A DATA SHARING PROTOCOL TO MINIMIZE SECURITY AND PRIVACY RISKS IN CLOUD STORAGE USING STEGANOGRAPHY TECHNIQUES

S. Nandhini Devi[1], S. Rajarajan[2]

[1](M.E) CSE Student, Dept. of CSE, Kings College of Engineering, Thanjavur, Tamil Nadu, India
[2](M.E) Assistant Professor, Dept of CSE, Kings College of Engineering, Thanjavur, Tamil Nadu, India

---***---

Abstract - *Data sharing inside the cloud is a way that lets in users to without difficulty get admission to records over the cloud. The data proprietor outsources their statistics in the cloud because of price reduction and the awesome conveniences provided by way of cloud services. Data owner isn't always able to control over their statistics, because cloud Provider Company is a 3rd party company. The important disaster with facts sharing within the cloud is the privateness and safety issues. Various strategies are to be had to help user privateness and comfy information sharing. This undertaking awareness on numerous schemes to cope with comfortable statistics sharing such as Data sharing with forward protection, relaxed information sharing for dynamic organizations, Attribute based totally statistics sharing, encrypted information sharing and Shared Authority Based Privacy-Preserving Authentication Protocol for access control of outsourced information.*

***KeyWords*: Data, Security, Encryption, Decryption, Steganography**

I. INTRODUCTION

CLOUD computing is hastily emerging because of the provisioning of elastic, bendy, and on-call for storage and computing services for clients. Cloud computing offers an effective manner to lessen capital expenditure and operational expenditure. This monetary gain is a major cause of the cloud recognition. However, SECURITY and privateness represent principal concerns inside the adoption of cloud technology for statistics garage. An method to mitigate those concerns is the usage of cryptography in which records are commonly encrypted earlier than storing to the cloud [1]. Whereas cryptography assures the confidentiality of the information towards the cloud, when the statistics are to be shared among a set, the cryptographic services want to be bendy enough to deal with specific customers, exercising the get entry to manage, and control the keys in an powerful manner to guard statistics confidentiality. The facts handling among a set has positive additional characteristics in place of two-party communication or the data handling belonging to a unmarried person. The current, departing, and newly becoming a member of organization participants can show to be an insider hazard violating facts confidentiality and privacy. While adopting a cloud for garage, the loss of manage over statistics and computation raises many safety concerns for corporations. The lack of manage over information and the garage platform additionally motivates cloud customers to maintain the get admission to manipulate over information (person information and the facts shared among a collection of customers via the general public cloud).The cloud consumer encrypts the statistics earlier than storing to the cloud, this guarantees cloud doesn't study any facts approximately purchaser's records. The get admission to rights are given to one-of-a-kind users by means of dispensing key used for encryption. However, this can bring about immoderate load over clients. By placing a third birthday celebration in between customer and cloud and delegating all operational loads to a third party will help to decrease load from the consumer. But whilst doing so there may be a possibility that 1/3 birthday celebration may additionally show malicious conduct. Hence there should be an technique to triumph over this. In this paper, we advocate a method named Secure Data Sharing in Clouds through limiting agree with in Third birthday party/Server that offers with the aforementioned protection. It helps to limit consider in third birthday celebration/server. While delegating a few operational load to a third party this approach guarantees statistics confidentiality. For this the concept of layer encryption is used where decrease layer encryption is finished through the records proprietor and top layer encryption is achieved by means of 1/3 party. The owner presents the authority of record get right of entry to to user through proving key used for decrease layer encryption, whilst encryption or decryption of the report. Hence, by using keeping manage over operations returned to statistics proprietor this method helps to hold confidentiality [2].The departing member cannot decrypt the statistics on its own as he/she will not able to get a key used for lower layer encryption from records owner. Similarly, no frequent decryption and encryption are wished for new consumer inclusion and person's departure.

