To Propose A Novel Technique for Watermarking In Cloud Computing

Shakun Gupta, Harsimran Singh
M.Tech Students, Assistant Professor

***Abstract* - Cloud computing is one of the emerging technology which is widely used. It has many challenges in which security and privacy is the most important factor. In this work, watermarking technique has been implemented to provide data security. To implemented technique of watermarking SVD-DCT-DWT techniques has been implemented on cloud architecture. To check robustness of the watermarked data, sharpened attack, contrast attack and salt-pepper attack has been triggered and performance is analyzed with PSNR and MSE value. In proposed technique, KALMAN filter is implemented with SVD-DCT-DWT technique to improve PSNR and MSE value of the extracted image in watermarking.**

***Keywords* - Cloud architecture, Kalman, PNSR, watermarking, SVD, DCT, DWT**

I. INTRODUCTION

Cloud computing is computing that is based on the internet and it is most recent trend in IT world. In cloud computing shared information resources and software that are providing to computers and many other devices on demand. Email was probably first service on the "cloud". In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. Cloud is a technology based on internet that uses the internet and central remote servers to support data and applications. [1] By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. In Cloud computing due to network traffic and make network bandwidth more efficient introduced cloud to both infrastructure and server. With the help of Cloud Computing, users can access their databases from anywhere in the world only if they connected to the internet. Today's world depends on cloud computing to store their public data as well as personal data. That data may be required by them or others at any instant of time. As a result, data security in cloud computing has required lots of attention from the research society. Amazon played energetic role in this. IBM, google, many universities and companies adopted it [2].

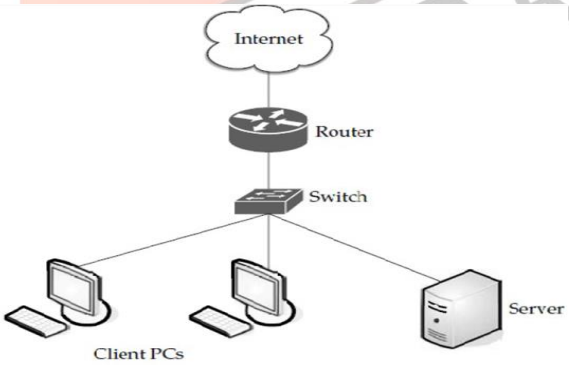

Fig 1: A cloud is used in network diagrams to depict the Internet

1.1 Service Model of Cloud Computing: There are three service model of Cloud computing:

1. Software as a Service (SaaS):In this, the consumers purchase the ability to access and use an application or service that is present in the cloud. Where applications are introduced and distributed online through a web browser proposing functionality of traditional desktop for example Google Apps and Oracle on demand.

2. Plat1form as a Service (PaaS): This service models purpose the service to the consumer as both operation and development platform. The cloud provide the software platform for system for example Google App Engine and force.com. These service models have been taken together which is also known as SPI model.

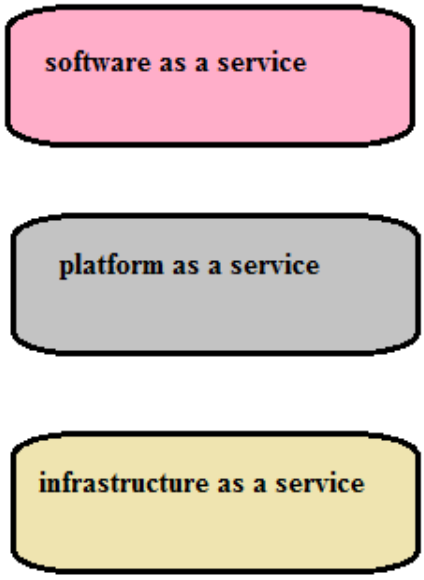

Fig 2. Cloud Computing Service Models

There are also several other service models such as Identity as a Service (IdaaS), Compliance as a Service (CaaS), and Storage as a Service (StaaS) [3].

3. Infrastructure as a Service (IaaS): The Consumers can use infrastructure as a service based service offering to organize their own operating system and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over the operating system and deployed applications. For example Amazon Elastic Compute Cloud and Simple Storage Service. For example Amazon Elastic Compute Cloud.

1.2 *Challenges of Cloud Computing:* There are some of the challenges to be faced through cloud computing.

1.2.1 Security & Privacy:The two of more hot button may issues surrounding cloud computing to storing and securing data. The cloud computing can be monitor by the service providers [4]. These issues of the cloud computing may responsible for slowing the deployment of cloud services.

1.2.2 Lack of Standards

In the cloud computing, clouds have documented interfaces. Hence responsible for sub-standard cloud computing. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices [5].

