Analysis of Various Security Techniques of Cloud Computing: A Review

Pratul Sharma, Brajesh Kumar Singh
Deptt. Of Computer Science & Engineering
R.B.S Engineering technical Campus, Bichpuri, Agra

Abstract:

The cloud computing has the distributed nature in which data is stored on the multiple virtual servers. The clients from the different regions interact with the cloud service provide to access data from the virtual servers. The various security algorithms are proposed by the various authors and these algorithms are broadly classified into fully disk encryption and fully homomorphic encryption schemes. The other techniques techniques for the cloud data are watermarking, stenography etc. In this paper, various security algorithms are reviewed and analyzed in terms of various parameters.

KEYWORDS

Fully Disk Encryption, Fully Homomorphic encryption, Watermarking, stenography

Introduction

A public or private type of connections amongst large pool of systems in order to facilitate scalable infrastructure for an application is known as cloud computing. Huge amount of data and files are stored and extracted as per requirement within cloud computing applications. There is a significant reduction in the computation host, hosting of application and the delivering and storage of content within this technology [1]. Direct cost benefits are provided within the cloud computing applications in which the variable priced environment is setup on the basis of number of facilities used by the users. The basic methodology on which the cloud computing is based on is the reusability of IT capabilities. There are various service-models present within cloud computing. On the basis of demand for a service, an application is provided to the user with the help of Software as a Service (SaaS) model. On the cloud there is a single instance of service made to run through which services are provided to numerous end users. The customers here do not need any kinds of servers or software licenses. The encapsulation of a layer of software or development environments in order to be provided as a service is provided in Platform as a Service (PaaS) [2]. Higher levels of service can be generated on the basis of this encapsulated service. The applications that are possible to run on infrastructure of a provider can be built by the customer within his own applications. The standardized services are provided over the network through Infrastructure as a Service (Iaas) which provide storage and computing services to various users. On the basis of requirements of the customers, the cloud computing technique can be deployed within various applications. There are four different types of deployment models which have different characteristics through which the numerous services can be supported. In order to facilitate the requirements of a particular organization, the deployment of maintenance of cloud infrastructure is done with the help of private clouds. The users can access the cloud infrastructure publically or commercially with the help of a cloud service provider [3]. A service is developed and deployed by the customer within a public cloud which includes very less financial support in comparison to the requirements that are related to other deployment facilities which have high capital expenditure. In the hybrid applications, the private and public clouds are combined together in order to provide various requirements. These requirements are accessed by some organizations which require such complex services. Such services are provided within this cloud.Within cloud computing there are numerous challenges amongst which some are explained below. Some challenges might degrade the performance of some services within the cloud. However, there are several such challenges which might also provide several opportunities when they are resolved very carefully within the applications [4]. The data can be stored and secured with the help of few numbers of hot buttons present around the cloud computing. With the help of service providers the utilization of cloud can be monitored. The speed of deployment of cloud services can be minimized due to the presence of such issues. In case where such situation occurs in which the data is stored within the organization but is accessed within the cloud as well causes privacy issues. Robust cloud is to be required in order to provide such exchange of information within the organization and cloud. Such type of deployment can be supported by the hybrid cloud. There are no standard related to the clouds which have document interfaces present within them [5]. Thus, the clouds are interoperable in such conditions. Such issues can be resolved by developing an open cloud computing interface within these applications. The cloud computing standards and practices are presented on the basis of which the Open Cloud Consortium works. The requirements of the users, interfaces, networking as well as storage are evolving continuously. Thus, the public cloud especially in such conditions is not static and keeps evolving

in continuous manner. The embedding of information directly within the digital data which is also known as raw or host data in order to generate a watermarked data from it is known as digital watermarking technique. The insertion of group of bits within the digital data file is known as watermarking. This can help in copyrighting the information present on the file. The original data can be hidden from the external users with the presence of watermarked data on that source.On the basis of different types of documents present, the digital watermarking techniques are classified into various categories [6].They are:

a. Text Watermarking: in order to provide copyright protection to the text document, this approach is used. There are 3 types of digital watermarking provided here:

- Line shift coding: The vertical shifting of location of text lines in order to encode the document is provided by this method.
- Word shift coding: The document can be encoded through the horizontal shifting of the location of words.
- Feature coding: Specific features are selected here and alerted within this method.

b. Image Watermarking: Within the image derivatives, a watermark is added with the help of this method. It is not easy to remove the watermark from the image as it is already a part of that image.

c. Video Watermarking: The cryptographic information that is generated from the frames of digital video is used to provide the cryptographic information. This generated cryptographic information is embedded within the some video in this process. Amongst the original, unmarked and marked video, the user cannot easily differentiate. However, this watermark can be read with the help of watermark extraction application which can further result in attaining the embedded information. This technology is very different from the video file format as it is part of the video and not any other file [7].

d. Audio Watermarking: Within the audio signal, an electronic identifier is embedded within this approach. Within the audio file, the text or images are used to be embedded in such a manner within various techniques which can help in recovery of the text.