II. DATA SECURITY OVERVIEW

Data safety is essential to shielding confidential statistics, respecting the privateness of studies topics, and complying with applicable protocols and requirements. Even reputedly de-diagnosed facts can be re-identified if sufficient specific characteristics are covered.1 Additionally, the facts discovered on this technique will be adverse in surprising ways. For instance, computer scientist Arvind Narayanan successfully re-diagnosed a public-use de-recognized information set from Netflix. Through this, he changed into capable to deduce viewers' political possibilities and other potentially sensitive data. Many research universities offer assist and guidance for records safety via their IT departments and through committed IT group of workers of their academic departments. Researchers should consult with their home group's IT workforce in setting up records security features, because the IT department may also have guidelines and aid for specific security software program. In addition to working with information safety specialists, researchers must gather a working information of information safety problems to make sure the clean integration of security features into their studies workflow and adherence to the relevant facts safety protocols. Researchers need to additionally make certain that their research assistants, students, implementing companions, and facts companies have a fundamental information of statistics protection protocols. Data-security measures must be calibrated to the danger of harm of a facts breach and comprise any requirements imposed by means of the information issuer. Harvard University's category gadget for information sensitivity and corresponding requirements for information protection illustrate how this calibration may also function in exercise.

CLOUD STORAGE FOR BIG DATA

Beyond allowing customers to place all information into cloud, cloud storage offers all varieties of records offerings for customers. Because scale horizontally runs on cheap commodity tough in a allotted configuration and there is no want for customers to buy and preserve their very own IT centers, cloud based totally big information shops brings in inherent availability, scalability and value effectiveness.

III. STEGANOGRAPHY

Steganography actually way Covered Writing. It is the system of hiding the secret data interior a cowl picture such that most effective the meant receiver is aware of its life. Internet performs an crucial role for records transmission and statistics sharing. It is a worldwide and publicized medium, some confidentiality facts is probably stolen, copied changed or destroyed. Here security is a major problem so we use steganography as a solution. Its intention is to hide the fact that conversation is taking area. In the field of Stenography, a few terminology has been developed. The term cover is used to explain the authentic, innocent message, facts, audio, nonetheless, video and so forth. The growing possibilities of modem communications want the unique means of security particularly on computer community. The community security is turning into more critical because the quantity of information being exchanged on the Internet increases. Therefore, the confidentiality and information integrity are required to defend towards unauthorized get right of entry to. This has led to an explosive increase of the subject of statistics hiding. In addition, the fast boom of publishing and broadcasting era additionally calls for an alterative answer in hiding facts. The copyright of digital media inclusive of audio, video and other media available in digital shape may additionally cause massive-scale unauthorized copying. This is due to the fact the digital formats make it viable to offer excessive image satisfactory even beneath multi-copying. Unauthorized copying is of top notch trouble of specially to the music, film, e book and software publishing industries. To triumph over this hassle, some invisible statistics may be embedded in the virtual media in such a way that it couldn't be easily extracted without a specialized technique. Information hiding is an rising research vicinity, which encompasses packages which includes copyright protection for digital media, watermarking, fingerprinting, and Stenography .All these packages of statistics hiding are quite numerous. In watermarking packages, the message contains statistics such as proprietor identity and a virtual time stamp, which is typically carried out for copyright protection. This adds to copyright records and makes it viable to trace any unauthorized used of the facts set. Stenography hides the secret message within the host information set and its presence is imperceptible.

LSB

A least good sized bit insertion method is probably the most well known photograph Stenography approach. It is a common, simple method to embed facts in a graphical image report. Unfortunately, it's far extremely at risk of attacks, together with picture manipulation. A simple conversion from a GIF or BMP format to a lossy compression layout such as JPEG can wreck the hidden records within the photo. When applying 4LSB strategies to every bytes of a 8-bit picture, one bit may be encoded to every pixel. Any adjustments in the pixel bits may be indiscernible to the human eye. The principal gain of 4LSB insertion is that facts can be hidden in the closing 4 least full-size bits of pixel and still the human eye might be unable to notice it.

TYPES AND MEDIA

Steganography can be labeled as pure, symmetric and asymmetric. While pure steganography does not want any exchange of records, symmetric and uneven want to change of keys prior sending the messages. Steganography is fairly dependent on the kind of media getting used to cover the records. Medium being commonly used consist of textual content, images, audio files, and network protocols utilized in community transmissions. Image Steganography is usually extra preferred media due to its harmlessness and attraction. Additionally exchange of greetings through virtual means is at the boom through the multiplied used of the net and simplicity of consolation and flexibility is sending them. Technology advancement in design of cameras and virtual images being stored in cameras and then transfer to PCs has also enhanced many folds. Secondly, the text messages hidden inside the photos does now not distort the image and there are strategies which only disturb most effective one bit of an picture who's effects is nearly negligible on its quality. Applications of steganography may be vast. It could have valid use to defend copyrights, to essential confidentiality. It may be utilized by law breakers to bypass facts which can also have particularly disastrous results. One of the major drawbacks of steganography is that you can still disguise very little facts in the media decided on.

