INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

A survey on the security of multimedia contents with dual level encryption

Swapnali Anil Balshankar
swapnali971997@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Harshada Pacharane
harshu.18.03@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Vicky Bobade
vickybobade3@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Gauri Gherde
gaurigherde2@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Ujwala Gaikwad
ujwalavg@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

ABSTRACT

The cloud computing offers high quantifiability, confidentiality and therefore the simple accessibility of the knowledge over the net. tho' the traditional secret writing system provides security, the foremost involved issue is that the regular aspect channel attack for capturing ones sensitive and confidential image, audio and video. A malicious Virtual Machine (VM) besides a targeted VM will extract all info. Thus, this paper implements a double stage secret writing rule for the multimedia system content security exploitation random key generation approach. The primary stage encrypted multimedia system content into ciphertex -l employing a trigonal public key. The ciphertext-l is once more encrypted within the cloud exploitation a willy-nilly generated uneven non-public key. If anyone gets the cipher text, he couldn't extract the secret writing key to recover the multimedia system contents. Low complexness and simple implementation create the planned rule wide applicable safeguard within the cloud computing.

Keywords: *Cryptography, Cloud Computing, Multimedia Security, Encryption, Decryption.*

1. INTRODUCTION

This paper implements a double stage secret writing rule for the protection of multimedia system contents employing a willy-nilly generated key and therefore the sixty-four bit convertor. The willy-nilly generated secret's the outstanding feature that creates the second stage encrypted information unbreakable. These studies centered on the mixture of 2 totally different algorithms and generate a random security key for customers as a key to access the cloud. Cloud computing offers totally different services in commonplace models like Infrastructure as a service (IaaS), Platform as a service (PaaS) and code as a service (SaaS). This paper uses commonplace service module as IaaS.

2. PURPOSE

At present, the foremost dealing issue is that the security of the cloud, particularly the info and multimedia system contents like image, audio, and video. Many studies are done on the protection of the multimedia system contents within the cloud and reduce the aspect channel attack. It becomes Necessary to stop the info that is to be transmitted over cloud from aspect channel attack.

3. SCOPE

The aim of the project is to implement a double stage secret writing rule for the protection of multimedia system contents against a negligent third party and aspect channel attack. The planned willy-nilly generated key rule produces when a singular trigonal key that lets the info be encrypted with success. It will give high-level security to multimedia system contents to be transmitted from owner to user. Within the planned theme, {the data|the info|the info} owner is accountable for generating change information and causing them to the cloud server. Thus, the info owner has to store the encrypted file. During this system hybrid secret writing technique is applied to {the information|the info|the information} file exploitation AES and Blowfish rule to firmly store file data in the cloud. File sharing is feasible exploitation this cloud computing information. File information share between user and owner is secure exploitation hybrid secret writing technique.

4. LITERATURE SURVEY

4.1 Associate in Nursing Approach to increased Security of multimedia system information Model Technology supported

Cloud Computing Er. Mandeep Singh Sandhu Er. Sunny Singla

Cloud computing is rising field attributable to its performance, high convenience, least price and plenty of others. In cloud computing, the info is hold on in storage provided by service suppliers. However, still several business corporations don't seem to be willing to adopt cloud computing technology thanks to lack of correct security management policy and weakness in safeguard that cause several vulnerabilities in cloud computing. This paper has been written to concentrate on the matter of information security. Service suppliers should have a viable thanks to shielding their clients' information, particularly to stop the info from speech act by unauthorized insiders

4.2. An Enhanced Security Technique for storage of multimedia content over the cloud.

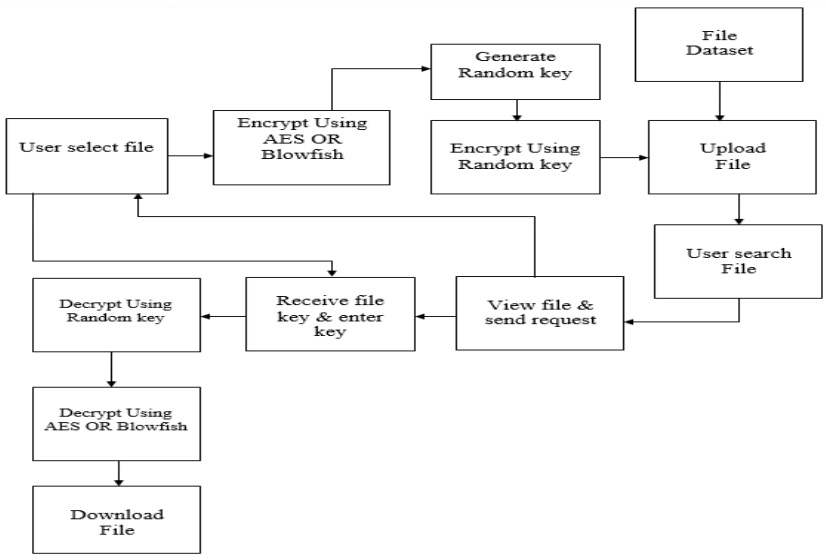
P. Gupta and A. K. Brar. This paper implements security on data such as audio, Video, text file and image stored in a cloud. This Security is provided using a combination of two Algorithms such as RSA and two fish algorithm. Storage of data files with the signature and an encryption algorithm based on a combination of RSA and Twofish (to have better security than RSA or Twofish alone) on Microsoft azure cloud.

