

Performance Analysis of Effective Video Copy detection using AES & KNN Algorithm of Multimedia Content in Cloud Environment

Mr. Shubham Dilip Vyawahare

M.E Student, Department of Computer Science & Engineering
Anuradha Engineering College, Chikhli (MS), India

Dr. Avinash Kapse

Head of Department, Information Technology,
Anuradha Engineering College, Chikhli (MS), India

Dr. Arvind S. Kapse

Professor, Department of Information Science & Engineering,
New Horizon College of Engineering, Bengaluru, India

ABSTRACT

In a vision of large-scale hypermedia content safeguard systems and the duties to deliver cloud substructures to deliver charge effectiveness, hasty deployment, scalability, and bounciness to provide accommodations fluctuating amount of work. We recommending a system that can be used to defend diverse multimedia comfortable types, including 2-D videos, 3-D videos, images, audio clips, songs, and music clips. It can be executed on private and/or public clouds. We proposal a structure with two manner processing: (i) Generating digital signs, and (ii) Contrast databank to acknowledged changes. The autograph method generates forceful and demonstrative signatures of contents. Contrast with storing that is physical in cloud with the existing contented. The high accurateness and scalability of the suggested scheme contain high database and stowing contented. In accumulation, we likened our scheme to the safeguard system used by some videos channels

Keywords: Cloud storage, Digital signatures, scalability, protection channels and database.

As per the definition provided by the National Institute for Standards and Technology (NIST) (Badger et al., 2011), “*cloud computing* is a classical for allowing suitable, on-demand complex access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal managing exertion or facility wage-earner interface”[1].

It signifies an archetype modification in information technology many of us are possible to grasp in our era. While the clientele are eager by the occasions to diminish the principal costs, and the planned to strip themselves of substructure organization and attention arranged essential capabilities, and in the air all the quickness obtainable by the on-demand provisioning of computing, there are problems are encounters which need to be addressed earlier an abundant implementation may happen.

Cloud computing refers to both the bids transported as services terminated the Internet and the hardware and organizations software in the datacenters that deliver those facilities. There are four basic cloud distribution models, as outlined by NIST (Badger et al., 2011), based on who provides the cloud facilities. The activities may service one model or a grouping of different models for well-organized and heightened delivery of requests and commercial facilities [2, 18].

1.1 Objectives

I. Introduction

- To provision a privacy-preserving application.
- To variety communal inspecting on mutual data deposited in the cloud consuming frequent encryption technique.

The recommend system a privacy-preserving public examining mechanism for mutual statistics in the cloud. We apply the sign signature to hypothesis homomorphism authenticators, so that a civic verifier is clever to review the communal records integrity without regaining the complete data, yet it cannot discriminate who is the signer on each block.

To rally the effectiveness of *verifying* numerous reviewing tasks, we supplementary spread our apparatus to provision batch reviewing. There are two stimulating problems we will continue to study for our future work. One of them is traceability, which means the aptitude for the collection administrator to reveal the uniqueness of the signer based on authentication metadata in some singular circumstances [3, 12].

II. Related Work

2.1 Cloud Service Delivery Models

The cloud computing prototypical affords the occasion to bring requests via the Internet, prevent the costs of possessing and functioning data centers, and influence the work of other software designers. This structure described the classes of cloud providers and, the purposes of cloud provision supervision. It also labeled the association amongst Web amenities, SOAs, and cloud computing [4].

The usage of any technology, of course, must occur in the context of our establishments. Establishments have many services that upset the implementation of new expertise. The next part of the book will delve into the services affecting the implementation Web facilities, service-oriented designs, and cloud computing. [5].

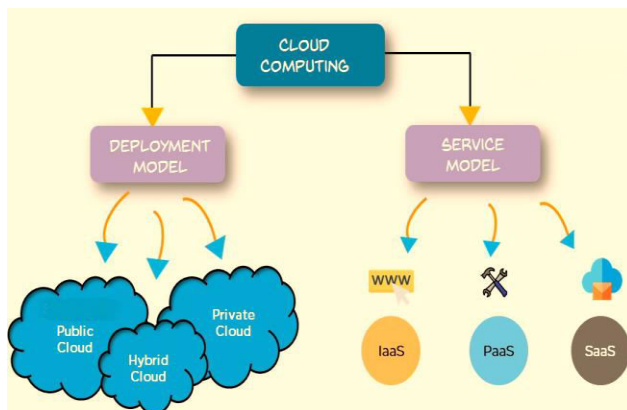


Fig.1: Classification of cloud computing.