BUILDING OF IMAGES

A digital photograph is "an array of numbers that represent light intensities at numerous points" . These mild intensities or pixels are combines to form the photo's raster facts. The pix may be of eight-bits or 24-bits. In GIF image size of each pixel is 8 bits. In this format the colors are represented from most used to least used shades. The photographs with 256 shades and pixel value of 640*480 sizes as much as 300 kilobits in which as a high resolution (1024*768) photograph of 24 bits might also have size larger than 2 megabits. Although large size document facilitates larger quantity of information to be hidden but moving larger size on the internet can cause suspicious in addition to require extra bandwidth accordingly highly-priced. Two varieties of record compression usually used to overcome above said troubles are Lossy and Lossless compressions. It is worth mentioning here that both of those strategies use separate mechanisms however intention is same that is to lessen the size of document to facilitate garage. JPEG (joint photographic experts group) is an example of lossy compression. Its advantage is that it saves extra area however in doing so loses its originality. On the alternative hand GIF (picture interchange layout) and BMP (bitmap record) are Examples of lossless compression that is in preferred recommended media sorts seeing that each of those keep their originality. Any photo consist of three primary colors specifically pink, inexperienced and blue, These colors typically known as RGB together form a digital photograph. As stated an photo is usually defined as range of pixels. Each colour of a pixel includes a byte or eight bits and carry sure statistics. Information is saved in the first bit of each successive pixel. Since statistics is saved inside the least substantial bit so equal does no longer affect the satisfactory of photo extensively. The entire message is embedded inside the photo on this way and outcomes have shown rarely any degradation within the photograph first-rate same technique can be implemented within the video file. It is pertinent to say here that this machine is the least comfy technique as message is embedded in undeniable text in harmless photographs to be transmitted to the locations. However its security lies in blending up this image with hidden message to be transmitted with heaps of other photos despatched of their normal course of movement. Thousands of pix want to be screened to find the desired photograph. It is of paramount importance to select photo; famous paintings should not be decided on, in reality regular pix have to be selected. Presently BMP pix of 800*600 pixels are not usually visible on the Internet consequently its use could be suspicious. In eight bit image, for the reason that hints to entries inside the palette changed, therefore, change of even one bit is fantastically major. Grey scale palettes because of least reported sun shades are endorsed.

SYSTEM ARCHITECTURE

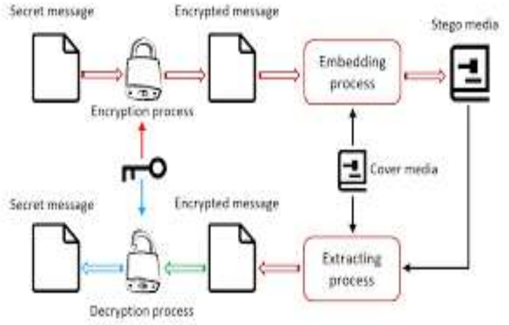

Fig.no:1

STEGANOGRAPHY Vs CRYPTOGRAPHY

Many a instances Steganography is associated with Cryptography. It can be a deceptive statement with respect to a Steganography approach. Steganography is associated with Cryptography with the aid of meaning that each are used for safety functions but with exceptional technique or implementation. Steganography is, along with Cryptography, a completely historic idea however its application varies in step with rising technologies. It is pertinent to say right here that both of these technology might not be taken as rival to each other however they are able to play a completely important role if these supplement each other.

TECHNIQUES

The steps in steganography include the writing the text messages, encryption of the textual content message is one of the alternatives available. Later, text is hidden in the selected media and transmitted to recipient. At receiver stop, reverse system is applied to recover the original text message. Various strategies used inside the art of steganography is the preparations of various bits of the characters of the textual content in an image or different media. Keeping in mind the above, documents are wanted; the image record and the textual content file that contains the information. LSB affects the smallest adjustments of the eight bits therefore it alters the photo to minimum. The maximum not unusual approach used is known as LSB (Least Significant Bit) Mechanism this is hiding if the facts in the least sizable Bit (LSB) of the message. However, one in all its primary limitations is small length of information which can be embedded in such sort of images the usage of only LSB. LSB is extraordinarily at risk of assaults. LSB techniques implemented to 24 bit formats are tough to come across opposite to eight bit format. The other strategies include Masking and Filtering. It is generally related to JPEG. In this technique image records is prolonged by covering secret statistics over it. Therefore, specialists do now not encompass this as a form of Steganography. All algorithms hired for any sort of layout have pros and cons and rely upon the environments used. It additionally depends upon the records to be embedded. Various techniques evolved were compared.

