CLOUD BASED SECRET COMMUNICATION

Mr.Abin K Markose

Assistant Professor

PG.Department of Computer Science

JPM Arts And Science College ,Labbakkada ,Kattappana,India

Abstract: Security ,trust and privacy issues are major obstacles for massive adoption of cloud computing the traditional cryptographic technologies are used to prevent data tapering and access to sensitive information . The massive use of virtualization technologies exposes the existing system to new threats, which previously were not considered applicable. New distributed steganography scheme based on the file integrity .Thus it guarantees that the exchanged file do not undergo any modification .this ensure a good security level with an undetectable secret communication

Index Terms - **cloud, steganography , distributed steganography**

I. INTRODUCTION

The rapid development of internet leads to an increase dependence in almost all areas of life. In the same way that it promotes communications, it also poses a threat both to users and to state institutions with the spying and theft of information. Security ,trust and privacy issues are major obstacles for massive adoption of cloud computing the traditional cryptographic technologies are used to prevent data tapering and access to sensitive information . The massive use of virtualization technologies exposes the existing system to new threats, which previously were not considered applicable. For example it might be possible that application hosted in the cloud can process sensitive information ;such information can be stored in the cloud storage facility by using most advanced technology in cryptography for protecting data ,and then consider safe from any attempt to access it without the required permission . While the data is processed in memory ,it has to be necessarily decrypted by the legitimate application .but since the application is hosted into a managed virtual environment ,it become accessible to virtual machine manager that by program is designed to access the memory pages of such application in this case what is experienced is a lack of control over environment in which the application is executed ,which is made possible by leveraging the cloud .it then happens that a new way of existing technologies creates new opportunities for additional thread to the security of application .the lack of control over their own data and process poses also severe problems for the trust we give to the cloud service provider and the level of privacy we want to have for our data. Steganography is the technique of hiding secret data within an ordinary ,non secret, file or message in order to avoid detection the secret data is then extracted at its destination .

1.1 DISTRIBUTED STEGANOGRAPHY

Recent research has introduced a new concept called distributed steganography by fragmenting the secret message and embedding each secret piece into a distinct cover media .the major interest of this approach is to make the secret message detection extremely difficult .however these file modification leaves a secret channel to an attacker . steganography paradigm transparent to any attacker and resistant to the detection and secret extraction .

New distributed steganography scheme based on the file integrity .Thus it guarantees that the exchanged file do not undergo any modification .this ensure a good security level with an undetectable secret communication .This techniques used exploits file storage in several cloud service providers .this solution is an excellent tool useful for the organization for data filtration in case of espionage or keep secure the participants shared keys involved in a secret sharing .there is no direct link between them during the communication process .one uploads file in the cloud storage while the second exploit these file. Each file implicitly holds a part of the secret data. The proposed techniques focus on maximum resiliency against secret detection and extraction .the ablty to use any file extension to establish the covert channel while maintaining their integrity . The proposed covert channel is a new paradigm transparent to secret communication between two parties .

II. CONCLUSION

The proposal of a secret communication where the file used as covert media carry the information without being modified .the cover media is a pointer to secret data this secret data is found in the key .this key consists of following set the lists of clouds and login credentials the list of files and the base used the sender and the receiver exchange this key before initiating their secret communication . The key exchange can be done in a physical meeting or using encrypted communication

III. ACKNOWLEDGMENT

REFERENCES

[1] Mastering cloud computing ,Rajkumar Buyya,Christian Vecchiola, S.Thamarai Selvi

[2] Security in Computing Fifth edition ,Charles P.Pfleeger ,Shari Lawrence Pfleeger,Jonathan Margulies.

[3] https://searchsecurity.techtarget.com/definition/steganography