2.2 Emerging Trends in Security & Privacy in Cloud Computing

Cloud computing surroundings are multi domain environments in which everyone domain can usage diverse safekeeping, confidentiality, and trust necessities and potentially employ numerous mechanisms, boundaries, and semantics. Such domain could represent independently enabled services or supplementary infrastructural or application mechanisms.

Service-oriented architectures are obviously relevant knowledge to expedite such multi domain development through provision arrangement and adaptation [6].

It is significant to influence prevailing research on multi domain policy mixing and the secure service configuration to build all-inclusive policy-based organization framework in cloud figuring environments (Takabi et al., 2010). In the succeeding trends, they identify some critical safekeeping and secrecy issues in cloud computing that need instant devotion for universal acceptance of this technology [17].

- Authentication & Identity management.
- Access Control & Accountancy.
- Trust management & Policy Integration.
- Secure Service Management.
- Privacy & Data Protection.
- Organizational Security Management.
- Increasing user of mobile Devices.
- Hardware Capability Improvement.
- Tracking Complexity Legislation and Security.

III. System Design & Deployment

3.1 ALGORITHM USED

In our proposed system we are using the 2 algorithm which are AES & KNN. The more prevalent and broadly accepted symmetric encryption algorithm probable to be come across currently is the Advanced Encryption Standard (AES). It is originate at least six time quicker than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing authority, it was measured defenseless against comprehensive key hunt attack. Triple DES was designed to overcome this drawback but it was found slow.

The structures 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 design details
- Software implementable in C and Java

The specification called for a symmetric algorithm (same key for encryption and decryption) using block encryption (see block cipher) of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum. The algorithm was required to be royalty-free for use worldwide and offer security of a sufficient level to protect data for the next 20 to 30 years [7].

K-nearest neighbors (KNN) algorithm is a kind of managed ML algorithm which can be hand-me-down for both classification as well as reversion predictive glitches. However, it is mostly secondhand for classification analytical problems in commerce. The subsequent two properties would describe KNN well –

- **Lazy learning algorithm** – KNN is a lazy knowledge algorithm since it does not have a specific training phase and uses all the data for training while cataloguing.
- **Non-parametric learning algorithm** – KNN is also a non-parametric learning algorithm because it doesn't assume anything about the underlying data.

Working of KNN Algorithm

K-nearest neighbors (KNN) algorithm uses 'feature similarity' to predict the values of new data points which further means that the new data point will be assigned a value based on how closely it matches the points in the training set. We can comprehend its working with the help of following steps –

Step 1 – for implementing any algorithm, we need dataset. So through the 1st step of KNN, we must freight the drill as well as test statistics.

Step 2 – Next, we essential to select the significance of K i.e. the adjacent data points. K can be any fraction.

Step 3 – for every single point in the test statistics do the subsequent –

- **3.1** – calculate the fallback among test statistics and each rumpus of exercise data with the support of any of the technique namely: Euclidean, Manhattan or Hamming distance. The maximum frequently used technique to gauge distance is Euclidean.
- **3.2** – Now, grounded on the remoteness value, sort them in climbing order.

- **3.3** – Next, it will select the top K rows from the prearranged array.
- **3.4** – Now, it will assign a period to the test point based on most recurring class of these rows.

Step 4 – Suppose our model is ready [2]

Why do we need a K-NN Algorithm?

Presume there are two groupings, i.e., Group A and Group B, and we consume an innovative data socket x1, so this data socket will propaganda in which of these groupings. To resolve this variety of problematic, we necessity a K-NN procedure. With the assistance of K-NN, we can effortlessly classify the grouping or session of a specific dataset. Reflect the underneath illustration:

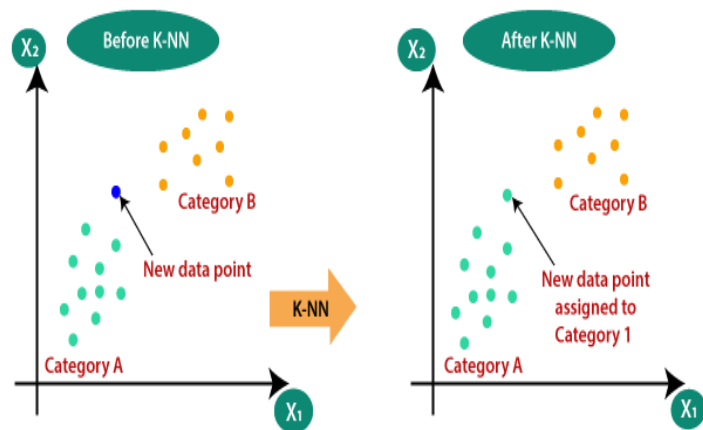


Fig.2: Comparison of Grouping before KNN & after KNN

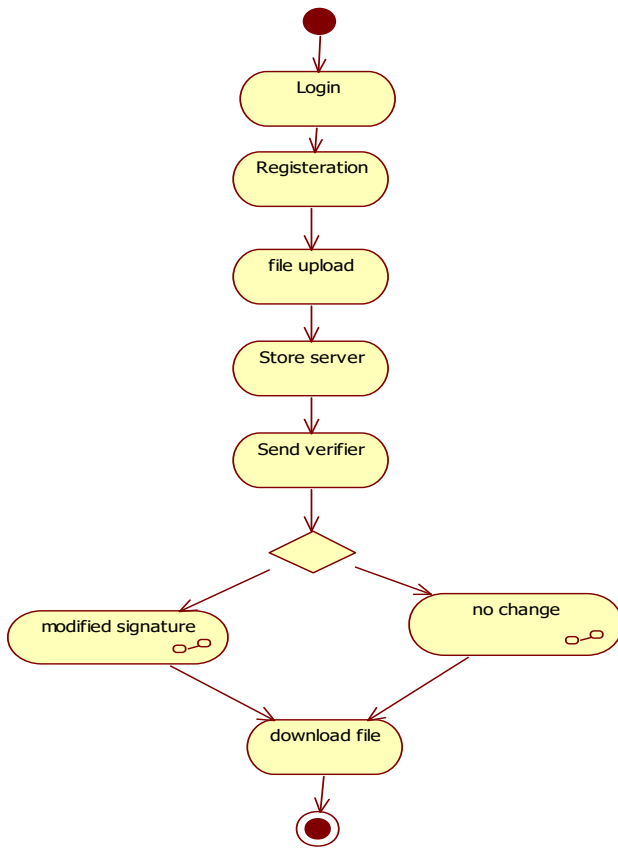
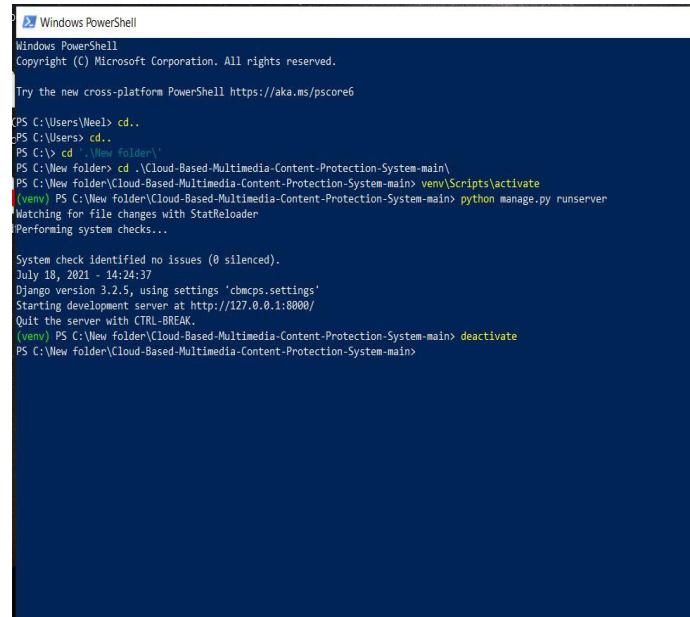


Fig.3: Activity structure

3.2 Steps of execution

Technology to be used in given System.

