ISSN: 2454-3659 (P), 2454-3861(E)
Volume II, Issue 12 December 2016
International Journal of Multidisciplinary Research Centre
Research Article / Survey Paper / Case Study

DISTRIBUTED PROVABLE DATA POSSESSION IN MULTI-CLOUD STORAGE THROUGH CLIENT AUTHENTICATION

Name: Lolla Srikanth
Affilation : M.Tech, CSE Dept
Miracle Educational Society Group of Institutions

COUNTRY : INDIA

Name: K. Rajendra Prasad
Affilation : Assistant Professor, CSE Dept
Miracle Educational Society Group of Institutions .

COUNTRY : INDIA

Name: Dr. A Arjuna Rao
Affilation : Principal & Director
Miracle Educational Society Group of Institutions

COUNTRY : INDIA

ABSTRACT

Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we introduced a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. The formal system model and security model are given. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed.

The ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational DiffieHellman) problem. In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the ID-DPDP protocol can realize private verification, delegated verification and public verification. In the proposed system we provided a client authorisation such that client can check integrated data over a cloud through secured process. Here we provide an authentication of client in the security model .

INTRODUCTION

The term Cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer network diagrams as an abstraction of underlying infrastructure it represents. Typical cloud computing providers deliver common business application online which are accessed from web browser, while the software and data are stored on server.Cloud computing is an internet based computing model which provides on-demand service, local independence, scalability, elasticity, ubiquitous network access, resource pooling and pay-as-you-go policies. Cloud Storage is one of the important services of cloud computing, which allows data owners to load data to the cloud. Data outsourcing is beneficial to small and medium sized businesses as it is cost effective solution. While making clients free from data storage burdens, cloud brings new and severe security threats in user's outsourced data. The critical issue of data integrity comes whenever client uploads data on un-trustworthy servers. In such scenarios, clients need to implement strategies to prove originality of data. The client may need to access whole file to ensure data integrity, which is time and space consuming. Considering the huge size of the outsourced data and the users constrained resource it is not always possible to access complete data. In this paper, we investigate the approaches of Provable Data Possession (PDP) along with their attributes, functionality, pros and cons. In this paper we surveyed latest core integrity techniques in detail considering functionality used, advantages and disadvantages.

EXISTING SYSTEM:

Remote data integrity checking is of crucial importance in cloud storage. In multi-cloud environment, distributed provable data possession is an important element to secure the remote data. A novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational DiffiHellman) problem. The ID-DPDP protocol can realize private verification, delegated verification and public verification.

DISADVANTAGES OF EXISTING SYSTEM:

- Does not provide security in remote data integrity checking.
- The existing system provides less flexibility.

PROPOSED SYSTEM:

Remote data integrity checking is of crucial importance in cloud storage. In multi-cloud environment, distributed provable data possession is an important element to secure the remote data. we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. In the proposed system we provided a client authorisation such that client can check integrated data over a cloud through secured process. Here we provide an authentication of client in the security model.

ADVANTAGES OF PROPOSED SYSTEM:

- The distributed cloud storage is indispensable.
- Efficient and Flexible.
- Elimination of the certificate management.

ARCHITECTURE:

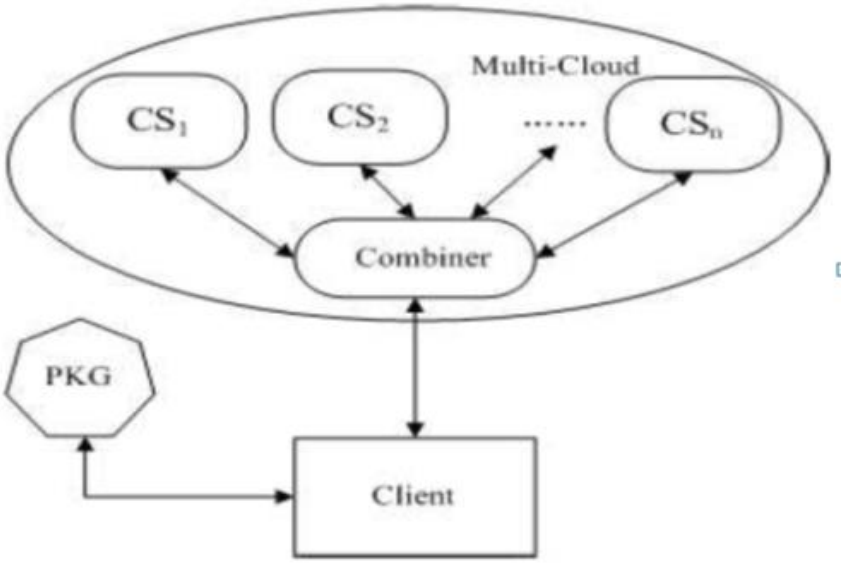


Fig.1 System Architecture

USER:

In the User section the user login to the system then either download the file from the cloud server or upload the file to the cloud server.

