Ownership Identification of Multimedia Content Prediction on a Large Scale

Ch.Sai Lakshman, Saravanan.M.S

Abstract: ***This article prepared with three main objectives, first it is to review the large size of multimedia file protection, second for ownership identification of the multimedia content and finally for implementing this setup for cloud based setup instead of web based service architecture. Therefore many of the infrastructure developed for multimedia content to enable the security against the file handling services for managing the better ownership identification. On private and/or public clouds, the device can be deployed. Our framework has two new components: (i) method of producing 3-D image signatures, and (ii) distributed multimedia object matching engine. The signature method produces stable and accurate 3-D video signatures capturing the depth signals in those videos as well as computationally efficient processing and comparison and having limited space. The corresponding distributed engine is highly scalable and designed to support different multimedia objects. We have introduced and deployed the proposed system on two clouds such as private and amazon based clouds.***

Keyword: Multimedia content, 3D videos, Images, Signature method, Amazon cloud.

I. INTRODUCTION

On cloud infrastructures, we are presenting a new platform for multimedia content protection. You can use the system to protect different types of multimedia files such as pictures, moving images, video and audio content related files also some small size clips of audio and video clips. The ownership of the content is not able to identify easily due to high volume of data on cloud with various privacy leakages but in real time the end users are expecting their data stored on cloud storage and even their server databases, hence it is a question to give better service to the user to provide the right data when they are retrieving the information. In this article, the new mechanism or framework proposed to prevent the security breach and reliable service [1].

The framework has many components, they are software, network and technology. First we will discuss about the software. The software is the one, which can access the data or information from the stored databases, it act as a tool to download the upload the file on the traditional databases or cloud enabled databases such as firebase. The second one is the technology, this can help the data enabling service provider such as public and private digital subscribers. If the technology is slow the data retrieval process have low performance on the other hand has high performance. Finally the network connectivity also an important part of the setup this enables, ownership identification against the multimedia files. The proposed framework has complex structure of multiple sizes and varieties of files with high velocity. This enables the service for generating high end data authorization facility bundled within the data retrieval processing. The originality of the multimedia content can be analyzed using signature based approach.

The proposed system implemented with fifty 2D videos and ten audio files using amazon cloud service provider. This deployment has high efficiency program model to demonstrate the setup with various computing resources and network costs. The same scenario can be used to protect identify the less network resources through many complete testing with actual deployment. This model produces high accuracy in terms of scalability and high precision with elasticity of the cloud services. The network resources has many limitations, even we have many constraints on data analysis and it will allow many precision in terms of accuracy and recall.

II. RELATED WORK

When a source node has common information for two recipients, the fading channel of confidential messages (BCC) is checked and confidential information is intended for one recipient only. The recipient-two confidential information shall be kept as secret as possible. In addition to the additive Gaussian noise terms, multiplicative fading gain coefficients corrupt the high end data sources which can help the multiple receivers to analyze the authentication process [4].

It is identified that the channel state need to maintain with security constraints due to intruders in the network. The first method for separating the channels with high end information retrieval process with fading the sub channels. The productivity of the system can be identified with privacy values for authorization of multimedia content, the fading of secrecy can be compressed with various algorithms used to provide security from the third person and definitely allows the owner to secure his data with minimal cost of maintenance.

The architecture of the system can be minimized with less management parameters such as memory, speed and technology.

The region of every part of the multimedia content applied on core Gaussian technology to predict the confidentiality of the training multimedia content. The ergotic secrecy capability is used to allow the boundary analysis of every zone. The power full allocation of the message analysis can be reduced due to limited edition of memory allocation and the boundary of each compression techniques.

The region of secrecy capacity is then established for the parallel Gaussian BCC and the optimal allocation of

Revised Manuscript Received on April 15, 2020.

Ch.Sai Lakshman, student, Department of Data Science and Computational Intelligence, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Tamil Nadu.

Dr.Saravanan.M.S, Professor, Department of Data Science and Computational Intelligence, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Tamil Nadu

source power that reaches the boundary of the region of secrecy capacity is derived. Especially for the basic Gaussian BCC, the secrecy capacity region is established.

The region of secrecy capability is built particularly for the core Gaussian BCC. The tests of the capability of confidentiality are then extended to the analysis of the disappearing BCC. First of all, they study the ergodic performance. It gets the area of ergodic secrecy capability and the optimum power allocations that reach the boundary of this zone. The power output is then evaluated, where it is believed that there will be a long-term energy limit. Power allocation is extracted which minimizes the likelihood of failure where either the common message target rate or the confidential message target rate is not reached.

This paper provides a comprehensive analysis of the security physical layer domain of multi-user wireless networks [4][9]. The basic principle of physical layer security is that sensitive messages can be transmitted over a wireless network in the presence of unauthorized eavesdroppers, without relying on higher-layer encryption.

Secret-key generation and organization protocols are subsequently protected on the basis of structures of physical substrate. Secrecy approaches based on the design of channel coding and a review of interdisciplinary approaches based on game theory and stochastic geometry are then explored [10].

III. OBSERVATIONS ON RELATED WORK

Academia and industry have attracted considerable attention to the issue of protecting multimedia content of different types. One approach to this issue is the use of watermarking, where the content itself contains some distinguishing data and a tool is used to check for this information to verify the validity of the content.

The digital watermarking is the technique, which can provide multiple object identification to find the presence of water marks on the picture of image. This method can give more accurate matching materials already published without watermarks.

The water marking approach has many role on information security, particularly the heterogeneous environments will provide the different multimedia content identification to utilize the special custom image protection and custom games. In day to day web world, the online contents such as audio and video files are the most valuable data are particularly need this information security.