Within the data the watermark is embedded and further this data is stored within the database of the systems. A unique key is utilized further along with the source data to retrieve the database. This results in achieving the integrity of data by verifying the integrity of this data with the extracted watermark's integrity.An intruder is recognized through fingerprinting method. The owner of the data would impose restrictions such that his data cannot be accessed by any unauthorized user across the network in case when the data is present publically.A digital identification can be embedded within the critical documents and images with the help of digital watermarking technique. The data from the original source or from the owner can be utilized to generate watermark data.Within all types of contents which are in the form of image, audio and video, the watermarks are embedded. The secret type of information which cannot be seen or heard by humans however, is easy to be identified by the computers is known as watermark. The watermarked content can be located in a unique manner with the help of various internet search services.

2. Review of Literature

Abid Khan, et.al (2017) presented in this paper [9], that in order to provide details of the previous events and help in monitoring, troubleshooting and forensics of the system the logs are utilized within the systems. A secure way should be followed in order to provide logging process such that the facilities can be used here. A secure log as a service reversible watermarking (SecLaaS-RW) method is proposed in this paper. In order to authenticate the content, the fragile watermarking method which is reversible watermarking is utilized. Within the extended period of time here all the records are saved. This proposed method is compared with the existing approaches. Results are achieved here on the basis of which the performance of proposed method is analyzed. As per these results, the proposed technique generates very less amount of overhead per log entry and from the outsourced logs, the changes can be identified through this technique.

Rita Choudhary, et.al (2016) presented in this paper [10], that there is an increase in demand of the robust and high quality of watermarking techniques as per the increment in growth of the digital data across the internet. The binary or grayscale watermark is embedded within the cover image or other multimedia images with the help of image watermarking methods. In order to insert the watermark in the low frequency component of the host image, the variable visibility factor is utilized within this technique. The 2-level is utilized in order to propose a DWT-based image watermarking technique in this paper. The comparison of various parameters like PSNR and NCC is done with relation to the 1-level DWT method. Within the simulation results, the enhancement is shown in comparison to the results achieved from existing techniques which shows the level of enhancement achieved here.

Mr. Y. Gangadhar, et.al (2016) presented in this paper [11], that various things have been converted into digital format on the basis of various enhancements made within the computer network and multimedia fields from past few years. A comprehensive survey on various digital watermarking

methods has been presented in this paper. An overview of various existing techniques is presented in this paper along with the various disadvantages being faced due to the presented of various types of attacks in the applications. Due to the robust nature of this technique, various geometric based watermarking methods are presented in this paper also. An effective study of the geometric invariant methods is provided in this paper which can help in further enhancing the watermarking research field here.

Ahmed S. Salama, et.al (2016) presented in this paper [12], a technique which utilizes less execution time and facilitates better imperceptibility in the applications. This technique will also help in enhancing the robustness in comparison to already existing digital watermarking techniques. The Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) techniques are combined here in order to generate improved technique (IMD-WC-T). With the help of PN-sequence and a specific key within the DCT transform, the watermark is spread. Further, the final watermarked image is generated by decomposing the host image with DWT within the level 2. An additional imperceptibility, minimized execution time and higher robustness is provided within the IMD-WC-T technique as per the results generated when this technique is compared within other existing techniques.

Mr. R. D. Shelke, et.al (2016) presented in this paper [13], the study related to numerous audio-watermarking techniques that will help in advising the owner to use the appropriate technique using the watermark within their image, audio or video data. It is very difficult to eliminate watermark from the data. The newly proposed algorithms have the main objective to enhance the already existing methods. Thus, the performance of the proposed algorithm can be enhanced and the complexity can be minimized along with the cost with the

utilization of new techniques. Thus, all such techniques are compared in order to gather a view regarding the benefits and disadvantages of various techniques which can help in understanding as to which technique can be useful at certain scenario.

