An Efficient Authentication Protocol for the Privacy Issues in the Cloud Storage based on Shared Access Authority Mechanism

Sumeet P. Badadali
M.Tech, Computer Network Engineering
T.John Institute Of Technology
Bangalore, India

Ms. Annie Sujith
Assistant Professor, Dept of CSE
T.John Institute Of Technology
Bangalore, India

***Abstract*— Cloud computing is a promising information technology architecture where data owners can remotely store their data in the cloud to enjoy on-demand cloud applications and services from a shared pool of computing resources. But during the data accessing among the multiple users, the data sharing becomes a challenging issue. In order to address this privacy issues, an Efficient Authentication Protocol using Shared Access Authority based mechanism is proposed. The basic idea is to achieve shared access authority when different users may want to access and share each other's authorized data fields. An authentication protocol is proposed to enhance a user's access request related privacy and use an attribute based access control mechanism to realize that a user can reliably access its own data fields. In addition, the security of our scheme is analyzed and it shows that it is both efficient and flexible during data accessing in the cloud computing to achieve privacy-preserving access authority sharing.**

***Index Terms*— Cloud computing, authentication protocol, privacy preservation, shared authority.**

1 INTRODUCTION

CLOUD computing is a promising information technology architecture for both enterprises and individuals. It launches an attractive data storage and interactive paradigm with obvious advantages, including on-demand self-services, ubiquitous network access, and location independent resource pooling [1]. Towards the cloud computing, a typical service architecture is anything as a service (XaaS), in which infrastructures, platform, software, and others are applied for ubiquitous interconnections. Recent studies have been worked to promote the cloud computing evolve towards the internet of services [2], [3]. Subsequently, security and privacy issues are becoming key concerns with the increasing popularity of cloud services. Conventional security approaches mainly focus on the strong authentication to realize that a user can remotely access its own data in on-demand mode. Along with the diversity of the application requirements, users may want to access and share each other's authorized data fields to achieve productive benefits, which brings new security and privacy challenges for the cloud storage.

An example is introduced to identify the main motivation. In the cloud storage based supply chain management, there are various interest groups (e.g., supplier, carrier, and retailer) in the system. Each group owns its users which are permitted to access the authorized data fields, and different users own relatively independent access authorities. It means that any two users from diverse groups should access different data fields of the same file. There into, a supplier purposely may want to access a carrier's data fields, but it is not sure whether the carrier will allow its access request. If the carrier refuses its request, the supplier's access desire will be revealed along with nothing obtained towards the desired data fields. Actually, the supplier may not send the access request or withdraw the unaccepted request in advance if it firmly knows that its request will be refused by the carrier. It is unreasonable to thoroughly disclose the supplier's private information without any privacy considerations. Fig. 1 illustrates three revised cases to address above imperceptible privacy issue.

- *Case 1:* The carrier also wants to access the supplier's data fields, and the cloud server should inform each other and transmit the shared access authority to the both users;
- *Case 2:* The carrier has no interest on other users' data fields, therefore its authorized data fields should be properly protected, meanwhile the supplier's access request will also be concealed;
- *Case 3:* The carrier may want to access the retailer's data fields, but it is not certain whether the retailer will accept its request or not. The retailer's authorized data fields should not be public if the retailer has no interests in the carrier's data fields, and the carrier's request is also privately hidden.

In the cloud environments, a reasonable security protocol should achieve the following requirements. *1) Authentication:* a legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user. *2) Data anonymity:* any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel. *3) User privacy:* any irrelevant entity cannot know or guess a user's access desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing. *4) Forward security:* any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages.

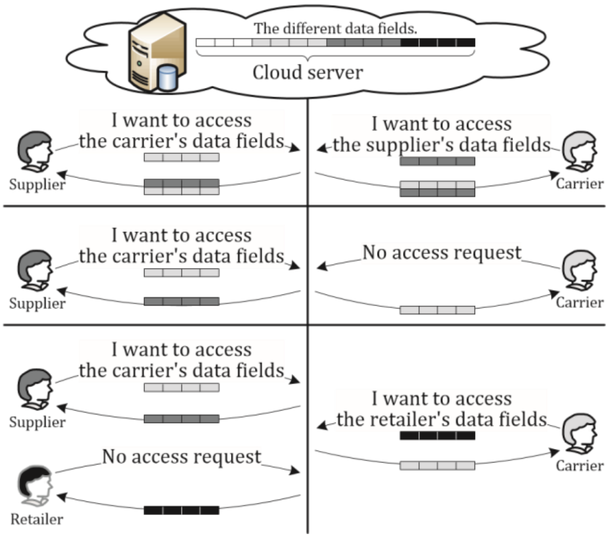
The different data fields.
Cloud server
I want to access the carrier's data fields
Supplier
I want to access the supplier's data fields
Carrier
I want to access the carrier's data fields
Supplier
No access request
Carrier
I want to access the carrier's data fields
Supplier
No access request
Retailer
I want to access the retailer's data fields
Carrier

Fig. 1. Three possible cases during data accessing and data sharing in cloud applications.