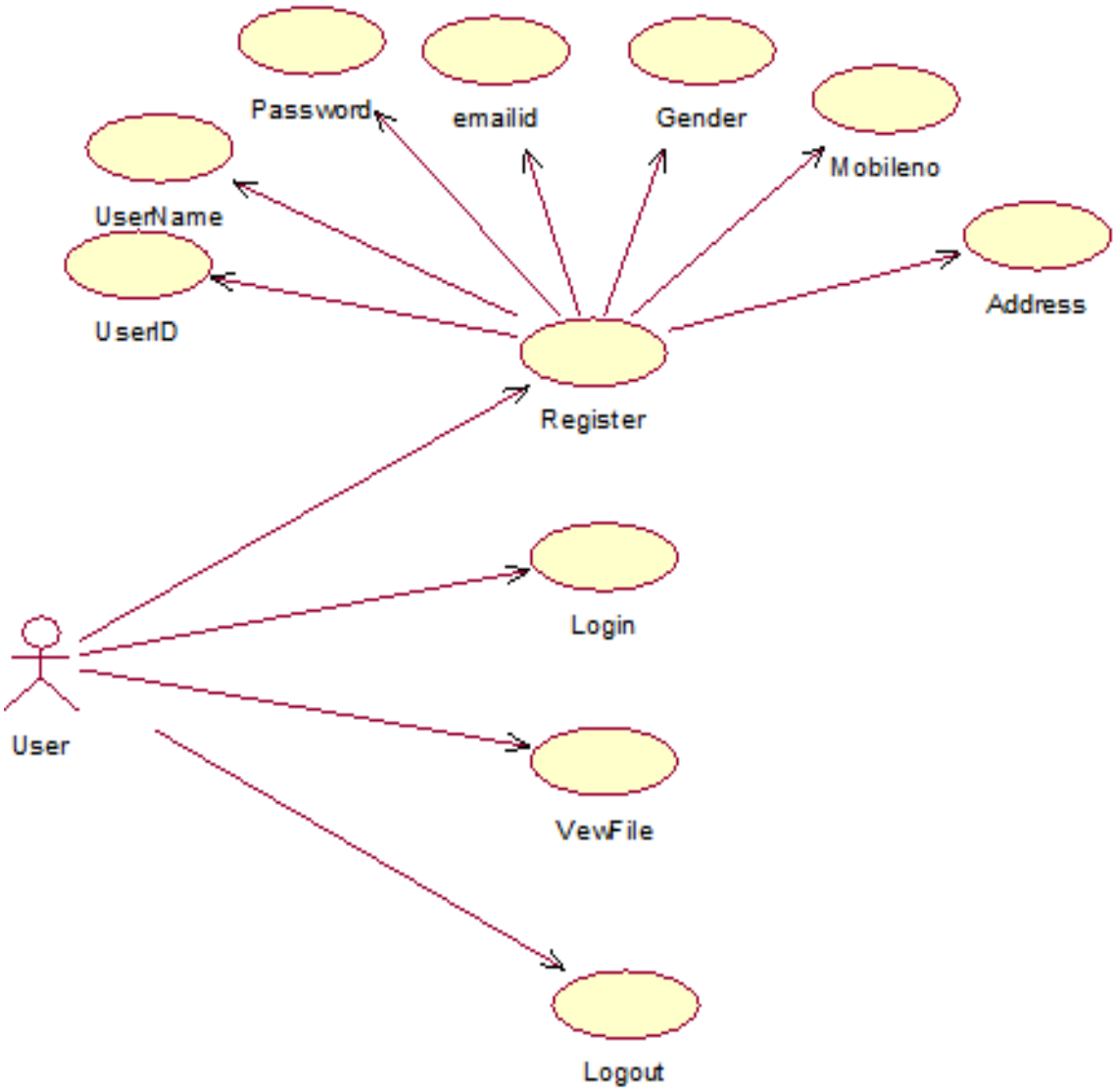


Fig.2 User side process

Owner:

In Owner side register in the system then login to the system after that upload the files then log out from the system

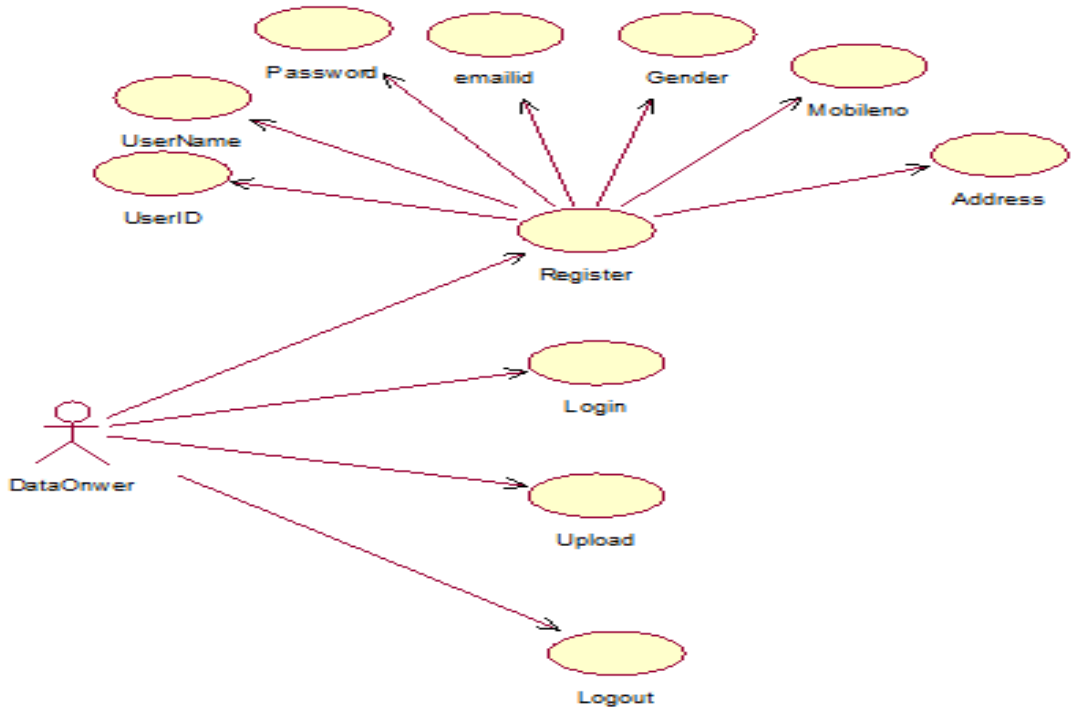


Fig.3 Owner Side Process

Cloud Server:

Cloud server checks the Server name , password and server no then log on to the system accepts the incoming requests.

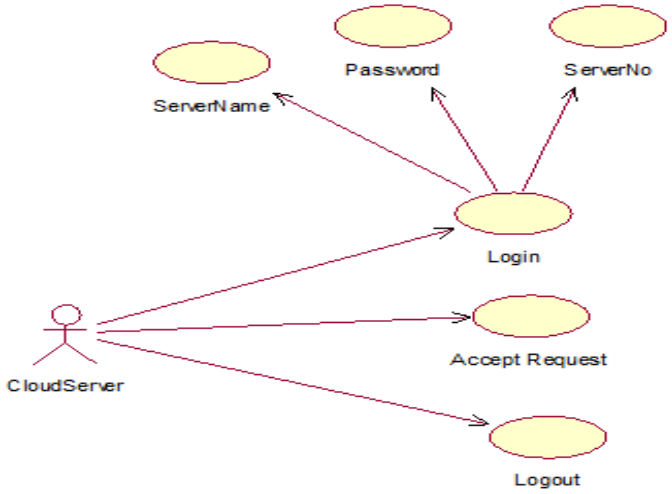


Fig.4 Cloud side process

Verifier :

Verifier can check remote data integrity with a high probability. Based on the RSA, they designed two provably secure PDP schemes.

