1st International Conference on Applied Soft Computing Techniques
22 & 23.04.2017
In association with
International Journal of Scientific Research in Science and Technology

Enhancing Social Video Services in Multi Cloud Using Distributed Graph

G. PrabuKanna, G. VijayaLalitha
Department of Information Technology, Kalasalingam University, Krishnankoil, Tamil Nadu, India

ABSTRACT

Cloud Computing is the emerging technology used to store and share data to various users. Online social network and videos which are generated by users are growing well in today's trend. Those social videos are hostedin cloud which is turning into a standard to give out the users, who generated and stored their contents in cloud. The crucial issue of cloud based video content sharing is that users found expansively, and they are not provided with good service provider. We proposed an algorithm in this paper, pixel permutation, to share social video to multi cloud providers and provide security to the video content as well as solution to the optimization problem. We exhibit the social video qualities and the tradeoff between them is uncovered for fulfilling the users and reducing the data transmission. Finally, the result is compared with the existing encryption algorithm and proved that the proposed algorithm is providing more security and the time required for processing is low when compared to existing algorithm. These are implemented using CloudSim and proved that proposed technique gives better result than the existing technique when compared to time and performance.

Keywords: Cloud Computing, Social Video, Cloud Service Provider, Pixel Permutation

I. INTRODUCTION

Now a day's the internet plays an important role in all places. Cloud computing is a term utilized for conveying the facilitated benefit over the web. Users are utilized to store their information in cloud. Cloud computing refers to the applications which are distributed as service over the Internet. Cloud is also defined as the datacenter with hardware and software. Cloud computing is used to use applications without installing it. With the help of Internet, users can access their datas and files anywhere and anytime.

Figure 1 represents the various challenges faced by cloud computing. Thus in this paper, need for security for the data stored in cloud and the allocation of the data to the cloud are presented in balanced manner and discussed below.

The information may be of text, image and video format. In future, video files will be progressively overwhelming today's traffic and all network traffic in 2018 will be video based. The encryption is the procedure used to scramble the information, which is shared to give security. First, the key value is generated and shared between sender and receiver. The sender first scrambles the data, utilizing the key as of now produced, so that the other persons are not able to find the original text. The receiver on the opposite side can unscramble the substance just by giving the right key. This is mainly used for all multimedia content, for example, text, image and video. There are different techniques required to encrypt and decrypt the data. This paper presents an alternate cryptographic approach to offer security to the video files that are stored in cloud and transmitted between the sender and receiver.

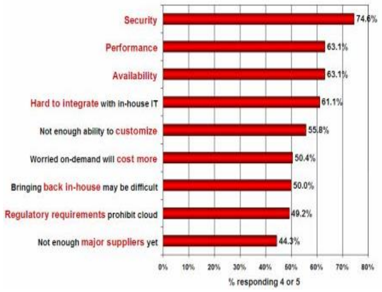


Figure 1. Cloud Computing Challenges

The various advantages of cloud computing are with the help of Internet the user can access, configure and manipulate applications. It is no necessary to install specific software to access or manipulate applications. It offers on-demand services to the users. It also offers load balancing.

RESOURCE ALLOCATION TECHNIQUE

The main technique used in this paper is Resource allocation. It is the process of assigningexisting resources to the cloud through the Internet. It resolves the problem by letting the service providers to accomplish the resources for specific module.Resource allocation strategy is about integrating cloud provider actions for exploiting and allotting resources within the cloud environment. The below diagram represents the resource allocation strategy in cloud.

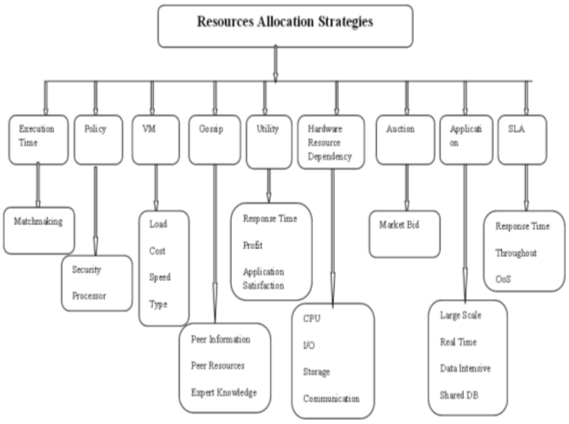


Figure 2. Resource Allocation Strategies

CLOUD COMPUTINGSECURITY ISSUES

Another process presented in this paper is cloud security issues. The issues confronted are:

1. Data issues

The first thing is the data in cloud can be retrieved anywhere and anytime by anyone. The service provider access and change the data using the data integrity methodin cloud. Then the second one is data stealing. Most of the users use other service providers because of its high cost. The third one is data loss. This is due to its financial or legal problem.

