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

Hybrid Cloud Data Security Model Using Splitting Technique

Siddharth Mishra[1*], Puneet Sharma[2]

[1]*Department of Computer Science and Engineering, Amity University, U.P., India*
[2]*Department of Computer Science and Engineering, Amity University, U.P., India*

www.ijcseonline.org

Received: May/26/2016 Revised: Jun/08/2016 Accepted: Jun/20/2016 Published: Jun/30/ 2016

***Abstract*— Cloud computing is an enticing technology that delivers services over the internet. It allows business organizations to use different applications and store information without accessing their personal files. In the recent years IT organizations prefer to move towards the adoption of Hybrid Cloud as it can be easily incorporated with the existing infrastructures of the enterprises. The cost of the implementation of hybrid cloud is quite low and it also provides the advantages of both public and private clouds. However, with the measurement of power, stability and the security of cloud one cannot ignore unlike coercion to user's data on cloud storage. In this paper, a security model has been proposed that secures sensitive and critical data with the help of symmetric cryptography and data splitting techniques. It also uses multi cloud service providers for the protection of overall cloud model. Data to be stored in the cloud will be first encrypted using AES encryption and then it will be split into numerous chunks. After splitting, these chunks of data will be stored in dissimilar clouds in a random manner.**

Keywords*— *Hybrid cloud, Data splitting, AES encryption, Cloud Computing

I. INTRODUCTION

Cloud computing possesses an immense probability of endowing vigorous computational strengths to the world at lower charge. It facilitates clients with inadequate assets to subcontract their hefty calculation workloads to the cloud and cost-effectively benefit from the enormous processing power, storage space, bandwidth and even suitable software which can be shared mutually in a pay-per-use approach. It may seem like the landscape of cloud computing is in a state of constant evolution. Cloud can be deployed in more than one way according to the usage and requirements. Four predefined ways for deploying cloud are public cloud, private cloud, community cloud and hybrid cloud. The debate over private versus public cloud will rage on but many experts quote several benefits of hybrid cloud environments. With the maturity of overall cloud, organizations have started moving towards hybrid cloud as it's architecture proposal provisions security along with cost saving, flexibility, scalability, high performance while gathering business and technical needs.

According to the survey conducted by Right Scale in 2016, the adoption of private cloud had increased up to 77%. On the other hand usage and adoption of hybrid cloud had been increased from 58 % to 71% year-over-year. Also, 82 % of enterprises have a hybrid cloud strategy, holding steady from 2015 [1].

While seeing the power, stability and the security of cloud, it cannot be ignored that there are different threats to user's data on cloud storage. There are many issues in Cloud Computing including data shredding, data misuse and data transmission security threats which are explained later in this paper. In our proposed framework, a security model has been proposed that secures sensitive and critical data with the help of a block cipher symmetric cryptographic and data splitting techniques. It also uses multi cloud service providers for the protection of overall cloud model.

Section 2 of this paper gives a brief about the techniques used in the proposed framework. In section 3 and section 4 we have explained our framework and the issues resolved by our model in detail respectively. Section 5 provides the simulation and result of our proposed method. Finally, section 6 concludes this paper.

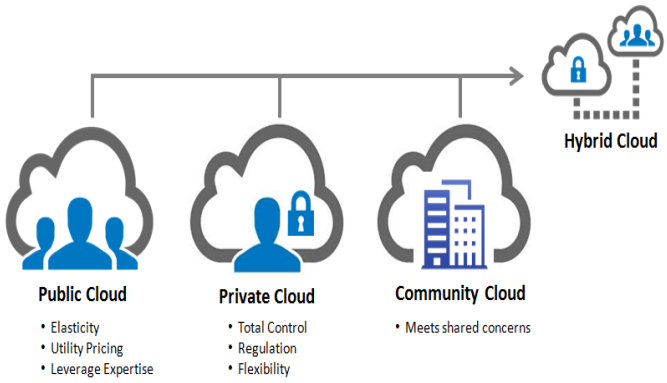

Fig. 1: Cloud Deployment Models [2]

II. METHODOLOGIES

A. *Advanced Encryption Standard*

After it was recognized by the National Institute of Standards and Technology, U.S.A. in 2001, AES or the Advanced Encryption Standard has become a prerequisite for the encryption of electronic data. AES is a symmetric or secret-key encryption technique which uses the identical key for encrypting and decrypting the file. Depending upon

the key length, AES is of three types i.e. AES-128, AES-192 and AES-256. Data blocks of 128 bits can be encrypted and decrypted using secret keys of sizes 128, 192 and 256 bits respectively. AES requires 10 rounds for 128-bit key, 12 rounds for 192-bit key and 14 rounds for 256-bit key. In Advanced Encryption Standard, 128 bit of data is separated into four operational blocks which are prearranged as state which is matrix of the order of 4×4. Every single round of AES contains numerous transformational steps that comprise substitution, transposition, mixing of the input plaintext and transforming it into the final output of cipher text. Below figure shows how a symmetric encryption uses the similar key for both encryption and decryption.