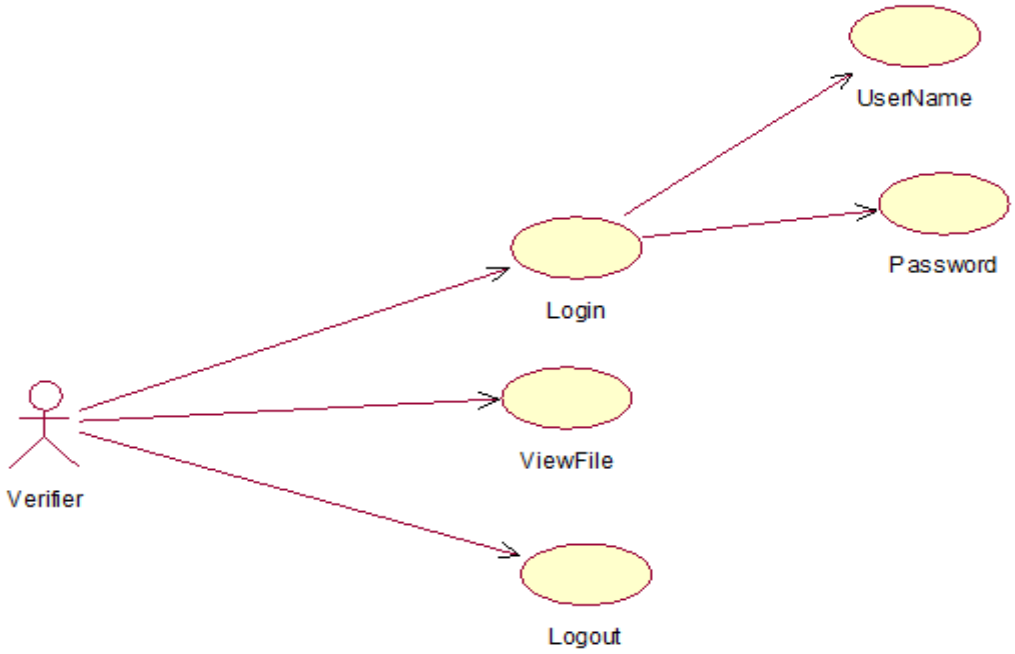


Fig 5. Verifier Side Process

PROVABLE DATA POSSESSION MODEL :

The Provable Data Possession (PDP) is one of the best techniques for ensuring data intactness when the client data is hosted on cloud server. In this technique, the client computes some metadata in order to ensure integrity of hosted data. The metadata is stored at client side and used later on for integrity verification by client. The server stores actual data along with appropriate metadata generated by client. Whenever the client asks for verification, server returns the response which is then verified by client.

In order to improve the performance of the PDP technique, many schemes are proposed under various systems and security models in last some years. The client with data hosted on cloud, requires guarantees about the authenticity of data on cloud, namely that storage servers possess data . It is inadequate to detect that data have been altered when accessing the outsourced data, because it may be too late to recover damaged data. Additionally, the cloud service providers (CSPs) may try to hide data loss and claim that the data is still intact in the Cloud. Hence, data owners need to be convinced always that their data is correctly stored and intact in the Cloud. So, one of the critical concerns with

outsourced data storage is that of data integrity verification. In order to overcome the problem of data integrity verification, many schemes are proposed under different systems and security models.

Algorithm :

Local Auditing Algorithm:

1. initially user_operation_table with null while issues an operation op do
2. if op = w(a) then

   record w(a) in user_operation_table
3. if op = r(a) then

   w(b) Belongs to user_operation_table is the last write
4. if w(a) -> w(b) then

   read your write consistency is violated

   r(c) belongs to user_operation_table is the last read
5. if w(a) -> w(c) then

   monotonic consistency is violated
6. record r(a) in user_operation_table

Global Auditing Algorithm :