1.2.3 Continuously Evolving: The requirements of the user are changing from time to time, hence interfaces, networking and storage requirements are increased and decreased according to the need of person. This means that a cloud does not remain constant and is also continuously changing.

1.2.4. Compliance Concerns: 'The Sarbanes Oxley Act (SOX) in the US and Data Protection directives in the EU are just two among many compliance issues affecting cloud computing, based on the type of data and application for which the cloud is being used [6].

II. Review of Literature

In paper [1] author talk over the security about cloud computing. It entails the architecture of IT enterprise. The cloud computing has numerous benefits in the field of information technology: on request self service, global network access, location librated resource pooling, fast resource elasticity, usage-based pricing and conversion of risk.Cloud computing carries the fresh and inspiring security threats towards consumer's subcontracted data. For this resolution, cloud service providers are castoff. These are the distinct administrative entities. The data perfection the great matter in cloud computing. For the cloud computing, third party assessor is castoff. It customs the two for most requirements as: the third party assessor should be capable to proffesionally review the storage of cloud data without challenging the data of local copy and the reviewing process must bring in no new liabilities to the consumers privacy of data. Here author talk about the public key based homomorphism authenticator. For this the random masking is castoff. It supports to attain the privacy preserving public cloud data auditing system, which come across wholly requirements. In paper [2] author talks about the many schemes about cloud computing that are used in the security. Cloud computing indicates a paradigm shift from owning computing systems to buying the services of computing. In the given paper, author inspires the file centric adoption and logging mechanisms of data centric.It supports in growing the accountability. The cloud computing security is a big issue. So For this drive, the cloud is accesses by the data transparency and absence of clearness in data ownership were textured. For this author purpose a fresh scheme, which supports in providing cloud computing security. This new scheme finds out the numerous approaching trust problems and traditional security. So here the approach of data centric is use, which supports in increasing trust and cloud data security. In paper [3] author talks over the usages of third party auditor scheme. The technology of Cloud computing turns as architecture of next generation of IT solution. It permits the consumers to relocate their data and application software to the network that is totally different from traditional solutions. Cloud computing offers the numerous services about IT, due to which it contains several tasks of security. The security of storage of data is the big

cloud computing issue. In the given paper, author talks about a fresh scheme named auditor of third party. It supports in giving the trusted confirmation to consumer. In paper [4] author talks over the numerous approaches and processes that supports in handling the cloud computing security. The security of information is serious matter in the Internet phase. The secured information is appreciated and vital. The security of information that has been made by cloud computing handling a very important and serious matter. In cloud computing the information security requires several influences. In the given paper, the significant issues of achievement are castoff. Those issues contains several parts as: first is external dimension, second is internal dimension, third is technology dimension, and other one execution dimension. A fresh scheme is purposed by those issues, which is castoff to overwhelmed the several difficulties those are associated to the security in the cloud computing. In paper [5] discuss that present world be dependent on cloud computing to stock their public as well as some private information which is required by the user themself or some additional persons. Service of cloud is that offered services to his users by cloud. As computing of cloud arises in service there are various problems such as privacy of user's data, security of user data is very significant aspects. In this paper author discuss about the enhancement of security of the data. Not only this marks researchers to make selected alterations in the current structure of the cloud, discover new model about cloud computing and much more but also there are some features of cloud computing that mark him as a super power.To enhance the security in cloud computing used the 3 dimensional framework and digital signature with Encryption algorithm of RSA. In 3 Dimensional frameworks, at client side user choice the parameters reactively between CIA (Confidentiality, Integrity & Availability) and earlier actual storing the data in cloud a digital signature is created using MD 5 Algorithm and then RSA Encryption algorithm is applied then it stored on cloud.

III. WATERMARKING IN CLOUD

Watermark technique is the technique that we use for information hiding behind the image as it stops illegitimate manipulation of the content. When the Intended node is not capable to extract the watermark from the content, it means that alteration has been done into the content. Watermarking holds a single identity that is only known by the node of source. Images can be used to hide the data, key used to insert the data into the image is the one used for extracting the data. Data is hidden in the least significant bit of the image. It is not visible and naked eye cannot judge whether any content is hidden in the image or not [8].

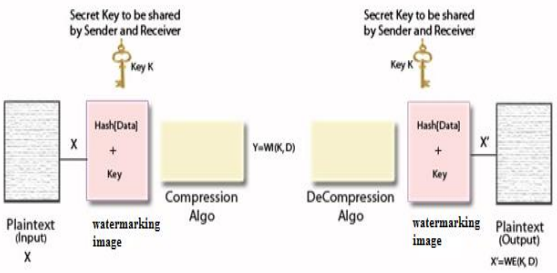

Fig 1.3 Watermarking process

At the Source End;

i. Data is embedded into an image and a key is used to lock the content into the image.
ii. Key is very essential as no key other than the one with which the data is locked can extract data from the image.
iii. It will give two images as an output that seems to be identical. But in actual, one image is the original one and the other image is the watermarked image that hid the content in it.
iv. Before the transmission of the image over the network, it is compressed as it would consume less bandwidth and other resources.
v. Compression takes place at the sender end in which dimensions of the image are made half to its actual size. It has no effect on the content hidden in it.
vi. Image is then transmitted over the network.