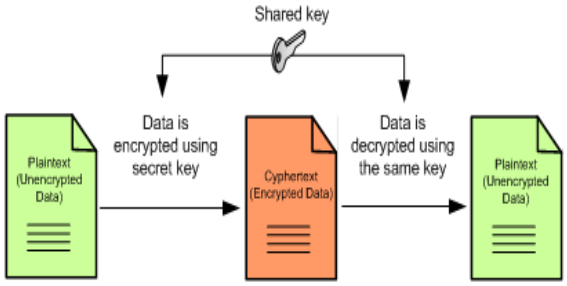

Fig. 2: Symmetric Encryption [3]

B. *Data Splitting*

The idea behind data splitting is to divide the data into various parts that can be stored over multiple clouds that are non communicable to each other. Whenever split data is accessed, the parts stored at different places are retrieved and combined. Data splitting is an excellent technique to protect the information because not only an unauthorized entity would require the knowledge of the positions of the servers holding the parts, he should also be able to access every server and know what data to unite.

III. PROPOSED FRAMEWORK

According to Cloud Security Alliance (CSA), over 70 percent of the world's businesses now functions, at least partially, on the cloud. One of the most challenging issues at present in single public cloud is data confidentiality and efficient data shredding. Critical and sensitive data of client is stored in server provided by third party provider. The proposed model for the multi-cloud architecture will secure data with data-splitting theory. Information that is being stocked up in the cloud will be encrypted first, and then it will be split into multiple chunks of equal sizes. These data chunks will be stored in different clouds. Each provider will have only a small segment of the original file and this small amount of segment alone will not have any potential informative value to anybody even if it is being accessed. Figure 3 shows the framework of our proposed model.

There are four phases in our framework namely Authentication, Encryption, Splitting and Uploading. These are explained in detail below:

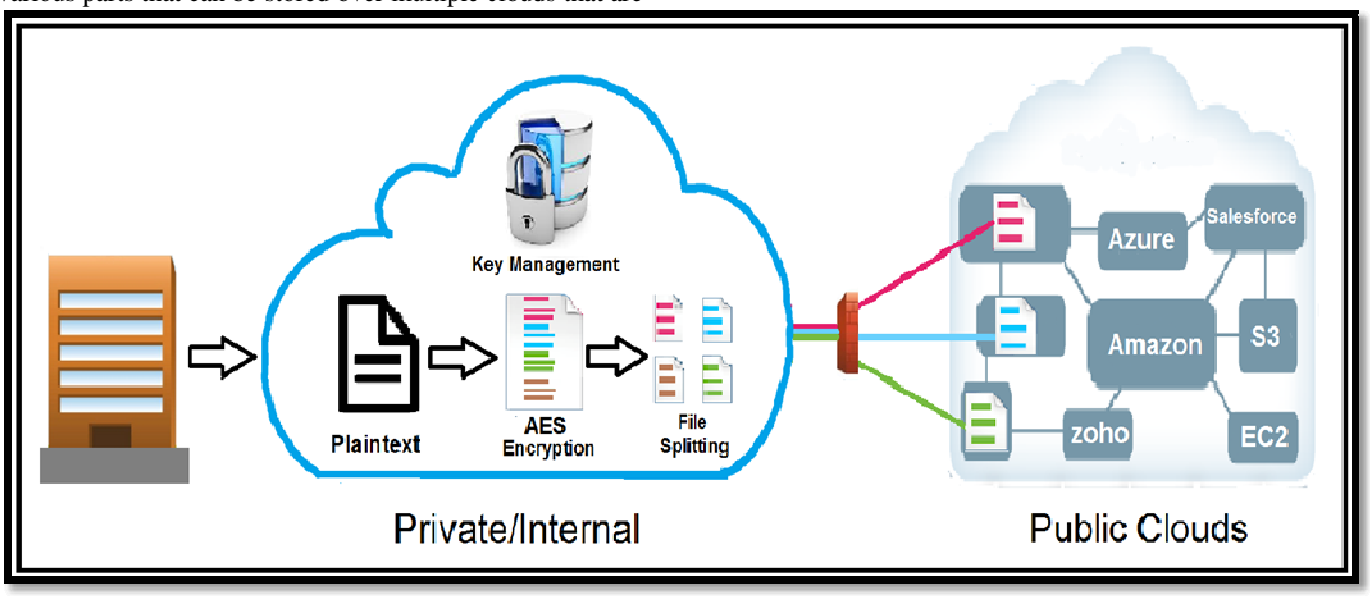

Fig. 3: Proposed Framework

Phase 1: Authentication
At first, the clients at the local infrastructure will have to register themselves by providing the required details. Then they would be redirected to the login page where they have to authenticate themselves by entering their correct login IDs and passwords. Clients can upload their data to hybrid cloud only after being authenticated.

Phase 2: Encryption
The client selects a file for AES encryption. He is required to enter a key of 256 bits. The key can be of client's choice. This step results in the creation of encrypted file, salt and IV. Salt and Initialization Vector (IV) enhances the security of the secret key and original file respectively. They are random input and are to be kept safe. People have the habit of using the same passwords again and again which results in creation of same cipher text. Salt is concatenated with the secret key resulting in different cipher text every time even if the same passwords are used. On the other hand, the first 16 bits of IV is XORed with the initial 16 bits of the plaintext of the file making it more secure.

Fig. 5: Encryption/Decryption using AES

Phase 3: Data Splitting
After encryption process, the client is redirected to splitting page. In this phase the encrypted file, irrespective of its size, is split into 3(n+1) data chunks where n is number of clouds present in the hybrid infrastructure. Here, the client also has the option to specify the size of each data chunk.

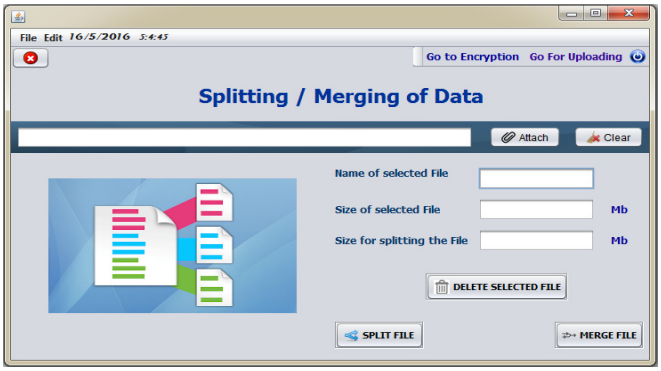

Fig. 6: Data Splitting

Phase 4: Uploading
Out of 3(n+1), 3n chunks are uploaded to different private/public clouds constituting the hybrid cloud. A random group of three chunks are uploaded in each cloud. The remaining parts along with salt, IV and key of the encrypted file remains stored at the local infrastructure. This provides an additional security layer as even if the parts stored at one location are captured, it's highly unimaginable that the attacker gets a hold of the other parts. This would prevent the data to be used in an illegal way.

IV. ISSUES RESOLVED

By bringing together these techniques, this approach offers a solution for various cloud challenges. They are:

A. *Data Shredding*
In cloud, to optimize the use of resources, clients have the option to move their data from one place to another. They may also completely remove it when they no longer require the cloud services. Ideally, when the data is moved or deleted, all the data in the previous location should be demolished. But sometimes data remnants remain which can create security issues as the residual data can be accessed in an unauthorized manner. This issue can be resolved using our proposed model. Because the client's data would be in an encrypted form in 3(n+1) parts on different private/public clouds, when they will be removed or deleted, their residue would not be of any importance.

B. *Data Confidentiality and Integrity*
Confidentiality means that only legal users or systems having the authorization and ability can access the data. Confidentiality ensures that the data which is residing in the cloud environment cannot be accessed by unauthorized party. The hazard of data concession is increased in the cloud, due to the enlarged number of parties, devices and applications involved, which results in the increase in the number of points of access. Data Integrity means safe-guarding data from unauthorized deletion, modification or fabrication. Data can be encrypted to provide improved confidentiality but there is no assurance that the data has not been modified while it inhabits the cloud. These issues can be resolved by our model as, first, it provides an authentication phase and second, the partial data in is in encrypted form and cannot be decrypted without the secret key.