Chengxiang Yin, et.al (2015) proposed in this paper [14], a novel approach which is introduced with the combination of cloud computing and audio watermarking. This approach helps in generating an innovative advertising technique which uses the background of music that is played within the public places for its execution. There were various experiments illustrated in this paper which help in analyzing the performance of proposed technique on the basis of various platforms and test the feasibility of this approach. The effectiveness of the system is also proved on the basis of usability test.

Muhammad Imran et.al (2016) proposed in this paper [15], a novel technique which is known as blind color image watermarking technique. The decomposition and principal component analysis techniques are utilized in this paper in order to propose this technique. During the designing of proposed technique, the robustness, imperceptibility, capacity as well as security are the mainly focused on. In terms of imperceptibility, there is an enhancement seen with the application of principal component analysis. Further, the robustness and capacity of the system are enhanced in order to provide better results due to the presence of singular value decomposition. Various experiments were performed to evaluate the performance of proposed method. Various color images were utilized here as host and watermark in order to perform the experiments. Comparisons were made amongst various techniques and it was seen that the proposed method outperformed various other methods.

Author's Name	Year	Description	Outcomes
Abid Khan,	2017	A secure log as a service reversible watermarking (SecLaaS-RW) method is proposed in this paper. In order to authenticate the content, the fragile watermarking method which is reversible watermarking is utilized.	As per these results, the proposed technique generates very less amount of overhead per log entry and from the outsourced logs; the changes can be identified through this technique.
Rita Choudhary,	2016	The 2-level is utilized in order to propose a DWT-based image watermarking technique in this paper.	Within the simulation results, the enhancement is shown in comparison to the results achieved from existing techniques which shows the level of enhancement achieved here.

Mr. Y. Gangadhar,	2016	An overview of various existing techniques is presented in this paper along with the various disadvantages being faced due to the presented of various types of attacks in the applications.	An effective study of the geometric invariant methods is provided in this paper which can help in further enhancing the watermarking research field here.
Ahmed S. Salama,	2016	The Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) techniques are combined here in order to generate improved technique (IMD-WC-T).	An additional imperceptibility, minimized execution time and higher robustness is provided within the IMD-WC-T technique as per the results generated when this technique is compared within other existing techniques.
Mr. R. D. Shelke,	2016	The newly proposed algorithms have the main objective to enhance the already existing methods. Thus, the performance of the proposed algorithm can be enhanced and the complexity can be minimized along with the cost with the utilization of new techniques.	All such techniques are compared in order to gather a view regarding the benefits and disadvantages of various techniques which can help in understanding as to which technique can be useful at certain scenario.
Chengxiang Yin,	2015	A novel approach is proposed in this paper which is introduced with the combination of cloud computing and audio watermarking.	There were various experiments illustrated in this paper which help in analyzing the performance of proposed technique on the basis of various platforms and test the feasibility of this approach. The effectiveness of the system is also proved on the basis of usability test.
Muhammad Imran	2016	A novel technique is proposed here which is known as blind color image watermarking technique. The decomposition and principal component analysis techniques are utilized in this paper in order to propose this technique.	Comparisons were made amongst various techniques and it was seen that the proposed method outperformed various other methods.

3. EVALUTION AND ANALYSIS

Mapping Study Plan Execution:

In this column, the description of the plan for execution is given step wise.

A. Conduction of Search

The various data bases like IEEE Xplore and Springer are searched with different strings and it is found that total number of 328 research papers have been published in the recent years. In the table 2, the individual database results are given.

TABLE 2: SEARCH STRING RESULT OF VARIOUS DATABASES

INDEX	DATABASE	RESULT
1	IEEE Xplore	143
2	Springer	185
TOTAL		**328**

B. Criteria for Efficient Result Extraction

The study is being conducted to check the authentication of the 328 papers which are searched with the search string criteria from the different databases. The 328 papers have been put into the plagiarism checker tool and we are only left with 223 papers which are unique and not copied from anywhere. The unique papers are analyzed manually and it is found that only 115 papers which represent different security techniques for the watermarking and remaining papers are based on other cloud security techniques. The search string is based on security analysis. In the end result we achieved only 40 papers which represent the cloud security

C. Results

This step illustrates the data of paper publication year wise.

- *Year*
  In the figure 1, it shows the percentage of papers which are being published from 2014 to 2017.