Researches have been worked to strengthen security protection and privacy preservation in cloud applications, and there are various cryptographic algorithms to address potential security and privacy problems, including security architectures [4], [5], data possession protocols [6], [7], data public auditing protocols [8]–[10], secure data storage and data sharing protocols [11]–[16], access control mechanisms [17]–[19], privacy preserving protocols [20]–[23], and key management [24]–[27]. However, most previous researches focus on the authentication to realize that only a legal user can access its authorized data, which ignores the case that different users may want to access and share each other's authorized data fields to achieve productive benefits. When a user challenges the cloud server to request other users for data sharing, the access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this work, we aim to address a user's sensitive access desire related privacy during data sharing in the cloud environments, and it is significant to design a humanistic security scheme to simultaneously achieve data access control, access authority sharing, and privacy preservation.

In this paper, we address the aforementioned privacy issue to propose a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user's private information. The main contributions are as follows.

1) Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.
2) Propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.
3) Apply ciphertext-policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users.

2 RELATED WORK

Dunning *et al.* [11] proposed an anonymous ID assignment based data sharing algorithm (AIDA) for multiparty oriented cloud and distributed computing systems. In the AIDA, an integer data sharing algorithm is designed on top of secure sum data mining operation, and adopts a variable and unbounded number of iterations for anonymous assignment. Specifically, Newton's identities and Sturm's theorem are used for the data mining, a distributed solution of certain polynomials over finite fields enhances the algorithm scalability, and Markov chain representations are used to determine statistics on the required number of iterations.

Liu *et al.* [12] proposed a multi-owner data sharing secure scheme (Mona) for dynamic groups in the cloud applications. The Mona aims to realize that a user can securely share its data with other users via the untrusted cloud server, and can efficiently support dynamic group interactions. In the scheme, a new granted user can directly decrypt data files without pre-contacting with data owners, and user revocation is achieved by a revocation list without updating the secret keys of the remaining users. Access control is applied to ensure that any user in a group can anonymously utilize the cloud resources, and the data owners' real identities can only be revealed by the group manager for dispute arbitration.

Grzonkowski *et al.* [13] proposed a zero-knowledge proof (ZKP) based authentication scheme for sharing cloud services. Based on the social home networks, a user centric approach is applied to enable the sharing of personalized content and sophisticated network-based services via TCP/IP infrastructures, in which a trusted third party is introduced for decentralized interactions.

Nabeel *et al.* [14] proposed a broadcast group key management (BGKM) to improve the weakness of symmetric key cryptosystem in public clouds, and the BGKM realizes that a user need not utilize public key cryptography, and can dynamically derive the symmetric keys during decryption. Accordingly, attribute based access control mechanism is designed to achieve that a user can decrypt the contents if and only if its identity attributes satisfy the content provider's policies. The fine-grained algorithm applies access control vector (ACV) for assigning secrets to users based on the identity attributes, and allowing the users to derive actual symmetric keys based on their secrets and other public information. The BGKM has an obvious advantage during adding/revoking users and updating access control policies.

Wang *et al.* [15] proposed a distributed storage integrity auditing mechanism, which introduces the homomorphic token and distributed erasure-coded data to enhance secure and dependable storage services in cloud computing. The scheme allows users to audit the cloud storage with lightweight communication overloads and computation cost, and the auditing result ensures strong cloud storage correctness and fast data error localization..

Sundareswaran *et al.* [16] established a decentralized information accountability framework to track the users' actual data usage in the cloud, and proposed an object-centered approach to enable enclosing the logging mechanism with the users' data and policies. Additionally, distributed auditing mechanisms are also provided to strengthen user's data control, and experiments demonstrate the approach efficiency and effectiveness.