At the Destination End;

i. Compressed image is received at the destination end.
ii. Compressed image is then decompressed to bring the dimensions of the image back to the original size.
iii. Key used for insertion of data in the image is used at the destination end to extract the data from the image.

3.2 Algorithms for watermarking: There are many algorithms for watermarking. These are

1.Kalman Filtering: In radio communication systems, filtering is a desirable factor. As radio communication signals are often corrupted with noise, a good filtering algorithm is required to remove noise from electromagnetic signals while retaining the useful information. Kalman Filtering is an effective method to filter impurities in linear systems. The Kalman filter basically consists of a set of mathematical equations that provides an efficient computational means to estimate the state of a process that minimizes the mean of the squared error. It operates recursively on streams of noisy input data to produce statistically optimal results The filter is very powerful in several aspects: it supports estimations of past, present, and even future states, and it can do so even when the precise nature of the modeled system is unknown[9].

2. Gabor Filtering: The images are filtered using the real parts of various different Gabor filter kernels. The mean and variance of the filtered images are then used as features for classification, which is based on the least squared error for simplicity.

3. Salt and Pepper Filtering: We consider salt-and-pepper noise, for which a certain amount of the pixels in the image are either black or white (hence the name of the noise). Salt-and-pepper noise can, e.g., be used to model defects in the CCD or in the transmission of the image. Given the probability r (with $0 \leq r \leq 1$) that a pixel is corrupted, we can introduce salt-and-pepper noise in an image by setting a fraction of r/2 randomly selected pixels to black, and another fraction of r/2 randomly selected pixels. The anti process will be followed to retrieve data. User will use anti-watermarking algorithm to retrieve key then use one detection algorithm to fetch information from image and by using this key user will decrypt it [10].

IV. PROPOSED METHODOLOGY

The main problem cloud computing faces today is to preserve confidentiality and integrity of data. Organizations use cloud in a variety of different service models and deployment models. A large number of security issues are associated with cloud computing, these are issues faced by cloud service provider and security issues faced by their customers. Some of these issues are:

- Privacy
- Trust
- Multi-tenancy
- Key management
- Lack of user control

As cloud computing which brings many benefits when occurs as platform of resource sharing. It also hosts major security concerns. In our work the technique of watermarking had been applied in cloud computing. The watermarking technique had provide extra security to cloud data. In this work, The data received by the end user, the user extract the original data from the watermarked data some noisy data left behind which increase MSE value and reduce PSNR value. In proposed work first we have apply some attacks like sharpened attack, contrast attack and salt & pepper attack on original image to check the robustness of the image. After that to remove noise from that data, technique of KALMAN filter had been applied. The Kalman filter helps to decrease the value of MSE and increase the value of PSNR so that the quality of the watermarking image can improve. The kalman filter has helped to increase the quality of the watermarking image as well maintaining its security.

V. EXPERIMENTAL RESULTS

The whole scenario has been implemented on MATLAB.

VARIATIONS	PSNR	MSE
SVD-DWT-DCT	30.05	65.05
SHARPENED ATTACK	30.01	65.49
CONTRAST ATTACK	24.09	244.29
SALT & PEPPER ATTACK	30.04	64.87
KALMAN FILTER/ONE DIMENSION	30.05	65.03
KALMAN FILTER/TWO DIMENSION	33.02	32.72

Fig. 4: Comparison of PSNR AND MSE values of existing approach

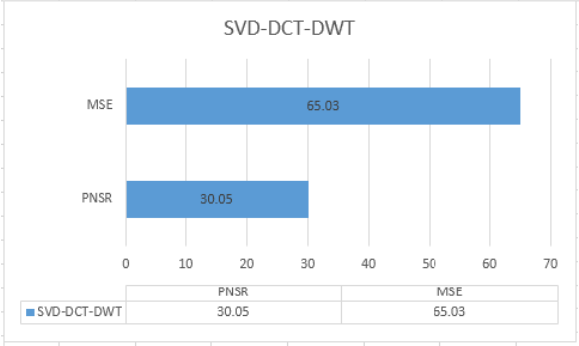

Fig. 5 PNSR and MSE value of existing SVD-DCT-DWT technique

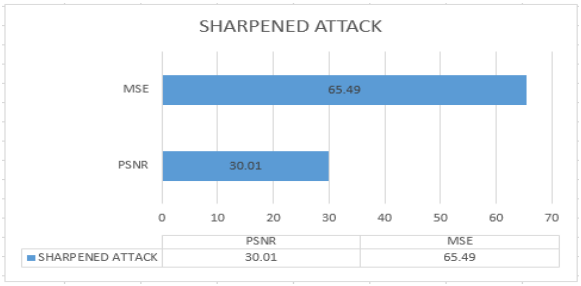

Fig.6: PSNR and MSE value of sharpened image.