EXTRACTION

The extraction technique takes vicinity on the receiving side when the second celebration gets the Stego image and uses it with the extraction software such that the name of the game message will be extracted with none mistakes or modifications. In fashionable, the embedding method entails cover picture to mystery message to Stego photograph, whilst the extraction process runs in the opposite, in which the Stego photograph is entered earlier than the secret messages are extracted.

IV. ALGORITHMS

AES ALGORITHM

The greater famous and extensively adopted symmetric encryption set of rules probably to be encountered nowadays is the Advanced Encryption Standard (AES). It is observed as a minimum six time quicker than triple DES. A alternative for DES changed into wanted as its key length was too small. With increasing computing power, it changed into taken into consideration inclined towards exhaustive key seek attack. Triple DES turned into designed to conquer this downside however it became found sluggish.

The functions of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and layout details
- Software implementable in C and Java

OPERATION OF AES

AES is an iterative as opposed to Feistel cipher. It is based totally on 'substitution–permutation community'. It contains of a sequence of related operations, some of which involve changing inputs by using unique outputs (substitutions) and others involve shuffling bits round (diversifications). Interestingly, AES performs all its computations on bytes in preference to bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix – Unlike DES, the number of rounds in AES is variable and depends at the period of the important thing. AES makes use of 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of those rounds makes use of a distinctive 128-bit round key, that's calculated from the unique AES key.

CONCLUSION

Security mechanism in our scheme ensures the privateness of grids data in cloud storage. Encryption secures the transmission on the general public channel; confirmed security scheme make the grids information simplest accessed by means of authorized parties. The better performance in terms of storage and computation make our scheme greater sensible.

REFERENCE

[1]Tang Y, Lee P P C and Lui J C S, "Secure overlay cloud storage with access control and assured deletion," Dependable and Secure Computing., IEEE Transactions on, vol.9, no.6, pp.903-916, Nov.2012.

[2] J.Shao, R.Lu and X.Lin, "Fine-grained data sharing in cloud computing for mobile devices," in Proc IEEE Conf, Comput. Commun. (INFOCOM), Apr 2015, pp.2677-2685.

[3] Wang C, Chow S S M and Wang Q, "Privacy-preserving public auditing for secure cloud storage," Computers, IEEE Transactions on., vol.62, no.2, pp.362-375, Feb.2013.

[4]Zhang, T., Li, W., Zhang, Y. and Ping, X.; "Detection of LSB Matching Steganography Based on Distribution of Pixel Difference in Natural Images". International Conference on Image Analysis and Signal Processing (IASP), Pp.629-632, 2010.

[5] Fujisaki E and Okamoto T. "Secure integration of asymmetric and symmetric encryption schemes," Journal of cryptology., vol.26, no.1,pp.80-101, Jan.2013.

[6] Y.S.Rao, "An secure and efficient ciphertext-text policy attribute based signcryption for peosonal health records sharing in cloud computing,"Future Gener.Comput.Syst., vol.67, pp.133-151. Feb.2017.

[7] Su J S, Cao D and Wang X F, "Attribute based encryption schemes,"Journal of Software., vol.22, no.6, pp:1299-1315, Jun.2011.

[8]L.Wu, Y.Zhang, K.Choo, et al., "Efficient and secure identity-based encryption scheme with equality test in cloud computing," Future GenerationComputer Systems, vol.73, pp.22-31, 2017.

[9] Q.Xu, C.Tan, Z.Fan,et al.,"Secure Multi-Authority Data Access Control Scheme in Cloud Storae System Based on Attributr-based Signcryption",IEEE Access, vol.6,pp.34051-34074.

[10] H.He, R.Li, X.Dong, et al,"Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud," IEEE trans.on Cloud Computing, vol.2, no.4, pp.471-484, Oct, 2014.