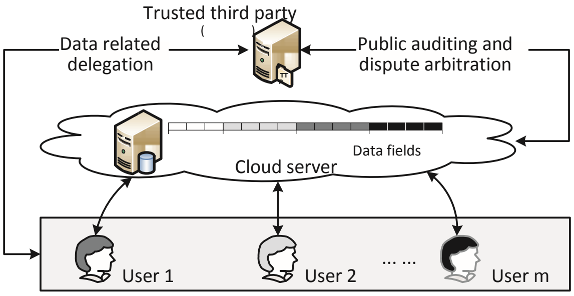

Fig. 2. The cloud storage system model.

In the aforementioned works, various security issues are addressed. However, a user's subtle access request related privacy problem caused by data accessing and data sharing has not been studied yet in the literature. Here, we identify a new privacy challenge, and propose a protocol not only focusing on authentication to realize the valid data accessing, but also considering authorization to provide the privacy-preserving access authority sharing. The attribute based access control and proxy re-encryption mechanisms are jointly applied for authentication and authorization.

3 SYSTEM MODEL

Fig. 2 illustrates a system model for the cloud storage architecture, which includes three main network entities: users (U_x), a cloud server (S), and a trusted third party.

- *User:* an individual or group entity, which owns its data stored in the cloud for online data storage and computing. Different users may be affiliated with a common organization, and are assigned with independent authorities on certain data fields.
- *Cloud server:* an entity, which is managed by a particular cloud service provider or cloud application operator to provide data storage and computing services. The cloud server is regarded as an entity with unrestricted storage and computational resources.
- *Trusted third party:* an optional and neutral entity, which has advanced capabilities on behalf of the users, to perform data public auditing and dispute arbitration.

In the cloud storage, a user remotely stores its data via online infrastructures, platforms, or software for cloud services, which are operated in the distributed, parallel, and cooperative modes. During cloud data accessing, the user autonomously interacts with the cloud server without external interferences, and is assigned with the full and independent authority on its own data fields. It is necessary to guarantee that the users' outsourced data cannot be unauthorized accessed by other users, and is of critical importance to ensure the private information during the users' data access challenges. In some scenarios, there are multiple users in a system (e.g., supply chain management), and the users could have different affiliation attributes from different interest groups. One of the users may want to access other associate users' data fields to achieve bi-directional data sharing, but it cares about two aspects: whether the aimed user would like to share its data fields, and how cannot expose its access request if the aimed user declines or ignores its challenge. In the paper, we pay more attention on the process of data access control and access authority sharing other than the specific file oriented cloud data transmission and management.

Towards the trust model, there are no trust relationships between a cloud server S and a user U_x.

- *S is semi-honest and curious:* Being semi-honest means that S can be regarded as an entity that appropriately follows the protocol procedure. Being curious means that S may attempt to obtain U_x's private information (e.g., data content, and user preferences). It means that S is under the supervision of its cloud provider or operator, but may be interested in viewing users' privacy. In the passive or honest but-curious model, S cannot tamper with the users' data to maintain the system normal operation with undetected monitoring.
- *U_x is rational and sensitive:* Being rational means that U_x's behavior would be never based on experience or emotion, and misbehavior may only occur for selfish interests. Being sensitive means that U_x is reluctant to disclosure its sensitive data, but has strong interests in other users' privacy.

Towards the threat model, it covers the possible security threats and system vulnerabilities during cloud data interactions. The communication channels are exposed in public, and both internal and external attacks exist in the cloud applications [15]. The internal attacks mainly refer to the interactive entities (i.e., S, and U_x). There into, S may be self-centered and utilitarian, and aims to obtain more user data contents and the associated user behaviors/habits for the maximization of commercial interests; U_x may attempt to capture other users' sensitive data fields for certain purposes (e.g., curiosity, and malicious intent). The external attacks mainly consider the data CIA triad (i.e., confidentiality, integrity, and availability) threats from outside adversaries, which could compromise the cloud data storage servers, and subsequently modify (e.g., insert, or delete) the users' data fields.

4 THE SHARED AUTHORITY BASED PRIVACY-PRESERVING AUTHENTICATION PROTOCOL

4.1 *System Initialization*

The cloud storage system includes a cloud server S, and users $\{U_x\}$ ($x = \{1,...,m\}$, $m \in N^*$). Thereinto, U_a and U_b are two users, which have independent access authorities on their own data fields. It means that a user has an access permission for particular data fields stored by S, and the user cannot exceed its authority access to obtain other users' data fields. Here, we consider S and $\{U_a, U_b\}$ to present the protocol phases for data access control and access authority sharing with enhanced privacy considerations.

