Volume 6, Issue 4, April 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Mobile Computing for Sensitive Data Storage Using Multi-Clouds

[1]Abhijeet Mishra, [2]Arjun Aggarwal, [3]Gaurav Singhal, [4]Sushil Kr. Saroj
[1, 2, 3] CSE Department, GCET, Greater Noida, Uttar Pradesh, India
[4] AP, CSE Department, GCET, Greater Noida, Uttar Pradesh, India

Abstract— It is not recommended to store a person's sensitive data on mobile devices like mobile phones etc. As mobile devices have higher threat of getting lost or theft. Some people say that it is safer to have data stored over clouds, yes it is but only to an extent as the data exposer can be easier on data stored over single cloud. So it is the need of this time to have multiple clouds for data storage over clouds and this work is proposed as a vision for implementing multiple clouds by integrating some of the techniques of network security as data splitting, key handling etc. The proposed scheme basically can be used for highly sensitive data that are necessarily needed to be secured and stored on clouds.

Keywords— multi-cloud, mobile cloud computing, secure data storage, key handling, data handling, splitting

I. INTRODUCTION

According to [1] the cloud computing market, both public and private shows highly positive growth from the years 2010 to 2016 and is expected to show the same in the future as the continuous increment in the implementation of mobile computing and mobile devices[2]. The mobile cloud computing is an advanced introduction to the cloud computing model. The mobile cloud computing helps both mobile computing as well as cloud computing overcome its previous limitations and also benefits in its application. The commonly benefits that are clearly visible to all are summarized into three aspects: the battery life is extended by the as the mobile devices offload the computation tasks to be done by the cloud itself, the storage availability is extended by the mobile cloud computing, the reliability is also improved because the scalability and dynamic provisions are added to the mobile cloud computing.

Here in this paper our focus is on providing a way of storing the sensitive data on cloud for better security. The cloud storage now a days becomes the first choice for everyone due to its advantages over the other techniques. The cloud computing delivers Storage as a Service as its earliest service in which a user poses the availability of an optional storage i.e. Cloud to store his personal data as a personal storage unit. The data stored on clouds can be exposed because of four points: communication done on internet, due to external editing and monitoring, complexity of the cloud security, sharing of resources with other customer [3] [4]. The mobile cloud computing also possesses great threat for the sensitive data stored on it because the intruder if gets access to the cloud then there is no clause of saving the data exposer from it. So a new term called Multi cloud is introduced. The term stands for a technique where the cloud is not used for storage of the whole data of a user but it is divided into sub cloud architecture so as to provide a more secure storage because intruders have to achieve the access of all the sub clouds to get the whole of the data stored in portions on to the multi clouds. There are some available schemes that provide a way to store data on multi clouds but even now we need a more efficient data storing scheme which can be easily implemented and is helpful in overcoming the existing drawbacks.

The remaining portion of this paper is organized as follows. In Section II, we present our proposed scheme. In Section III, we conclude the paper. Finally, the references used to prepare this paper in last section.

II. PROPOSED SCHEME

In this section we proposed a framework to secure data using multi cloud with a mobile device, we propose a set of four modules:

- Cloud service providers for storage of the data on the multiple clouds.
- Data splitting technique that splits the data required to store into slices for better security.
- Encrypting/Decrypting mechanisms that are employed over data at different stages of proposed schemes.
- User platform and data.

The tasks performed throughout in the proposed scheme is explained below:

- Encrypting the data files that are to be stored on clouds.
- Splitting the data on the mobile according to the needs and comforts of the data owner as number of segments or size of files etc.
- Re-naming of the encrypted segments so as to make it difficult of any intruder to get access and control over the data slices.
- Assigning of the segments to the respective clouds as we are using multiple clouds so we have to assign each segment with a cloud on which it is stored.
- Distributing these segments to their respective clouds.

- As the other task we have the slices of the secret key that should be secret to the individual shareholders but collectively they should be able to reconstruct the secret again. So a threshold is generated that defines the minimum number of slices required to reconstruct the keys at the request.
- The key slices are provided to the shareholders with the surety that even if the security is compromised by some of the shareholders the individual shares get no use to them.
- At last the requested data from multi clouds is decrypted and merged again to reform the data uploaded.