2. Privacy issues

The service provider makes sure that the datas are stored with high security and observing that who is maintaining and accessing the data.

3. Infected issues

The cloud service providers have all the rights to monitor and maintain the server. This will prevent malicious action by user from uploading wrong information on to the cloud, which may affect the services.

4. Security issues

The service provider should make sure that the server is provided with high security from all the external threats. Although, the cloud service provider should provide security for the client’s information.

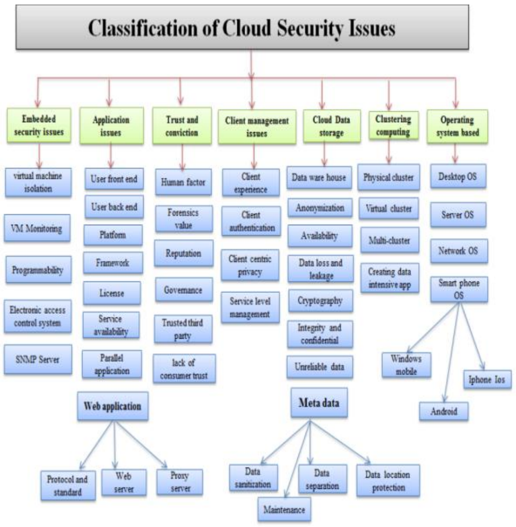


Figure 3.The classification of cloud security issues.

The below diagram represents the parameters that affect the cloud security issues.

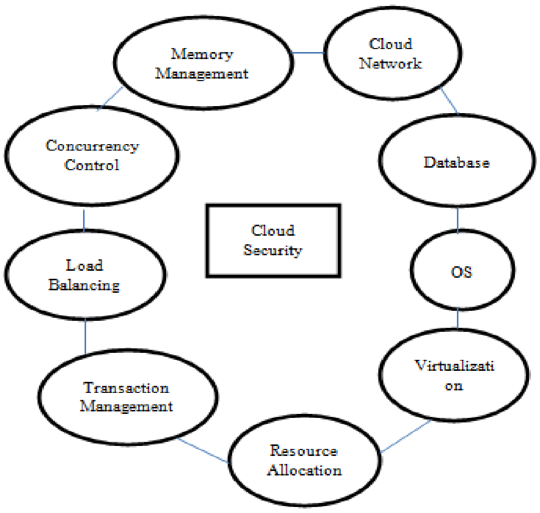


Figure 4. Parameters that affect cloud security

The security issues are briefly explained in [1], by Prince Jain. In this paper, the parameters which affect the cloud security and at the same way discover the security issues and problems faced by service providers are proposed. [2], by RojaRamani A, describe the data access control and data security in cloud and the architecture of the cloud,. Sharma et al., [3], proposed the description of various video encryption algorithms based on some parameters and difficult for particular algorithm to satisfy all parameter's performance. Omar et al., [4], proposed a description and comparison between encryption methods. Negi et al., [5], proposed various encryption algorithms for encrypting the video frames. Madhvi et al., [6], proposed a various encryption algorithms for video frames. The existing system proposes that the video frames are first encrypted using the standard tradition algorithm called Full Encryption Algorithm.The drawback of the full encryption is it is not appropriate for real time video frames because of its high computation and slow speed.

In this paper, we proposed a secure video sharing and storing process. The procedures involved are:

1. The size of the video frames is calculated using Random Walk Approach.
2. Then they are partitioned and stored to the specified cloud provider using Replacement Algorithm For Partitioning.
3. Then they are encrypted using Pixel Permutation Algorithm.