4.3 to reinforce multimedia system security in cloud computing surroundings exploitation Crossbreed rule.Sonal Guleria and DR. Sonia vatta

This paper implements framework for access management during a cloud to facilitate style|the planning|the look} of the security system and scale back the complexness of system design and implementation. This can exploit the likelihood of RSA to support public-key cryptosystem and digital signatures. On the opposite hand, RSA and DES well outlined additionally as policy templet in his specific domain are provided for reference. to style Associate in Nursing secret writing rule supported combination on RSA and DES to own higher security than RSA or DES alone to write in the code the info files before storage on the cloud. It increased security and forestall replay attacks so, the results of this MI is delivered to the service model, and perform actions consistent with this security checking method.

5. SYSTEM DESIGN

BLOCK DIAGRAM



5.1. Secret writing Part

There square measure 2 levels of secret writing. The Encryption-I **:-** Has 2 rules like AES and Blowfish algorithm and produces ciphertext-I, the planned Encryption- a pair of is Associate in Nursing attachment supported the design in the paper to secure the cloud information exploitation willy-nilly generated key and convert the ciphertext-I into ciphertext-2. The willy-nilly generated secret's unknown to the content manager too.

5.2. Secret writing Part

In the shopper, the decipher processor has double secret writing processes (Decryption-l and Decryption-2) and a content player. The planned Decryption-I is decrypted by random key and converts the ciphertext-2 into ciphertext-I. The Decryption- a pair of finally converts the ciphertext-I to multimedia system contents exploitation trigonal key. While not the willy-nilly generated key, the Decryption-I method is troublesome and so the planned design provides economical security.

6. SYSTEM ANALYSIS

6.1 Advantages

- Encryption Double trigonal methodology key and uneven key.
- Key kind Random.
- Key exposition chance low

6.2 Disadvantages

- Encryption Singular trigonal methodology key and uneven key.
- Key kind mounted.
- Key exposition chance high.

6.2 Application

- M-commerce
- Data updates: we have a tendency to solely let {the information|the info|the information} owner perform data updates. this can be inflexible for applications wherever users might have to update the info additionally. Our answer is extended to permit users to perform information updates additionally to information homeowners.
- Ticketing theme: A ticketing scheme is used. The info owner can issue and sign a timestamp to authorize the user to perform a write. The user can submit the price ticket alongside his updates to the CSP, which is able to then apply the updates

7. CONCLUSION

This paper represents a double stage secret writing rule that gives the protection of multimedia system contents like image, audio, and video within the cloud. The planned rule is crucial in the second stage. The willy-nilly generated key provides a lot of security than the traditional secret writing system. The 64-bit convertor generates the multimedia system contents into the ciphertext. The ciphertext is held on within the cloud rather than original multimedia system content. The cipher text is, without doubt, exhausting to recover the first content for the random uneven key. Wide application of the planned rule shield {the information|the knowledge|the information} from the aspect channel aggressor to grab the multimedia system data into the cloud. Thus, the multimedia system content is safe within the cloud.

8. REFERENCES

[1] w. Kim, "Cloud Computing: these days and tomorrow." Journal of object technology, vol. 8, no. 1, pp. 65-72, 2009.
[2] P. Gupta and A. K. Brar, "An increased Security Technique for Storage of multimedia system Content over Cloud Server," International Journal of Engineering analysis and Applications (lJERA), vol. 3, no. 4, pp. 2273-2277, ACM, 2013.
[3] Associate in Nursing Approach to increased Security of multimedia system information Model Technology supported Cloud Computing Er. Mandeep Singh Sandhu Er. Sunny Singla
[4] Sonal Guleria and DR. Sonia vatta, "To enhance multimedia system security in cloud computing surroundings exploitation Crossbreed rule." International Journal of Application or Innovation in Engineering and Management, vol. 2, half dozen June 2013.