C. *Data Transmission issues*
Internet is the correspondence system for cloud clients to exchange their information where it can be tainted. An imperative part of cloud computing is to give secure and effective transmission of information. The encryption phase of our model resolves this issue mostly successfully.

V. STIMULATION AND RESULT

In this segment, we have examined the performance and experimental results of proposed framework. We have compared the graphical representation and histogram of file, before and after execution. Graphical image has been generated using Binary Viewer tool. Figure 7 and figure 8 shows the original file when viewed in File Visualizer and its Histogram respectively. Figure 9 and figure 10 shows the AES Encrypted file when viewed in file visualizer and its Histogram and Figure 10 represents the split file when viewed in file visualizer. In all the images, green pixels show the printable ASCII characters

S.No	Summarizes the graphical characteristics of the selected file.	
1	Logical Pixel Size	2 Screen Pixels
2	Image Width	256 Logical Pixels
3	Pixel Density	1 Byte per Logical Pixel
4	Rendering Mode	Linear
5	Color Map	Standard

Table 1: Detalis of bitmap image.

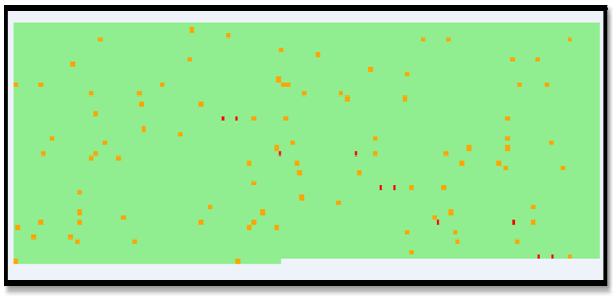

Fig. 7: Original File using File Visualizer.

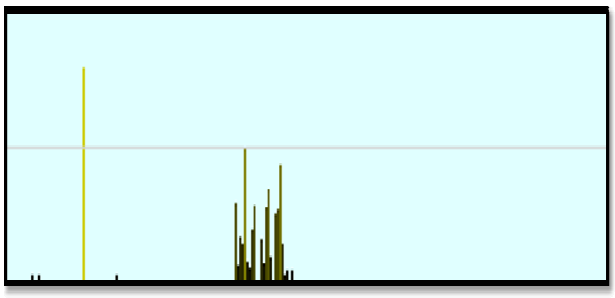

Fig. 8: Histogram of Original File

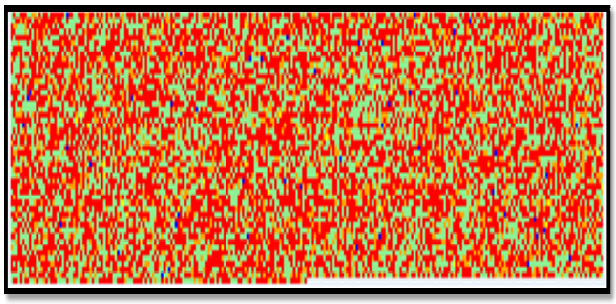

Fig. 9: AES Encrypted File using File Visualizer

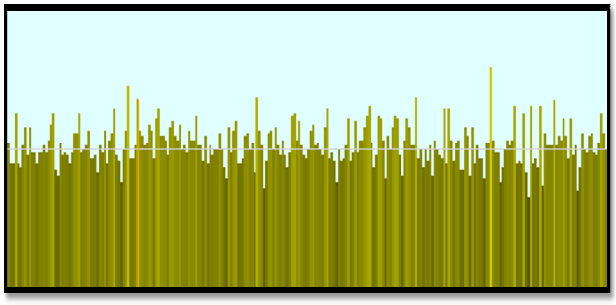

Fig. 10: Histogram of AES Encrypted File

S.No	Properties of Images Before and After Encryption		
		Before AES Encryption	After AES Encryption
1	Entropy	0.550687	0.998410
2	Average	93.359855	127.394491
3	Min. Frequency	0	31
4	Max. Frequency	1885	74
5	Sample Size	12405	12416

Table 2: Comparison of data before and after encryption

VI. CONCLUSION

In the recent years utilization of cloud computing has quickly expanded but still security is viewed as a noteworthy issue in the cloud computing atmosphere. Along with that, operational working in the cloud is still not transparent enough to user. In this paper, a framework has been proposed that can be adopted by any existing local infrastructure or private cloud to decrease the risk of data shredding, data misuse and data transmission issues. With

the help of the proposed framework, we are extending the cloud storage security by encrypting and distributing the data among multiple clouds. In the results section we have presented its implementation outcome. On comparing the graphical representation of plaintext, encrypted file and split file, we found that its security has been increased and it can be implemented over hybrid cloud environment for better efficiency and protection.