II. EXISTING WORK

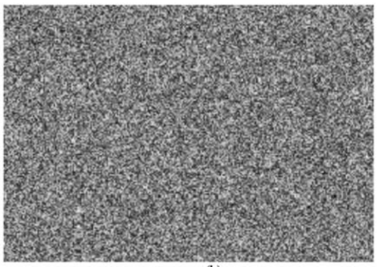
A. FULL ENCRYPTION ALGORITHM

The existing system proposes that the video frames are first encrypted using the standard tradition algorithm called Full Encryption Algorithm. Hector et al., [9], proposed the networks performance and reduce the packet lossand SalahAly et al., [10], proposed various techniques for securing the multimedia contents.The process of encrypting each and every byte will be a slow and expensive one. The drawback of the full encryption is it is not appropriate for real time video frames because of its high computation and slow speed. While encrypting each and every frame it takes more time for processing. In existing work, the receiver is unable to have quality guarantee of an image. Thus the time needed for full encryption technique is greater than the permutation technique. The users have to wait for long time to encrypt and decrypt the content. This leads to high cost.

B. PERFORMANCE AND RESULT

The results of the full encryption algorithm are shown below and it represents that the full encryption provides better result.

The original video frame before encryption process



The video frame after encryption

The video frame after decryption

The drawback of the full encryption is it is not appropriate for real time video frames because of its high computation and slow speed. Thus the time needed for full encryption technique is greater than the permutation technique. The users have to wait for long time to encrypt and decrypt the content. This leads to high cost.

III. PROPOSED WORK

In this paper, first, the sizes of the video content are calculated and as per the frame size the video contents are hosted to the specified cloud provider using Random

Walk Algorithm. Then, the video contents are re-hosted to change the cloud providers using Partitioning Algorithm..Then the video files are encrypted and then stored in cloud usinga technique called, permutation algorithm. These are implemented using CloudSim and proved that this proposed technique gives better result than the existing technique when compared to time and performance. Thus the time needed for full encryption technique is greater than the permutation technique.

ALGORITHM STEPS

A. RANDOM WALK ALGORITHM

For re-hosting process the following algorithm is used. The random walk approach is one in which the highest node in the process is taken. Here node represents the video files and graph represents the deployment models. Then it is inserted as new node and the worst node is removed. This process is repeated when the value is less than its parameter value otherwise the process is stopped. The following equation (1) is used for the random walk approach.

$$p_{uv}=\begin{cases}\left(\frac{\mathrm{a}}{\mathrm{m}}+1\right)\div(\mathrm{d_u}\ +\mathrm{a}), \text{if i and j are linked}\\ \left(\frac{\mathrm{a}}{\mathrm{m}}\right)\div(\mathrm{d_u}+\mathrm{a}),\ \text{if i and j are not linked}\end{cases}\quad \ldots. \tag{1}$$

Table 1.Random Walk Algorithm

1. Assign n, a and x
2. Now random walk approach is executed according to the equation (1). If the first step is satisfied, uniform distribution is started.
3. The current node has the highest degree than the other node in the n list, insert new node and delete the worst node.
4. Return to 2 step if the random walk steps is less than x. Otherwise stop.

Here a and x are the parameters and the performance is based on these parameters.

We implemented the random walk approach for determining highest ranking node. This algorithm is not possible to apply ranking algorithm. In ranking algorithm, the calculation occurs at each and every graph of a global graph concurrently. The video files are stored in the cloud based on the sub graph placement algorithm. Then they assigned to store in to the various cloud providers. This process is based on the ranking algorithm. In which each files are assigned to various providers. Thus, it provides more security and does not allow other unauthorized persons to access the video files. Thus, the video files are re-hosted for changing the providers in cloud for clients and stored in cloud based on this algorithm. Finally they are encrypted using proposed pixel permutation algorithm.

B. REPLACEMENT ALGORITHM FOR PARTITIONING

Multi cloud means multiple clouds services in a single architecture. Multi cloud approaches can offer hardware, software and infrastructure redundancy to optimize fault tolerance. It can also navigate traffic from different clients through the internet. Instead of storing contents to a single cloud, multi cloud is used.When the whole content is stored in a single cloud provider, there is a possibility to hack the entire data by unauthorized persons. Thus the datas are partitioned and stored in multiple clouds to avoid unauthorized access to the content in cloud. The below diagram represents the multi cloud hosting. In single cloud, if whole server is cracked it is impossible to get back the content. But if we are using multi cloud there are various advantages. When one cloud provider is hacked or cracked it is possible to get the content back, because, if one server get cracked the remaining data may be retrieved from another server. So with the help of remaining content it is possible to get the original data.

