE SCOPE

In this paper, we identified security issues related to the data present in the cloud. We focused on the various techniques by which we can save our cloud data from attackers.We proposed a new approach to secure various kinds of data like text, images, and videos. We use the most efficient algorithm i.e. AES algorithm having a large key size which is tough to recognize. AES takes the least time to encrypt and decrypt data either it is text or image, various other parameters have also been examined mentioned in Table 3.For the video data we have shuffled the video frames for its security. In future works we will enhance the security of Video data by applying AES on it as well. After this the main objective should be, to reduce the space occupied by the encrypted data.

V. REFERENCES

[1] V. Chang , M. Ramachandran ,"*Towards achieving data security with the cloud computing adoption framework*", IEEE Trans. Serv. Comput. 9 (1) (2016) pp. 138–151.

[2] K. Gai , M. Qiu , L. Chen , M. Liu, "*Electronic health record error prevention approach" using ontology in big data*", 17th IEEE International Conference on High Performance Computing and Communications, New York, USA, 2015, pp. 752–757

[3] K. Gai , L. Qiu , H. Zhao , M. Qiu ,"*Cost-aware multimedia data allocation for heterogeneous memory using genetic algorithm in cloud computing*", IEEE Trans. Cloud Computing. 1 (2016) pp. 99

[4] M. Rajasekhar Reddy, Akilandeswari R, S. Priyadarshini, B. Karthikeyan, E. Ponmani " *A Modified Cryptographic Approach For Securing Distributed Data Storage in Cloud Computing*" 2017 International Conference on Networks & Advances in Computational Technologies (NetACT) |20-22 July 2017| Trivandrum

[5] Akanksha Bansal , Arun Agrawal "*Providing Security ,Integrity and Authentication Using ECC Algorithm in cloud storage*" 2017 International Conference on Computer Communication and Informatics (ICCCI -2017), Jan. 05 – 07, 2017, Coimbatore, INDIA

[6] Dr. P. Raviraj, Angeline Lydia, Dr. M.Y. Sanavullah *"An Accurate Image Segmentation Using Region Splitting Technique"* GESJ: Computer Science and Telecommunications 2011|No.2 (31) pp. 16-18 10 June 2010.

[7] Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas, Aniket More "*Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study*" International Journal of Computer Applications (0975 – 8887) Volume 65– No.1, pp. 3-5 March 2013.

[8] Jolly Shah and Dr. Vikas Saxena" *Video Encryption: A Survey*" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, pp. 5-8 March 2011

[9] Mohit Kumar, Akshat Aggarwal, Ankit Garg "*A Review On Digital Image Encryption Techniques and Security Criteria*" International Journal of Computer Applications (0975 – 8887) Volume 96– No.13, pp. 4-8 June 2014

[10] Mark Brinda, Michael Heric "*The Changing Faces of the Cloud*" Bain Global Technologies, Bain & Company, New York, pp. 5-12, 2017.

[11] Anju Bala, Dr. Aman Kumar Sharma "*Split and Merge: A Region Based Image Segmentation*" ,International Journal of Emerging Research in Management & Technology ISSN: 2278-9359 (Volume-6, Issue-8), August 2017

[12] Yunchuan Sun, Junsheng Zhang, Yongplng Xlong, Guangyu Zhu *"Data Security and Privacy in Cloud Computing*", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 16 April 2016

[13] S. Arul Oli , Dr. L. Arockiam "*Confidentiality Technique to Obfuscate the Numerical Data to Enhance Security in Public Cloud Storage*", 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) pp. 3-5

[14] Swapnil Rajesh Telrandhe, Deepak *Kapgate* "*Authentication Model on Cloud Computing*" International Journal of Computer Sciences and Engineering (IJCSE) Volume-2, Issue-10, pp. 33-37

[15] Sajjan R.S., Vijay Ghorpade, Vishvajit Dalimbkar "*A Survey Paper on Data security in Cloud Computing*" " International Journal of Computer Sciences and Engineering (IJCSE) Volume-4, Special Issue-4

[16] Dr. Prerna Mahajan, Abhishek Sachdeva, "*A Study of Encryption Algorithms AES, DES and RSA for Security*" Global Journal Of Computer Science And Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013, Type: Double Blind Peer Reviewed International Research Journal Publisher: Global

Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350, pp. 7-8

Author Profiles

Gaurav Shukla, a student at Dr. A.P.J. Abdul Kalam Technical University is currently in the final year of his Bachelor of Technology in the field of Computer Science and Engineering . He is an active member of Computer Society of India since 2015. He has also presented his paper on " Digital forensics Investigation Models & its Applications" in National Seminar of Computer Society of India. His Interest areas are Cryptography, Cloud Security, Web Programming, Python Programming .

Prashant Srivastava, is currently working as Assistant Professor in Department of Computer Science & Engineering at Shambhunath Institute of Engineering & Technology. He had completed his master of Cyber laws and Information Security in 2012 from Indian Institute of Information Technology, Allahabad (IIITA). Prior to this he had completed Engineering from SHIATS, Allahabad. His research interest includes cloud security, web application security, network security and database security.

Rishank Kesarwani, a student at Dr. A.P.J. Abdul Kalam Technical University is currently in the final year of his Bachelor of Technology in the field of Computer Science and Engineering . He is an active member of Computer Society of India since 2015.. His interest ranges from Web Development to programming languages.

Hera Neyaz, a student at Dr. A.P.J. Abdul Kalam Technical University is currently in the final year of her Bachelor of Technology in the field of Computer Science and Engineering . She is an active member of Computer Society of India since 2015. Her interest ranges from Web Development to programming languages. She has also presented her paper on " Eternal 5D data storage" in National Seminar of Computer Society of India.