REFERENCES

[1] State of the Cloud Report from RightScale. www.rightscale.com/lp/2016-state-of-the-cloud. 2016.

[2] Cloud deployment model. http://transformcustomers.com/cloud-computing-benefits-and-challenges.

[3] AES Encryption. https://countuponsecurity.com/tag/openssl

[4] Vijayanand K.S. and Mala T., 'A Framework for Preserving Data Security in Hybrid Cloud Environment using Trusted Multiple Cloud Service Providers', Sixth International Conference on Advanced Computing (ICoAC), ISBN: **978-1-4799-8466-4**, Page No. (**14 – 18**), Dec **17-19**, **2014**.

[5] Anitha Y, 'Security Issues in Cloud Computing- A Review', International Journal of Thesis Projects and Dissertations (IJTPD), Volume **1**, Issue **1**, pp: (**1-6**), December **2013**.

[6] Anjali Nigam and Vineet Singh, 'A Study on Data Transmission Security Threats in Cloud', International Journal of Innovative Research in Computer and Communication Engineering, Volume **4**, Issue **5**, ISSN (Online): **2320-9810,** May **2016**.

[7] Munwar Ali Zardari, Low Tang Jung and Mohamed Nordin B.Zakaria, 'Hybrid Multi-cloud Data Security (HMCDS) Model and Data Classification', International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Page No. (**166-171**), Dec **23-24, 2013.**

[8] Advanced Encryption Standard. http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard.

[9] Rajleen Kaur and Amanpreet Kaur, 'A Review Paper on Evolution of Cloud Computing, its Approaches and Comparison with Grid Computing', (IJCSIT) International Journal of Computer Science and Information Technologies, Volume **5**, Issue **5**, ISSN: **0975-9646**, May **2014**.

[10] Ritu Pahal and Vikas Kumar, 'Efficient Implementation of AES', International Journal of Advanced Research in Computer Science and Software Engineering, Volume **3**, Issue **7**, July **2013**.

[11] Koushik Annapureddy, 'Security Challenges in Hybrid Cloud Infrastructures', Seminar on Network Security, **2010**.

[12] Akanksha V. Patil and Navnath D. Kale, 'A Secure Authorized Hybrid Cloud Distributed Key Generation for Encrypted Deduplication of Data', International Journal of Science and Research (IJSR), ISSN: **2319-7064**, **2013**.

[13] K.R. Monisha, 'Secure Cloud Computing using AES and RSA Algorithms', Proceedings of 20th IRF International Conference, ISBN: **978-93-84209-01-8**, March **1**, **2015**.

[14] Anukrati Dubey, Gunjita Shrivastava & Sandeep Sahu, 'Security in Hybrid Cloud', Global Journal of Computer Science and Technology Cloud and Distributed, Volume **13**, Issue **2**, ISSN: **0975-4350,** February **2013**.

[15] Pasquale Donadio, Giovanni B. Fioccola, Roberto Canonico and Giorgio Ventre, 'Network security for Hybrid Cloud', Euro Med Telco Conference (EMTC), ISBN**: 978-8-8872-3721-4**, Page No. (**1-6**), Nov **12-15, 2014**.

[16] Ranjit Panigrahi, M.K. Ghose and Moumita Pramanik, 'Cloud Computing: A new Era of Computing in the Field of Information Management', International Journal of Computer Science Engineering (IJCSE), Volume **2**, No. **5**, ISSN: **2319-7323,** September **2013**.

[17] Siddharth Mishra, Puneet Sharma 'A Study on Concerns and Impetus Aspects for Hybrid Cloud Adoption', International Journal of Innovative Research in Computer and Communication Engineering, Volume **4**, Issue **3**, ISSN (Online): **2320-9810,** March **2016**.

Authors Profile

Siddharth Mishra, M.Tech student in Amity University, Department of Computer Science and Engineering, Lucknow, Uttar Pradesh, India. Perused B.Tech in Information Technology from Amity University in 2013.

Puneet Sharma is working as an Assistant Professor in the Department of Computer Science and Engineering, Amity University, Uttar Pradesh, India.