In our proposed work, the multi cloud concept is used. First, the sizes of the video contents are calculated and then they are hosted to the specified cloud provider using replacement algorithm for partitioning. This is used to store the video contents to the cloud to partition the users to various cloud providers so that the videos are received with better quality.

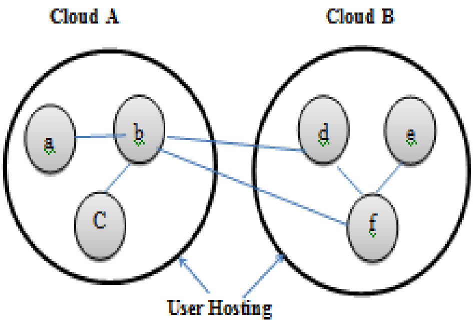


Figure 5. Multi-Cloud Hosting based on propagation.

Table 2.Replacement Algorithm for Partitioning

Here
a - Partitioned graph, p - Space in private cloud, c - Space in public cloud, t - Storage Multiplexer

```
result ←{}
for all ai in a do
    sortedP← sortDescending(P)
    if(sortedP.top().size()*t)>ai.size() hen
        sortedP.top().assign(ai)
        result.append(sortedP.top(),ai)
    else
        sortedC←sortDescending(C)
        if(sortedC.top().size()*t)>ai.size() then
            sortedC.top().assign(ai)
        result.append(sortedC.top(),ai)
        else
        uNew←allocateNewPublicVM()
            C.add(uNew)
            goto 3
        endif
    endif
end for
return result
```

The sub graph replacement algorithm is shown in Table 2. Here the video files are sorted based on their sizes. In addition, the space in private cloud is sorted based on the available free space at that specified time. Then the leading space is allocated to the cloud, which is having the largest free space. After that, we sort them again based on the largest free space. We carry on this process until all of them are allocated to the cloud. In case, if the space is not enough to store the data, then we assign a new node in the public cloud and which is used based on the remaining space in the private cloud. The operation of sub graph replacement algorithm is shown in Algorithm 1. This process is used to allocate the video files into the cloud.

C. PIXEL PERMUTATION TECHNIQUE

The Permutation Algorithm is one of the pseudo random generators in which a key is chosen randomly from a list of keys. The figure 6 represents the proposed permutation technique. The main purpose of permutation is to scramble only the particular video frames, not all the video frames are encrypted. SeshaPallaviIndrakanti and P.S.Avadhani in [7], and Hui et al., [8], proposed an image encryption for maintaining the quality of the imagebased on random permutation.

The pixel value of an image is chosen and permuted using the pseudo random index generator with the key already generated. These images are known as encrypted image. Now this encrypted image is transmitted to the receiver. The scrambled image is decrypted using pseudo random index generator and the same set of keys on the receiver side.

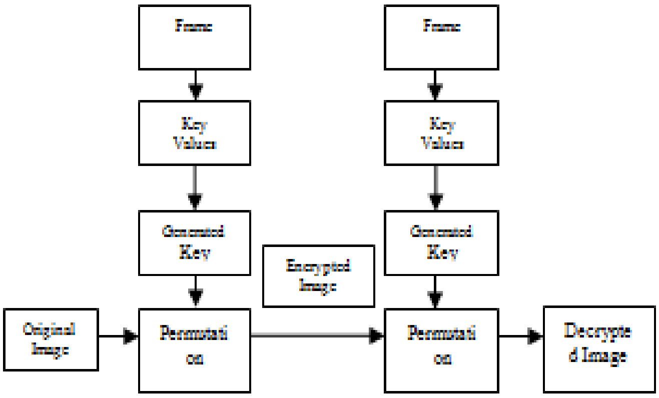


Figure 6. Permutation Technique

The following steps are used for implementing the pixel permutation algorithm.

Table 3. Proposed Pixel Permutation Algorithm

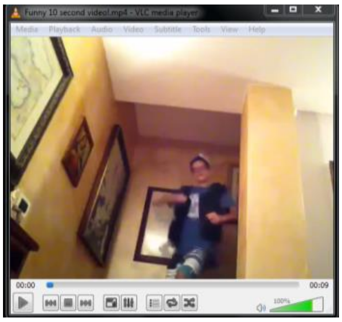
1. Choose the image and 8 bit key of an image is given as an input
2. Now the decimal pixel value of an image is converted into the binary value
3. The process is repeated for all the images' pixel value and based on the key value rearrange the bits.