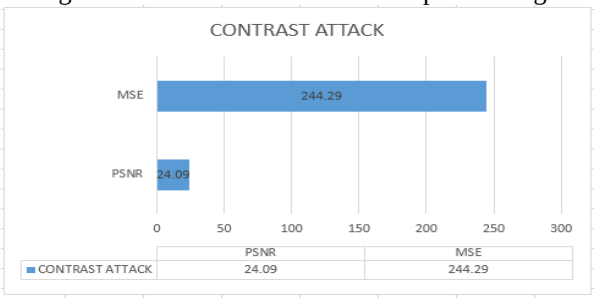

Fig.7 PSNR and MSE value of contrast image

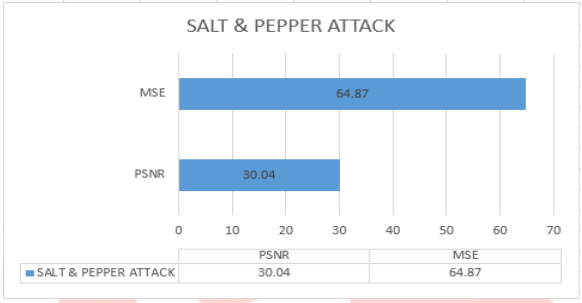

Fig.8 PSNR and MSE value of image after applying SALT & PEPPER attack

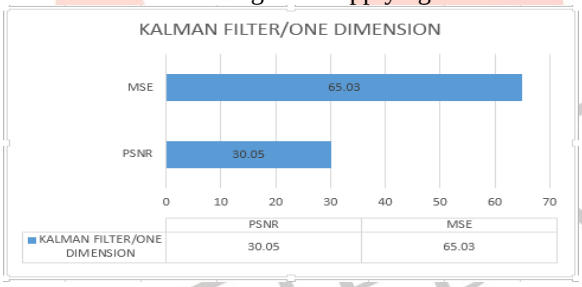

Fig.9: PSNR and MSE value of the extracted image in watermarking after implemented with Kalman Filtering

VI. Conclusion

In this work cloud computing architecture has been implemented with certain number of users. The users can present their credentials to the cloud services provider and cloud service provide access to users. In this work, watermarking technique has been implemented to provide data security. To implemented technique of watermarking SVD-DCT-DWT techniques has been implemented on cloud architecture. To check robustness of the watermarked data, sharpened attack, contrast attack and salt-pepper attack has been triggered and performance is analyzed with PSNR and MSE value. In proposed technique, KALMAN filter is implemented with SVD-DCT-DWT technique to improve PSNR and MSE value of the extracted image in watermarking. In future other filtering techniques like Gabor filter has been implemented with KALMAN filter to further improve PSNR and MSE value.

VII. References

[1] Cong Wang, Qian Wang, and Kui Ren Wenjing Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, 978-1-4244-5837-0/10/$26.00 ©2010 IEEE

[2] Ryan K. L. Ko, Markus Kirchberg, Bu Sung Lee , From System-centric to Data-centric Logging Accountability, Trust & Security in Cloud Computing

[3] Shuai Han, Jianchuan Xing, ensuring data storage security through a novel third party auditor scheme in cloud computing, Proceedings of IEEE CCIS2011

[4] Jen-Sheng Wang, Che-Hung Liu, Grace TR Lin, How to Manage Information Security in Cloud Computing,2011

[5] Pradeep Bhosale Priyanka Deshmukh Girish Dimbar Ashwini Deshpande , Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012

[6] Jasmin James, Dr. Bhupendra Verma, efficient VM load balancing algorithm for a cloud computing environment, Jasmin James et al. International Journal on Computer Science and Engineering (IJCSE)
[7] Pengfei Dai et.al, A Software Watermark Based Architecture for Cloud Security, 2012
[8] Tejinder Sharma, Vijay Kumar Banga. Efficient and Enhanced Algorithm in Cloud Computing, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013
[9] Sonal Guleria1, Dr. Sonia Vatta2, to enhance multimedia security in cloud computing environment using crossbreed algorithm, Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com, Volume 2, Issue 6, June 2013
[10] Yan Yan, Xiaohong Hao, privacy security issue under mobile cloud computing mode (CCIT-14) ISBN: 978-90786-77-97-0, January 2014