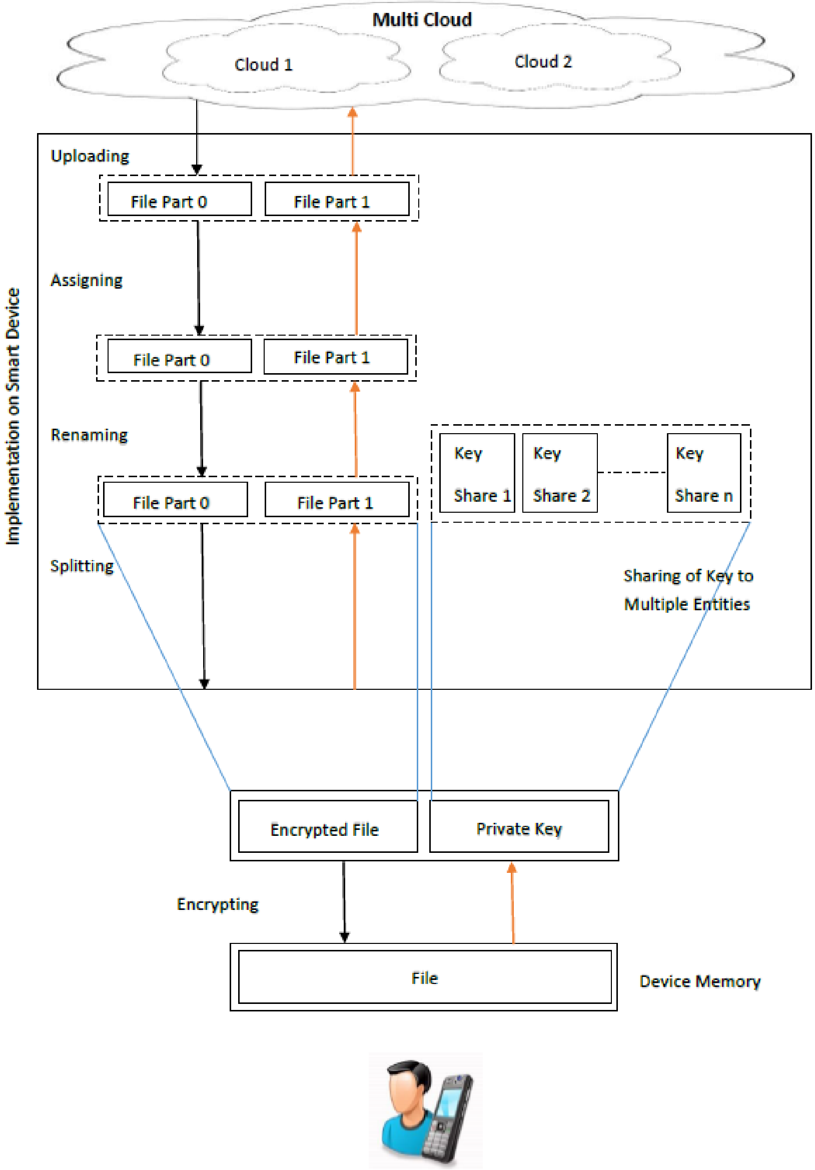

Fig. 1 The workflow of operations

In the Figure 1 the workflow of operations is explained through a flowchart. It shows how the mobile application can interact and update the multi-clouds status; and in which stage the data on-site storing and data archiving need to be completed.

To add up some security features, the proposed scheme not only handle the data but also handle the key. As the key is split into slices and is distributed among shareholders to make the key safe and secure. In this way it is difficult for intruder to decrypt the data. Part of a future work is to evaluate and confirm that claim using formal methods.

III. CONCLUSION

To add up, here we propose an approach that is supposed to offers more efficient and secure storage of the data on clouds over other already existing methods of cloud security. It's been found through studies that cloud computing services are more effective than traditional IT solutions for data storage. It provides better handling of key by distributing key using threshold cryptography and data by splitting it dynamically in nested cloud[5][6]. This approach that we have proposed is for handling the sensitive data so at first it may not seem to be economically efficient. As here we are more focused and concerned about the security of sensitive data rather than the implementation or operational cost of this proposed scheme. As the area of cloud computing and cloud security is a fastest growing field and every day we get a new technology so there is always a possibility of advancements and updates. The approach followed by us may be enhanced at some points as at the level of data splitting and access paths maintenance.

The data splitting and the key handling scheme used here in this approach may be challenged by new schemes in the future. But here we have tried to follow up the new trends of security of cloud storage to derive an efficient scheme that can solve the existing problems of cloud computing and storage.

REFERENCES

[1] Pring, B., Brown, R., Leong, L., Couture, A., Biscotti, F., Lheueux, B., Frank, A., Roster. J., Cournoyer, S., Liu, V., 2010. Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014. Gartner, 02 June. 2010.

[2] M. Alizadeh and W.H. Hassan, "Challenges and opportunities of Mobile Cloud Computing ," in Wireless Communications andMobile Computing Conference (IWCMC), 2013 9th International, pp. 660-666, 2013.

[3] W. Song and X. Su, "Review of mobile cloud computing," in Proc. of 2011 IEEE 3rd International Conf. on Communication Software and Networks (ICCSN), May 2011, pp. 1-4.

[4] N.J. King and V.T. Raja, "Protecting the privacy and security of sensitive customer data in the cloud," Computer Law & Security Review, vol. 28, pp. 308-319, 6. 2012.

[5] Doyel Pal, Praveen kumar Khethavath, Johnson P. Thomas, and Tingting Chen, "*Multilevel Threshold Secret Sharing in Distributed Cloud,*"Third International Symposium on Security in Computing and Communications (SSCC), 2015Springer,vol. 536, no., pp.13-23, 10-13August 2015.

[6] Balasaraswathi V.R., and Manikandan.S, "*Enhanced Security for Multi-Cloud Storage using Cryptographic Data Splitting with Dynamic Approach,*" International Conference on Advanced Communication Control and Computing.