4. Now the permuted value is converted to decimal value then form a matrix
5. Now the pixels are permuted based on the key and finally, they are arranged

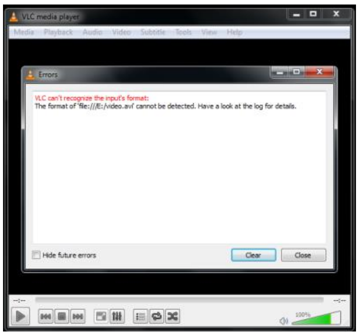
The users have to choose the image and then encrypt. The key generated is used to encrypt and decrypt the frames. Then convert each frames decimal pixel value to the binary value and repeat the process for all the three planes. According to the key, rearrange the bits. Then convert the permuted value back to the decimal value then form a temporary matrix by transferring row of pixels, and permute pixels as per the key generated and then, partition the image into 8 blocks vertically or horizontally. Finally, rearrange the blocks based on the key generated.

IV. PERFORMANCE RESULT AND COMPARISON

This section determines the comparison of the proposed pixel permutation algorithm with the existing full encryption algorithm.

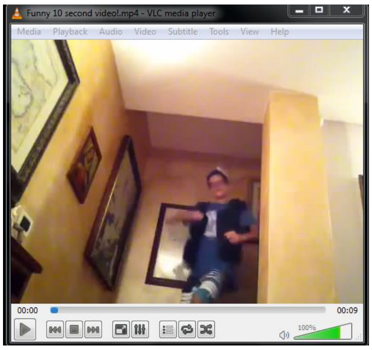

Funny 10 second video!.mp4 - VLC media player
Media Playback Audio Video Subtitle Tools View Help
00:00
00:09
100%

The original video frame before encryption process.



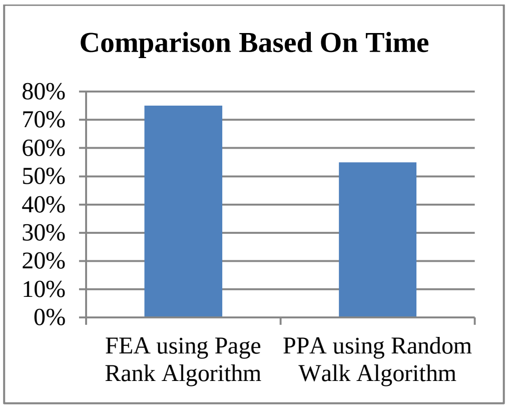
VLC can't recognize the input's format:
The format of 'file:///E:/video.avi' cannot be detected. Have a look at the log for details.

The video frame after encryption.


Funny 10 second video!.mp4 - VLC media player
Media Playback Audio Video Subtitle Tools View Help
00:00
00:09
100%

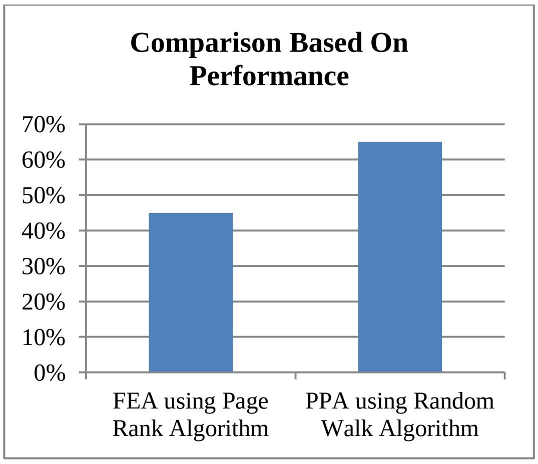
The video frame after decryption.

Here FEA – Full Encryption Algorithm and PPA – Pixel Permutation Algorithm.



Comparison between Existing and Proposed Algorithm based on Time

The above comparison represents that the proposed pixel permutation algorithm is giving better result when compared to the existing full encryption algorithm based on time.



Comparison between Existing and Proposed Algorithm based on Performance

The above comparison represents that the proposed pixel permutation algorithm is better when compared to the existing full encryption algorithm based on performance.

V. CONCLUSION

In this paper, we studied hosting of the social video content with multiple providers in cloud. The problem in multi-cloud hosting is used to enhance users' satisfaction of provider preference in cloud and it is proved using Replacement Algorithm for Partitioning. Thus, the simple and effective methods are proposed in this paper for video content encryption using permutation techniques. The implementation is carried out using CloudSim. The result is compared with the existing encryption algorithm and proved that our algorithm shows better result based on both time and performance.