This paper's focus is not on watermarking. The following are the drawbacks of the existing system, including massive space, poor reliability and scalability, loss of revenue for content creators, and multimedia content available on the Internet, and the difficulty of comparing material to distinguish copies.

IV. OWNERSHIP IDENTIFICATION AND SIGNALING OF MULTIMEDIA CONTENT COMPONENTS

The ownership of the multimedia content can be provided with multiple complex information security features such as multimedia analysis of hosting sites with image, audio and video files. In distributed systems the multimedia files are used spread across the network and the single node control is not possible. Hence the query against the each defined networks need more deep information security analysis.

For the second and third components, we propose novel methods, and we use off - the-shelf tools for the crawler. With more than 11,000 3-D videos and 1 million images, we have developed and tested a complete running system of all components. The figure 1 shows the various multimedia content on different platforms.

In figure 1, it is shown that the different multimedia content handled on various platforms, here the platforms are the dependence on each independent multimedia content, due to large amount of data located on various locations. The location based multimedia content has different water marking and security algorithms embedded on it. Hence security of the multimedia content has large deep analysis for finding the original content right for ownership identification.

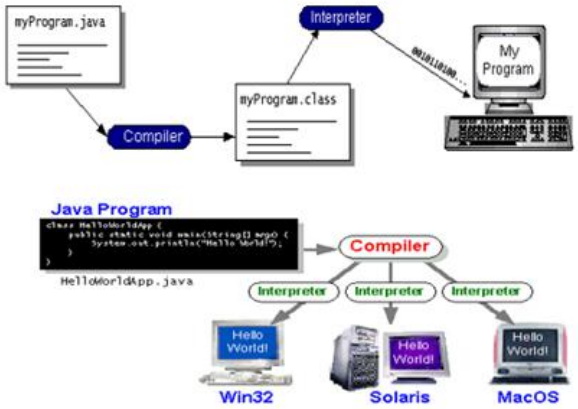

Figure 1: The architecture of the distribution of multimedia content on various platforms

Table 1. Classes of watermarking applications

Application Class	Purpose of the embedded watermark	Application Scenarios
Protection of Intellectual Property Right.	Conveys information about content ownership and intellectual property rights.	Copyright Protection, Copy Protection, Fingerprinting.
Content Verification.	Ensures that the original multimedia content has not been altered, and or helps determine the type and location of alteration.	Authentication Integrity Checking.
Information hiding.	Represents side-channel used to carry additional information.	Broadcast Monitoring System Enhancement.

The above table 1, shows the various classes of watermarking applications, in the column of applications classes such as protection of intellectual property right, content verification and information hiding. The second column has the purpose of the embedded watermark such as conveys information about content ownership and intellectual property rights, ensures that the original multimedia content has not been altered and or helps

determine the type and location of alteration and represents side channel used to carry additional information and the final column has the copy right protection, copy protection, finger printing, authentication integrity checking and broadcast monitoring system enhancement.

V. CONCLUSION

The media fingerprinting method in is adopted to check the quality of ownership recognition. In addition to TRECVID's benchmarking dataset, a new large-scale dataset with more natural editing operations such as video concatenations has been built. A 3-minute clip is an audio or video sample. And as test sets, 10,000 samples of various transformations are used for each type of media. Presents experimental results of recognition of possession. The speed of extraction and querying of fingerprints is fast. As for the identification of ownership, the accuracies imply relatively high low false alarm and missing rates show that concatenated video clips can be detected and located accurately.

REFERENCE:

1. Y. Liang, H. V. Poor, and S. Shamai, Secure communication over fading channels, IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security, November 2006.
2. Saravanan.M.S, Thirumoorthy "Signature Based Intrusion Detection in Cloud Based Multi-Tenant System using MTM Algorithm" Published in ARPN Journal of Engineering and Applied Sciences by Asian Research Publishing Network ,India, Vol.10, Issue.14, Aug' 2015, pp.5764-5769, ISSN:1819-6608.
3. E. Lin, A. Eskicioglu, R. Lagendijk, and E. Delp, "Advances in digital video content protection," Proceedings of the IEEE, vol. 93, no. l, pp. 171-183, 2000.
4. I. Cox, M. Miller, J. Bloom, "Digital Watermarking," Morgan Kaufmann Publishers, 2001.
5. D. Zheng, Y. Liu, J. Zhao, and A. E. Saddik, "A survey of RST invariant image watermarking algorithm," ACM Comput. Surv., vol. 39, no. 2, pp. 1-91, 2007.
6. Saravanan.M.S, Shafiya Banu, "Building Private Cloud Infrastructure and Related Issues for Healthcare System", Published in International Journal of Applied Engineering Research by Research India Publications, India, Vol.10, Issue.4, March'2015, pp.3040-3045, ISSN:0973-4562..
7. L. Mou, T. Huang, Y. Tian, M. Jiang and W. Gao, "Content-based copy detection through multimodal feature representation and temporal pyramid matching," ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 10, no. 1, 5:1-5:20, 2013.
8. L. Mou, T. Huang, L. Huo, W. Li, W. Gao, X. Chen. "A secure media streaming mechanism combining encryption, authentication, and transcoding." Signal Processing: Image Communication, 24(10):825-833, 2009.
9. Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, pp. 436-444, May 28, 2015.
10. Y. Bengio, A. Courville and P.Vincent, "Representation learning: a review and new perspectives," IEEE Trans. Pattern Anal. Machine Intell. 35, 1798-1828, 2013.