1. Python
2. Power shell.
3. Sub line Text
4. Django



```

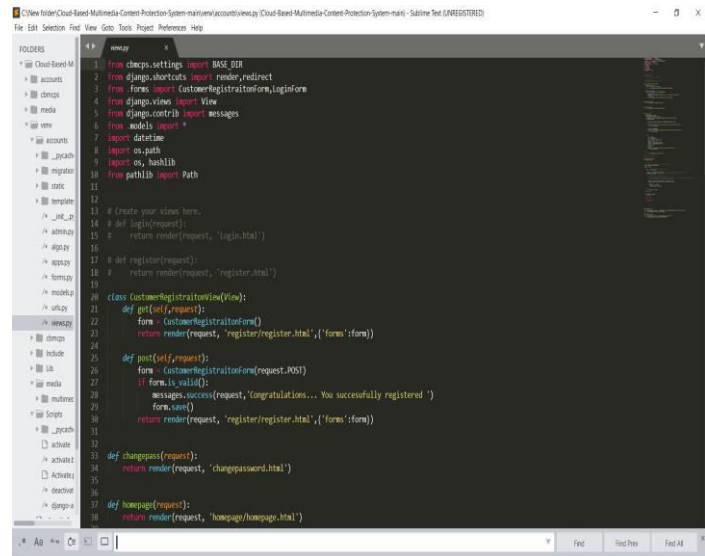
    Windows PowerShell
    Copyright (C) Microsoft Corporation. All rights reserved.

    Try the new cross-platform PowerShell https://aka.ms/pscore6

    PS C:\Users\Weel> cd..
    PS C:\Users> cd..
    PS C:\> cd ".\New folder\"
    PS C:\New folder> cd ".\Cloud-Based-Multimedia-Content-Protection-System-main\"
    PS C:\New folder\Cloud-Based-Multimedia-Content-Protection-System-main> venv\Scripts\activate
    (venv) PS C:\New folder\Cloud-Based-Multimedia-Content-Protection-System-main> python manage.py runserver
    Matching for file changes with StatReloader
    Performing system checks...

    System check identified no issues (0 silenced).
    July 18, 2021 - 14:24:37
    Django version 3.2.5, using settings 'cbmcpss.settings'
    Starting development server at http://127.0.0.1:8000/
    Quit the server with CTRL-BREAK.
    (venv) PS C:\New folder\Cloud-Based-Multimedia-Content-Protection-System-main> deactivate
    PS C:\New folder\Cloud-Based-Multimedia-Content-Protection-System-main>
  
```

Fig.4: Step to activate Django powershell.



```

    # @ Cloud-Based-Multimedia-Content-Protection-System-main\accounts\views.py (Cloud-Based-Multimedia-Content-Protection-System-main) - Sublime Text (LAFEGE0R2C)
    # Fat Edit Selection Find View Goto Tools Project Preferences Help

    # @ Cloud-Based-Multimedia-Content-Protection-System-main\accounts\views.py
    1 from django.shortcuts import render, redirect
    2 from django.contrib.auth.forms import UserCreationForm
    3 from django.contrib.auth import login
    4 from django.contrib import messages
    5 from django.contrib.auth.decorators import login_required
    6 from django.shortcuts import render
    7 import datetime
    8 import os.path
    9 import os, hashlib
    10 from pathlib import Path
    11
    12
    13 # Create your views here.
    14 def register(request):
    15     return render(request, 'register.html')
    16
    17 def register(request):
    18     return render(request, 'register.html')
    19
    20 class CustomUserCreationForm(UserCreationForm):
    21     def __init__(self, request):
    22         self.request = request
    23         super().__init__(request.POST or None, request.FILES or None)
    24
    25     def post(self, request):
    26         form = CustomUserCreationForm(request.POST)
    27         if form.is_valid():
    28             messages.success(request, 'Congratulations... You successfully registered.')
    29             form.save()
    30             return render(request, 'register/register.html', {'form': form})
    31
    32
    33 def change_pass(request):
    34     return render(request, 'change_password.html')
    35
    36
    37 def home_page(request):
    38     return render(request, 'home_page/homepage.html')
  