VI. REFERENCES

[1]. "Security Issues and their Solution in Cloud Computing", Prince Jain Malwa Polytechnic College Faridkot, Punjab-151203, India

[2]. "Encryption And Decryption Of A Cloud Computing File", RojaRamani A

[3]. "A Study Based on the Video Encryption Technique", Saurabh Sharma, Pushpendra Kumar Pateriya, Lakshmi *Department of Computer Science Engineering Lovely Professional University, Phagwara, India*

[4]. "An Overview of Video Encryption Techniques", M. Abomhara, Omar Zakaria, Othman O. Khalifa

[5]. "A Survey on Video Encryption Techniques", YogitaNegi*Asstt. Professor, BCIIT, Delhi* Haghighat, M., Zonouz, S., & Abdel-Mottaleb, M. (2015). CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. Expert Systems with Applications, 42(21), 7905–7916.

[6]. "A Survey of Video Encryption Methodologies", MadhviSoni , SapnaChaudhary, Dept. of Computer Science & Engineering, Shri Ram Group of Institutions, Jabalpur, India

[7]. "Permutation based Image Encryption Technique",SeshaPallaviIndrakantiP.S.Avadhani Department of CS and SE, Andhra University College of Engineering(A), Andhra University, Visakhapatnam

[8]. "Algorithm of Image Encryption based on Permutation Information Entropy", Guang-hui, Hu Kai, Yang He and E Xu, Beijing University of Aeronautics and Astronautics Beijing, China

[9]. "NAIVE – Network Aware Internet Video Encoding", Hector Briceno, Steven Gortler, Leonard McMillan, MIT.

[10]. "A Light – Weight Encrypting For Real Time Video Transmission", Salah Aly

[11]. "Known-Plaintext Attack Against a Permutation Based Video Encryption Algorithm", Adam J. Slagell slagell@ncsa.uiuc.edu January 16, 2004

[12]. "Digital Video Encryption Algorithms Based on Correlation-Preserving Permutations", Daniel Socek, Spyros Magliveras, DubravkoCulibrk, Oge Marques, HariKalva and BorkoFurht Florida Atlantic University, Boca Raton FL 33431

[13]. P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-145, 2009.

[14]. W. Zhu, C. Luo, J.Wang, and S. Li, "Multimedia cloud computing," IEEE Signal Process. Mag., vol. 28, no. 3, pp. 59–69, May 2011.

[15]. D. D´ıaz-S´anchez, F. Almenarez, A. Mar´ın, D. Proserpio, and P.A. Cabarcos, "Media cloud: An open cloud computing middleware for content management," IEEE Trans. Consum. Electron., vol. 57, no. 2, pp. 970– 978, May 2011.

[16]. Srinavasin, Madhan (2012). "State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment". ACM ICACCI'.

[17]. "Identity Management in the Cloud". Information Week. 2013-10-25. Retrieved 2013-06-05

[18]. T. ElGamal, "A public key cryptosystem and a signature scheme basedon discrete logarithms," in Advances in Cryptology. New York, NY, USA:Springer-Verlag, 1985, pp. 10–18.

[19]. G. B. Algin and E. T. Tunali, "Scalable video encryption of h. 264 svccodec," J. Vis. Commun. Image Represent., vol. 22, no. 4, pp. 353–364,2011.

[20]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebasedencryption," in Proc. IEEE Symp. Security Privacy, 2007,pp. 321–334.

[21]. D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes forstateless receivers," in Proc. CRYPTO, 2001, pp. 41–62.

[22]. L. Qiao and K. Nahrstedt, "A new algorithm for mpeg video encryption,"in Proc. 1st Int. Conf. Imag. Sci., Syst. Technol., 1997,pp. 21–29.

[23]. J. Ren, K. Zhang, and X. Shen, "Exploiting mobile crowdsourcing forpervasive cloud services:Challenges and solutions," IEEE Commun.Mag.,vol. 53, no. 3, pp. 98–105, Aug. 2015.

[24]. J. Ren, K. Zhang, and X. Shen, "Social aware crowdsourcing with reputationmanagement in mobile sensing," Comput. Commun., vol. 65, no. 1,pp. 55–65, Aug. 2015.