Fig. 3 shows the system Architecture for the proposed model. The following section describes the proposed system architecture with their each module description.

- Owner Registration: An owner has to upload its files in a cloud server, and then user should register first. After that only the user will be able to do it. Then Registration method is then followed. These details are stored in a database.
- Owner Login: This specifies among the registered person have to login, they should be able to login by mentioning their email ID, password.
- User Registration: If a user has to access the data from cloud, the as mentioned registration is a mandatory step to be followed and data is updated in Database.
- User Login: An authorized user can download the file by using file_id which the owner has specified already.
- Access Control: Owner can allow the access or deny access for accessing the data.
- Encryption & Decryption: aes_encrypt & aes_decrypt is used for encryption and decryption. The file we have uploaded which has to be in encrypted form and decrypt it.
- File Upload: Owner uploads file into database and with the help of this metadata and its contents, it is been downloaded by user and as its encrypted it has to be decrypted.
- File Download: Authorized users can only download the file.
- Cloud Service Provider Registration: If a cloud service provider (maintainer of cloud) wants to do some cloud offer, they should register first.
- Cloud Service Provider Login: After logged in, user can see Cloud provider can view the files uploaded by their clients. This file is to be uploaded to cloud.
- TTP (Trusted Third Party) Login: In this module TTP has monitors the data owners file by verifying the data owner's file and stored the file in a database .CLOUD SERVICE PROVIDER is verified.

Note that full-fledged cryptographic algorithms (e.g., attribute based access control, proxy re-encryption, and theirs variants) can be exploited to support the SAPA.

4.2 The Proposed Protocol Functionality

The SAPA adopts integrative approaches to address secure authority sharing in cloud applications.

- *Authentication:* The ciphertext-policy attribute based access control and bilinear pairings are introduced for identification between U_x and S, and only the legal user can derive the ciphertexts. Additionally, U_x checks the re-computed ciphertexts according to the proxy re-encryption, which realizes flexible data sharing instead of publishing the interactive users' secret keys.
- *Data Anonymity:* The pseudonym $PID_{U\theta}$ are hidden by the hash function so that other entities cannot derives the real values by inverse operations. Hence, an adversary cannot recognize the data, even if the adversary intercepts the transmitted data, it will not decode the full-fledged cryptographic algorithms.
- *User Privacy:* Only if both users are interested in each other's data fields, S will establish the re-encryption key $k_{U\theta}$ to realize authority sharing between U_a and U_b. Otherwise, S will temporarily reserve the desired access requests for a certain period of time, and cannot accurately determine which user is actively interested in the other user's data fields.
- *Forward Security:* The dual session identifiers $\{sid_{S\theta}, sid_{U\theta}\}$ and pseudorandom numbers are introduced as session variational operators to ensure the communications dynamic.

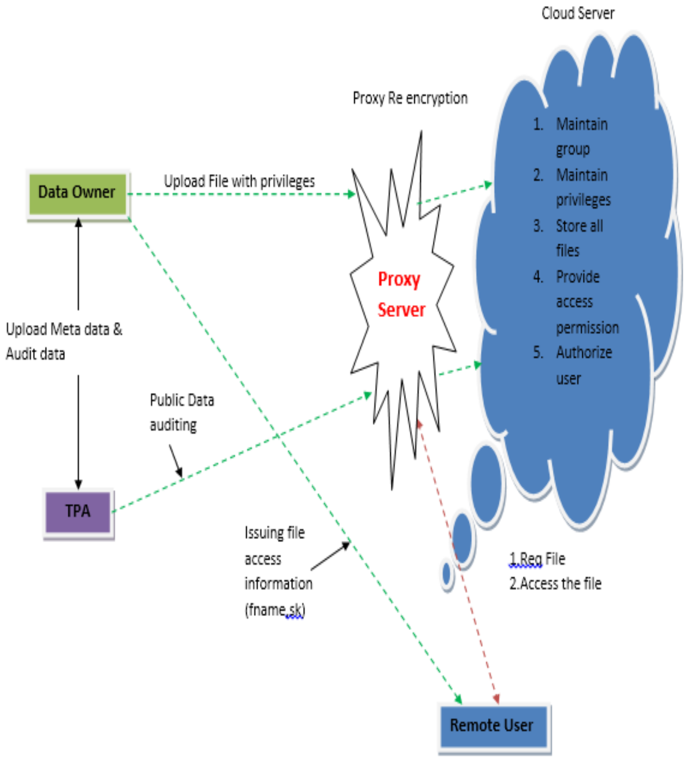

Fig. 3. System Architecture.