```

Fig.5: Basic structure of proposed system

```

100  # test for creating an MD5 hash from a string
101  # the Python hashlib module is an interface for hashing messages easily. This contains numerous methods which
102  # will handle hashing any raw message in an encrypted format.
103  # hashlib() - Returns the encoded data in hexadecimal format.
104  filehash = hashlib.md5(open(file_name, 'rb').read()).hexdigest()
105
106  # filehash not in unique:
107  unique[filehash] = file_name
108
109  # else:
110  print("Path not exists")
111  # print(unique)
112
113  # newfilehash is unique:
114  # print("True")
115  return True
116
117  # else:
118  # print("False")
119  return False

```

Fig.6: Code of Algo processing

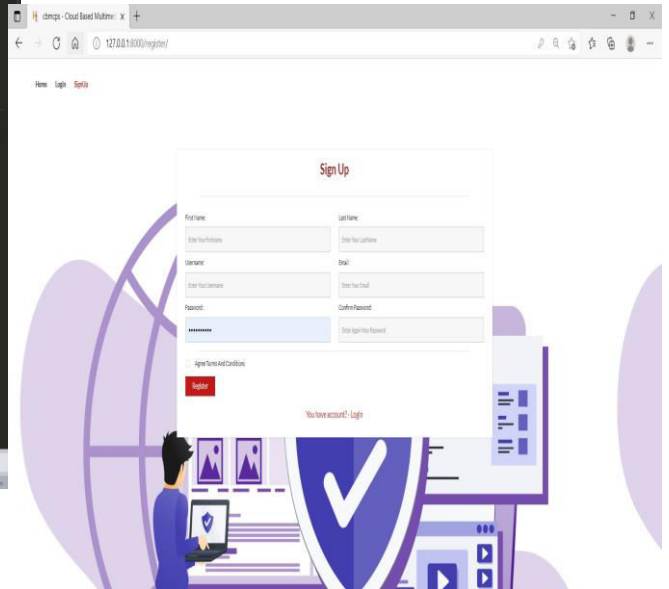


Fig.8: Registration Page

IV. Performance Analysis

4.1 Result & Screen Shot

To make it implemented in the way it was design with easily accessible, more secure technologies. Technical feasibility on the existing system and extend it can support the proposed addition. In this new modules it added easily without affecting the core program structure. Most of parts are running in this server using the concept of stored procedures.

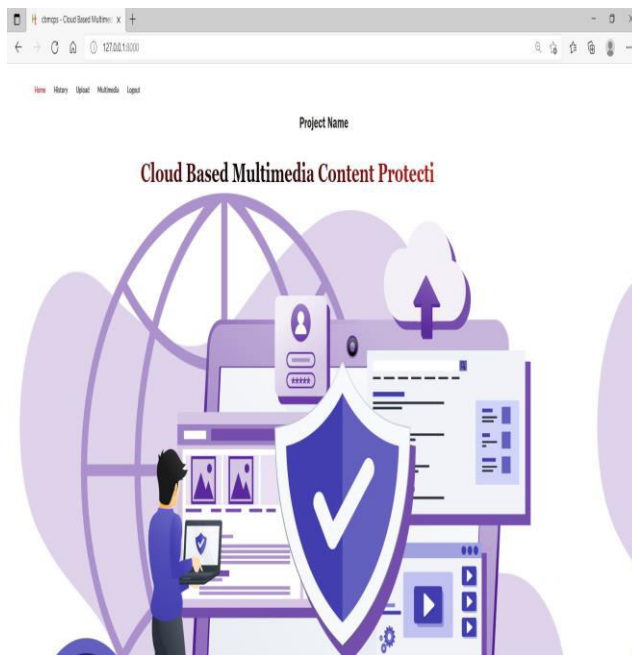


Fig.7: Home Page

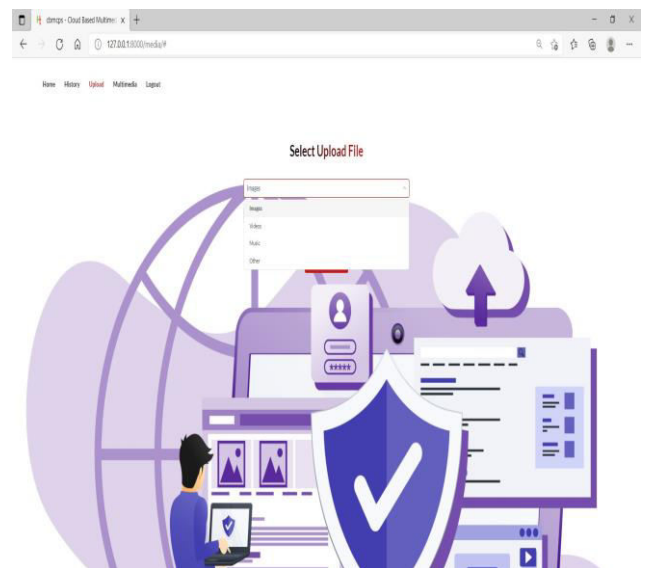


Fig.9: Selection of upload category.