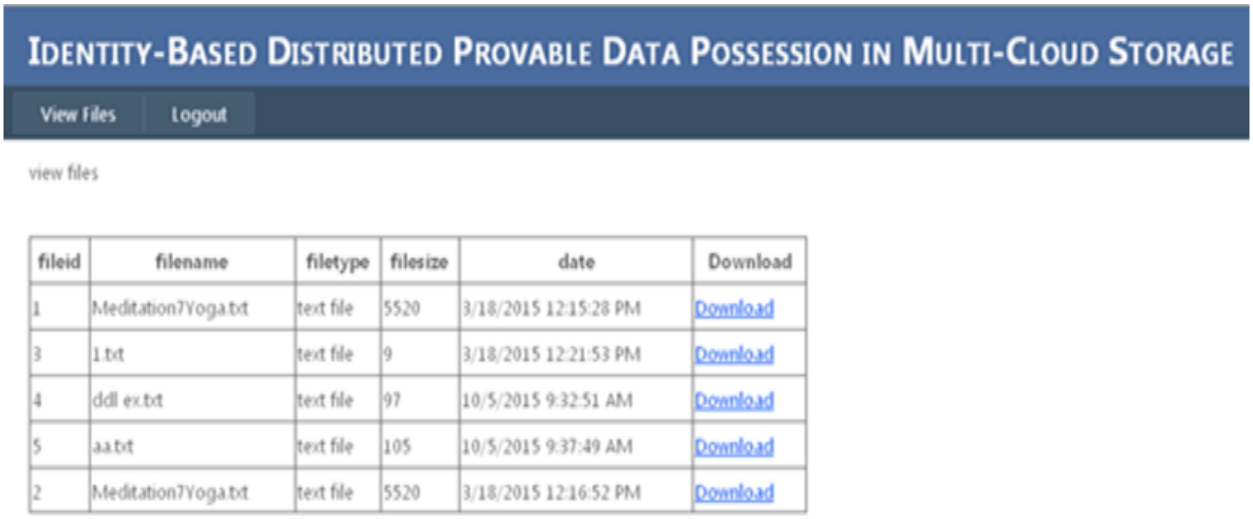
1. for every operation in the global trace is represent by a vertex
2. for operation op1 and op2 do
3. if op1->op2

   Then time edge is added between op1 and op2
4. if op1=w(a),op2=r(a) op1 and op2 comes from different user then data edge is inserted between op1 and op2
5. if op1=w(a) and op=(b) and op1 and op2 comes from different users and w(a)->w(b)->r(b)

then causal edge is inserted between op1 and op2

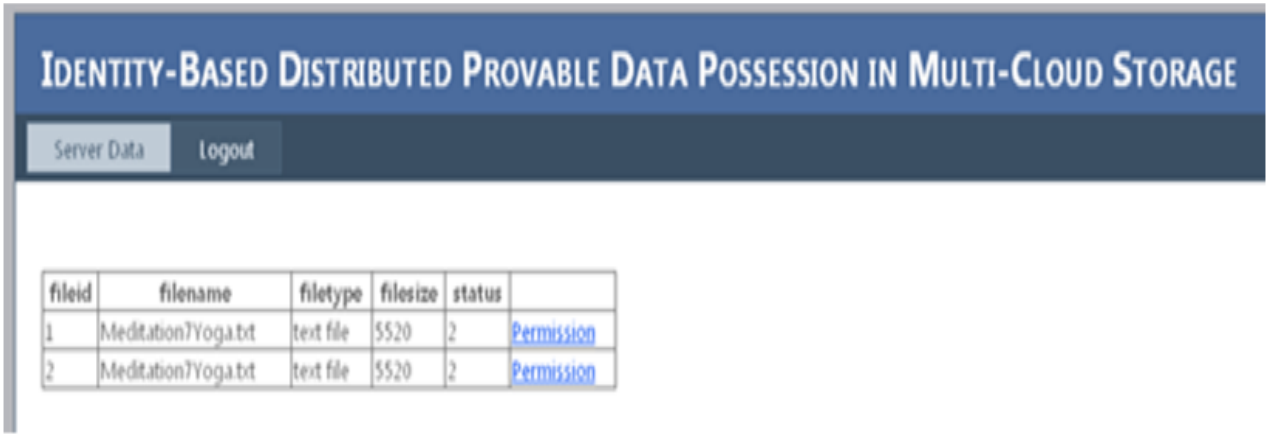
6. verify whether the graph is directed acyclic graph by topological sorting method

Results:

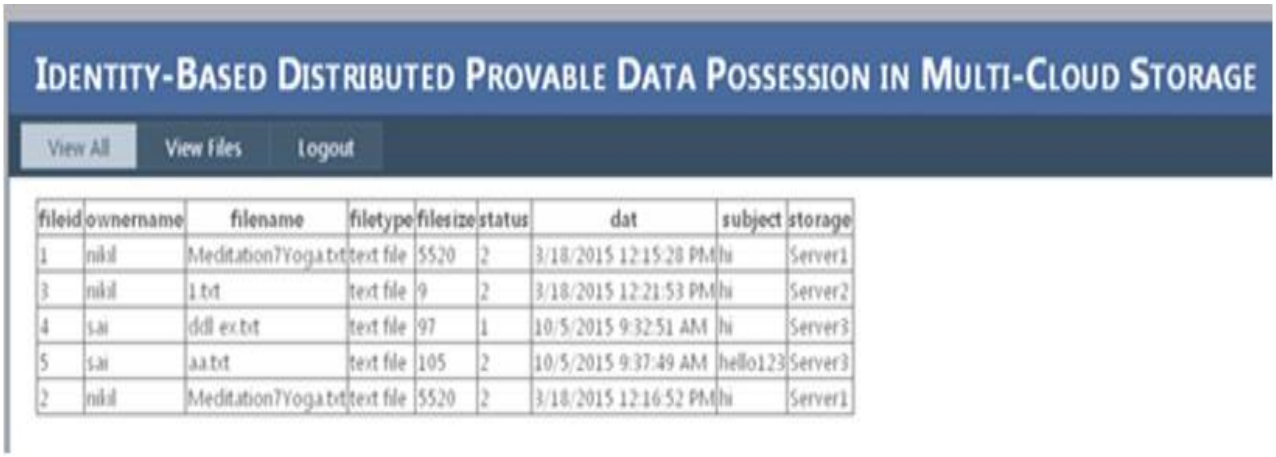


User views the uploaded files

Owner uploads the files



Cloud server checking the files and accept the requests



Cloud server view all the files

Verifier verifies the files in the system

Conclusion :

In cloud computing, the data integrity verification is crucial part. There are many PDP techniques which are available and further improved to achieve efficient integrity verification. We have identified latest PDP variations and compared those PDP schemes based on their approaches, techniques, advantages and disadvantages. As a result, we have proposed the enhanced Identity based PDP scheme for data integrity verification which will make client free from the data intactness checking and also will provide a scheme to perform administrative tasks.We presented the construction of an efficient PDP scheme for distributed cloud storage. Based on Homomorphic verifiable response and hash index hierarchy, we have proposed a cooperative PDP scheme to support dynamic scalability on multiple storage servers. We also showed that our scheme provided all security properties required by zero-knowledge interactive proof system, so that it can resist various attacks even if it is deployed

as a public audit service in clouds. Furthermore, we optimized the probabilistic query and periodic verification to improve the audit performance. Our experiments clearly demonstrated that our approaches only introduce a small amount of computation and communication overheads. Therefore, our solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems. As part of future work, we would extend our work to explore more effective CPDP constructions. Finally, it is still a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. We would explore such a issue to provide the support of variable-length block verification.

REFERENCE:

1. Qi Liu, Enhong Chen, Hui Xiong, Yong Ge, Zhongmou Li, and Xiang Wu ,"A Cocktail Approach for Travel Package Recommendation", IEEE TRANSACTIONS, VOL. 26, NO. 2, FEBRUARY 2014.

2. G.D. Abowd et al., "Cyber-Guide: A Mobile Context-Aware Tour Guide," Wireless Networks, vol. 3, no. 5, pp. 421-433, 1997.

3. G. Adomavicius and A. Tuzhilin, "Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions," IEEE Trans. Knowledge and Data Eng.,
vol. 17, no. 6, pp. 734-749, June 2005.

4. D. Agarwal and B. Chen, "fLDA: Matrix Factorization through Latent Dirichlet Allocation," Proc. Third ACM Int'l Conf. Web Search and Data Mining (WSDM '10), pp. 91-100, 2010.

5.O. Averjanova, F. Ricci, and Q.N. Nguyen, "Map- Based Interaction with a Conversational Mobile Recommender System," Proc. Second Int'l Conf. Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM '08), pp. 212-218, 2008.

6.D.M. Blei, Y.N. Andrew, and I.J. Michael, "Latent Dirichlet Allocation," J. Machine Learning Research, vol. 3, pp. 993-1022, 2003.

7. R. Burke, "Hybrid Web Recommender Systems,"The Adaptive Web, vol. 4321, pp. 377-408, 2007.