5 FORMAL SECURITY ANALYSIS WITH THE UNIVERSAL COMPOSABILITY (UC) MODEL

The universal composability (UC) model specifies an approach for security proofs [28], and guarantees that the proofs will remain valid if the protocol is modularly composed with other protocols, and/or under arbitrary concurrent protocol executions. There is a real-world simulation, an ideal-world simulation, and a simulator *Sim* translating the protocol execution from the realworld to the ideal-world. Additionally, the Byzantine attack model is adopted for security analysis, and all the parties are modeled as probabilistic polynomial-time Turing machines (PPTs), and a PPT captures whatever is external to the protocol executions. The adversary controls message deliveries in all communication channels, and may perform malicious attacks (e.g., eavesdropping, forgery, and replay), and may also initiate new communications to interact with the legal parties.

6 CONCLUSION

In this work, we have identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," National Institute of Standards and Technology, USA, 2009.

[2] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," *IEEE Communications Magazine*, vol. 50, no. 9, pp, 24-25, 2012.

[3] R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services," *IEEE Internet Computing*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493, 2012.

[4] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," *IEEE Internet Computing*, vol. 14, no. 5, pp. 14-22, 2010.

[5] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," *Computer*, vol. 45, no. 7, pp. 73-78, 2012.

[6] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no, 12, pp. 2231-2244, 2012.

[7] H. Wang, "Proxy Provable Data Possession in Public Clouds," *IEEE Transactions on Services Computing*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, 2012.

[8] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, 2012.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847-859, 2011.

[10] C. Wang, K. Ren, W. Lou, J, Lou,"Toward Publicly Auditable Secure Cloud Data Storage Services," *IEEE Network*, vol. 24, no. 4, pp. 19-24, 2010.

[11] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 402-413, 2013.

[12] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure MultiOwner Data Sharing for Dynamic Groups in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.

[13] S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 3, pp. 1424-1432, 2011.

[14] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," *IEEE Transactions on Knowledge and Data Engineering*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, 2012.

[15] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220-232, 2012.

[16] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 556-568, 2012.

[17] Y. Tang, P. C. Lee, J. C. S. Lui, and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE *Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 903-916, 2012.

[18] Y. Zhu, H. Hu, G. Ahn, D. Huang, and S. Wang, "Towards Temporal Access Control in Cloud Computing," in *Proceedings of the 31 st Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012)*, pp. 2576-2580, March 25-30, 2012.

[19] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds," *IEEE Transactions on Parallel and Distributed Systems*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6463404, 2013.

[20] R. Sanchez,´ F. Almenares, P. Arias, D. D´ıaz-Sanchez,´ and A. Mar´ın, "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 1, pp. 95-103, 2012.

[21] H. Zhuo, S. Zhong, and N. Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," *IEEE Transactions on Knowledge and Data Engineering*, vol. 23, no. 9, pp. 1432-1437, 2011.

[22] Y. Xiao, C. Lin, Y. Jiang, X. Chu, and F. Liu, "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing," in *Proceedings of Global Telecommunications Conference (GLOBECOM 2010)*, December 6-10, 2010.

[23] I. T. Lien, Y. H. Lin, J. R. Shieh, and J. L. Wu, "A Novel Privacy Preserving Location-Based Service Protocol with Secret Circular Shift for K-nn Search," *IEEE Transactions on Information Forensics and Security*, 2013.

[24] A. Barsoum and A. Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," *IEEE Transactions on Parallel and Distributed Systems*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6392165, 2013.

[25] H. Y. Lin and W. G. Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 995-1003 , 2012.

[26] J. Yu, P. Lu, G. Xue, and M. Li, "Towards Secure MultiKeyword Top-k Retrieval over Encrypted Cloud Data," *IEEE Transactions on Dependable and Secure Computing*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6425381, 2013.

[27] K. W. Park, J. Han, J. W. Chung, and K. H. Park, "THEMIS: A Mutually Verifiable Billing System for the Cloud Computing Environment," *IEEE Transactions on Services Computing*, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6133267, 2012.

[28] R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," in *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science (FOCS 2001)*, pp. 136-145, October 14-17, 2001.