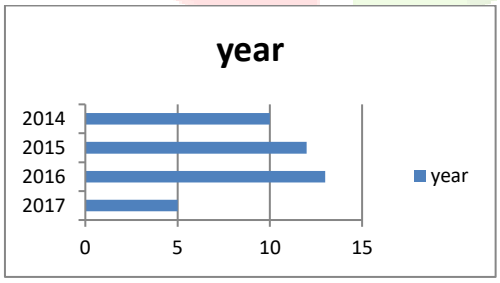

Fig. 1 Percentage of papers published year wise

- *Country of Authors*
  The contribution of authors from China is 25% and rest 30% is published by the European authors. 45% papers have been published by the India authors.
- *Published in Conference or Journals*
  In the Fig 2, it shows the percentage of papers published in Conference or Journals. From the data which is collected from the search string, it is being analyzed that 60% of the papers have been published in the conferences and rest of the 40% papers have been published in journals.

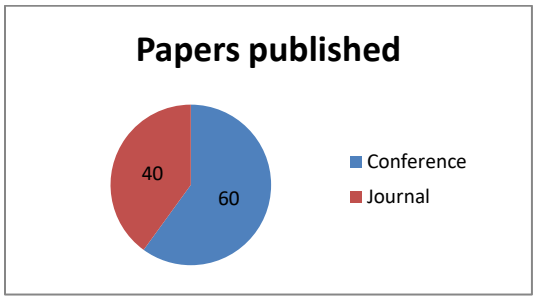

Fig. 2 Paper published for Research

Conclusion

In this work, it is concluded that the security is major concern of cloud computing. The security techniques has been proposed by the various authors to increase security of the cloud computing. The watermarking, stenography are the advance type of security techniques of cloud computing. In this review paper, various watermarking, stegnography and encryption techniques are compared , analyzed in terms of various parameters.

References

[1] U. Yadav, J. P. Sharma, D. Sharma and P. K Sharma, "Different Watermarking Techniques And Its Applications: A Review", International Journal Of Scientitlc And Engineering Research, vol. 5, no. 4, (2014) April.

[2] Chih-Chin Lai and Cheng-Chih Tsai, " Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 59, NO. 11, NOVEMBER 2010.

[3] C.-C. Lai and C.C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 11, (2010) November.

[4] M. Narang and S. Vashisth, "Digital Watermarking using Discrete Wavelet Transform", International Journal of Computer Applications (0975 - 8887) vol. 74, no. 20, (2013) July.

[5] Salama, A., Atta, R. , Rizk, R. , Wanes, F., "A robust digital image watermarking technique based on wavelet transform". In: IEEE Int. Conf. on Sys. Eng. and Tech., pp. 100-104 (2011).

[6] Ahmed S. Salama, Mohammed A. AI-Qodah, Abdullah M. T1iyasu, Awad Kh. AI-Asmari and Fei Yan: A Hybrid Fusion Technique for Watermarking Digital Images: Advances in Intelligent Systems and Computing Volume 240, pp 207-217, (2014).

[7] lliyasu, A., Le, P., Dong, F. , Hirota, K.: Watermarking and authentication of quantum images based on restricted geometric transformations. Information Sciences 186(1), 126-149 (2012). 562

[8] AI-Asmari, A., Salama, A., T1iyasu, A., AI-Qodah, M.: A DWT ordering scheme for hiding data in images using pixel value difference. In: IEEE Eighth Int. Conf. on Computational Intelligence and Security (CIS), pp. 553-557 (2012).

[9] Abid Khan¬, Ayyaz Yaqoob, Kinza Sarwar, Mouzna Tahir, Mansoor Ahmed, "Secure Logging as a Service Using Reversible Watermarking", The 12th International Conference on Future Networks and Communications, (FNC-2017)

[10] Rita Choudhary, Girish Parmar, "A Robust image Watermarking Technique using 2-level Discrete Wavelet Transform (DWT)", IEEE 2nd International Conference on Communication, Control and Intelligent Systems (CCIS)

[11] Mr. Y. Gangadhar, Dr. V. S. Giridhar Akula, Dr. P. Chenna Reddy, "A Survey on Geometric Invariant Watermarking Techniques", 2016 IEEE

[12] Ahmed S. Salama, Mohamed Amr Mokhtar, "Combined Technique for Improving Digital Image Watermarking", 2016 2nd IEEE International Conference on Computer and Communications

[13] Mr. R. D. Shelke, Dr. Milind U. Nemade, "Audio Watermarking Technique Protection: A Review", 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication

[14] Chengxiang Yin, Jin Hu, Xuejun Zhang, Xiang Xie, "Advertising system based on cloud computing and audio watermarking", 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing

[15] Muhammad Imran and Bruce A. Harvey, Adnan Ali Memon, "A Novel Blind Color Image Watermarking Technique Based on Singular Value Decomposition and Principal Component Analysis", 2016, The Sixth International Conference on Innovative Computing Technology