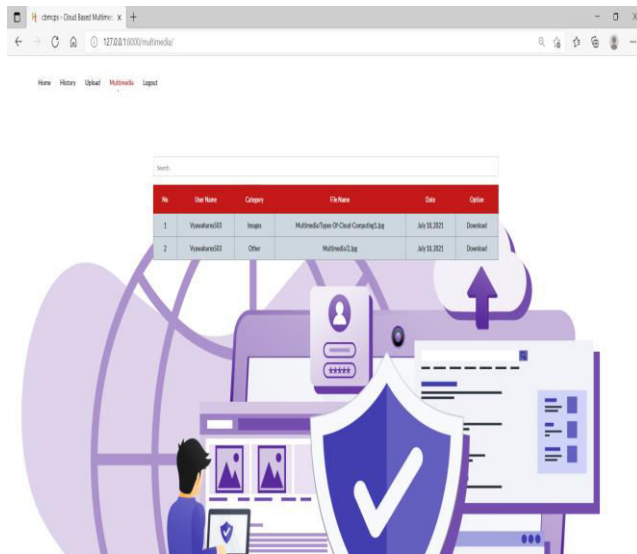


Fig.10: Upload Files

4.2 Advantages:

The proposed system can perform multiple auditing tasks simultaneously. They improve the efficiency of verification for multiple auditing tasks. High security provide for file sharing.

4.3 Limitation:

As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. They do not perform the multiple auditing task in simultaneously.

V. Conclusion

In this Study, the suggest system, the first privacy-preserving community auditing mechanism for communal data in the cloud for defending the hypermedia content. With this structure, the community verifier is able to professionally audit the honesty of communal data, yet cannot differentiate who is the signer on each block, which can reservation identity privacy for users. An thought-provoking problem in our future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor.

The main attention of this learning is to present an impression of different methods that are functional in diverse research models since the last 12–15 years. After this evaluation, it is shortened that duplicate features illustration is done by the use of low-level visual features such as color, texture, spatial layout, and shape.

The large-scale image datasets and high computational machines are the main requirements for

any deep network. It is a difficult and time-consuming task to manage a large-scale image dataset for supervised training of a deep network.

5.1 FUTURE SCOPE

In this era of Cloud Computing, it is expected steps of automation which do not involve humans also save the costing & time duration, as they can be erroneous. Future work may include building new detecting AI based apps that can help to find the similar context in deep network.

Therefore, the performance evaluation of a deep network on a large-scale unlabelled dataset in unsupervised learning mode is also one of the possible future research directions in this area.

References:

- [1] Abdelsadek, Distributed index for matching multimedia objects, M.S. thesis, School of Comput. Sci., Simon Fraser Univ., Burnaby, BC, Canada, 2014.
- [2] Abdelsadek and M. Hefeeda, Dimo: Distributed index for matching multimedia objects using MapReduce,” in Proc. ACM Multimedia Syst. Conf. (MMSys’14), Singapore, Mar. 2014, pp. 115–125.
- [3] M. Aly, M. Munich, and P. Perona, Distributed Kd-Trees for retrieval from very large image collections,” in Proc. Brit. Mach. Vis. Conf. (BMVC), Dundee, U.K., Aug. 2011.
- [4] J. Bentley, Multidimensional binary search trees used for associative searching,” in Commun. ACM, Sep. 1975, vol. 18, no. 9, pp. 509–517.
- [5] P. Cano, E. Batle, T. Kalker, and J. Haitsma, “A review of algorithms for audio fingerprinting,” in Proc.
- [6] Privacy-Preserving Public Auditing for Secure Cloud Storage (I. Agudo, D. Nunez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinouidakis, Cryptography goes to the cloud,” in Secure and Trust Computing, Data Management, and Applicat., 2011, pp. 190–197.)
- [7] Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data (G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, Provable data possession at untrusted stores,” in Proc. 14th ACM conf. Compu. Commun. Security (CCS), 2007, pp. 598–609.)
- [8] Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud (G. Ateniese, A. Faonio, and S. Kamara, “Leakage-resilient identification schemes from zero-knowledge proofs of storage,” in IMA Inte. Conf. Cryptography and Coding, 2015, pp. 311–28)
- [9] Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud (G. Ateniese,
- [10] R.D. Pietro, L.V. Mancini, and G. Tsudik, Scalable and efficient provable data possession, in Proc. 4th Int. Conf. Secure and Privacy in Commun. Netw. (SecureComm), 2008, pp. 110.)
- [11] Remote Data Checking for Network Coding-based Distributed Storage Systems (K. D. Bowers, A. Juels, and A. Oprea, Proofs of retrievability: theory and implementation,” in Proc. 2009 ACM Workshop Cloud Computing Security (CCSW), 2009, pp. 435–4.)
- [12] Short Group Signatures (L. Chen, Using algebraic signatures to check data possession in cloud storage, Future Generation Computer Systems, vol.29, no.7, pp. 1709–1715, 2013.)
- [13] Storing Shared Data on the Cloud via Security- Mediator (Y. Dodis, S. Vadhan, and D. Wichs, Proofs of retrievability via hardness amplification, in Proc. Theory Cryptography Conf. (TCC), 2009, pp. 109–127.)
- [14] Alliance for Telecommunications Industry Solutions. Homepage URL: <http://www.atis.org>. Amazon S3

- Availability Event: (2008). URL: <http://status.aws.amazon.com/s3-20080720.html> (Accessed on November 29, 2012).
- [15] AOL Apologizes for Release of User Search Data (2006). URL: news.cnet.com/2010-1030_3-6102793.html. August 7, 2006.
- [16] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinsky, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M (2009). Above the Clouds: A Berkeley View of Cloud Computing. Technical Report No. UCB/ECS-2009-28, Department of Electrical Engineering and Computer Sciences, University of California at Berkeley. February 10, 2009. Available on line at: <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/ECS-2009-28.pdf> (Accessed on: November 20,2012)
- [17] Association for Retail Technology Standards (ARTS). Homepage URL: <http://www.nrf-arts.org>. Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146. US Department of Commerce. May 2011. Available online at: <http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf> (Accessed on: November 20, 2012).
- [18] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinsky, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M (2009). Above the Clouds: A Berkeley View of Cloud Computing. Technical Report No. UCB/ECS-2009-28, Department of Electrical Engineering and Computer Sciences, University of California at Berkeley. February 10, 2009. Available on line at: <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/ECS-2009-28.pdf> (Accessed on: November 20,2012)
- [19] Association for Retail Technology Standards (ARTS). Homepage URL: <http://www.nrf-arts.org>. Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146. US Department of Commerce. May 2011. Available online at: <http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf> (Accessed on: November 20, 2012).
- [20] Bertion, E., Paci, F., & Ferrini, R. (2009). Privacy-Preserving Digital Identity Management for Cloud Computing. IEEE Computer Society Data Engineering Bulletin, pp. 1-4, March 2009.
- [21] Biggs & Vidalis (2009). Cloud Computing: The Impact on Digital Forensic Investigations. In Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST'09), London, UK, November, 2009, pp. 1-6,
- [22] Blaze, M., Kannan, S., Lee I., Sokolsky, O., Smith, J. M., Keromytis, A.D., & Lee, W. (2009). Dynamic Trust Management. *IEEE Computer*, Vol 42, No 2, pp. 44-52, 2009.
- [23] Bruening, P.J. & Treacy, B.C. (2009). Cloud Computing: Privacy, Security Challenges. Bureau of National Affairs, 2009.
- [24] Center for the Protection of Natural Infrastructure (CPNI)'s Information Security Briefing on Cloud Computing, 01/2010, March 2010.
- [25] Chen, Y., Paxson, V., & Katz, R.H. (2010). What's New About Cloud Computing Security? Technical Report UCB/ECS-2010-5, EECS Department, University of California, Berkeley, 2010. Available Online at: <http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/ECS-2010-5.html> (Accessed on: November 29, 2012).