Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 3, March : 2023

CLOUD TECHNOLOGY WITH CLOUD COMPUTING INFERENCE ATTACK-RESISTANCE E-HEALTH CARE BY USING FINE GRAINED ACCESS CONTROL

SHAIK SHAMMA PG Scholar, Dept of CSE, Quba College of Engineering & Technology, Venkatachalam, AP, India.

M.HYMAVATHI Assistant Professor, Dept of CSE, Quba College of Engineering & Technology, Venkatachalam, AP, India.

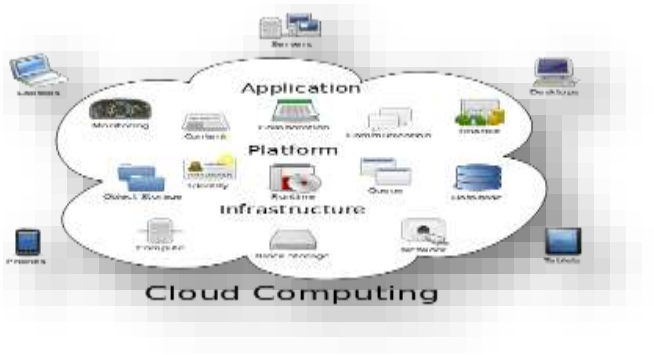
ABSTRACT

Data sharing among numerous users as well as cloud storage are both prevalent with cloud data services. Sadly, there are hardware/software failures, human errors, and other factors that raise doubts about the integrity of cloud data. Several procedures have been created to make it possible for both data owners and public verifiers to effectively verify the integrity of cloud data without having to download the complete database from the cloud server. Yet, using these current systems for public auditing on the integrity of shared data will ultimately lead to the disclosure of private information—identity—to public verifiers. I provide a novel privacy-preserving approach that permits public auditing of shared data kept in the cloud in this work. I use ring signatures in particular to compute the verification information required to audit the accuracy of shared data. With the help of our approach, public verifiers can effectively check the integrity of shared data without having to download the full file, while the identity of the signer on each block in private data is kept secret. Additionally, rather than validating each auditing activity individually, our mechanism may carry out several auditing tasks at once. Our test findings show that our technique is effective and efficient at verifying the integrity of shared data.

1. INTRODUCTION

Using computer resources (hardware and software) that are provided as a service across a network is known as cloud computing (typically the Internet). The name is derived from the widespread use of a cloud-shaped symbol in system diagrams as a metaphor for the intricate infrastructure it holds. Cloud computing entrusts the data, software, and processing of a user to remote services. Hardware and software resources are made accessible via the Internet as managed third-party services in cloud computing. These services often give users access to cutting-edge server networks and sophisticated software programmers..

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 3, March : 2023



Structure of cloud computing

Working Principle of Cloud Computing:

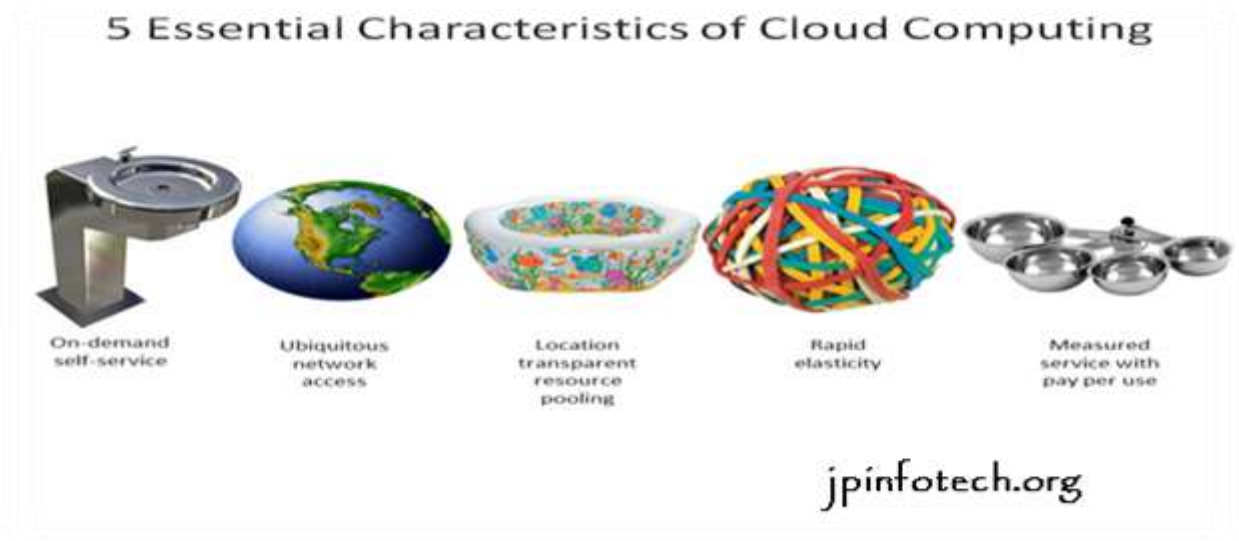
Cloud computing aims to apply conventional supercomputing, or high-performance computing power, typically used by military and research facilities, to perform tens of trillions of computations per second in consumer-oriented applications like financial portfolios, deliver personalized information, provide data storage, or power massively multi-player computer games. Networks of enormous clusters of computers, often running low-cost consumer PC technology with specialised connections, are used in cloud computing to distribute data processing tasks among them. Large networks of interconnected systems make up this shared IT infrastructure. Virtualization methods are frequently employed to increase the power of cloud computing..

Characteristics and Services Models

According to the National Institute of Standards and Terminology's (NIST) definitions, the key aspects of cloud computing are as follows:

On-demand self-service: A customer can automatically supply computing resources as needed, such as server time and network storage, without needing to deal with the supplier of each service in person.Wide network access: Capabilities are accessible via the network and used through common mechanisms to encourage adoption by various thin- or thick-client platforms (e.g., mobile phones, laptops, and PDAs).Resource pooling: Using a multi-tenant approach, the provider's computing resources are combined to serve numerous customers, with various physical and virtual resources being dynamically assigned and reassigned in response to customer demand. The customer typically has no control or knowledge over the precise location of the resources offered, although they might be able to specify location at a higher level of abstraction, giving the impression that the resources are location-independent (e.g., country, state, or data center). Storage, computation, memory, network bandwidth, and virtual machines are a few examples of resources.Fast elasticity: Capabilities can be provisioned

quickly and elastically, often automatically, to scale out quickly and released quickly to scale in quickly. Consumers frequently perceive the provisioning capabilities as being limitless and able to be ordered in any quantity at any time. Measured service: By utilizing a metering capability at some level of abstraction suited to the type of service, cloud systems automatically control and optimize resource utilization (e.g., storage, processing, bandwidth, and active user accounts). The management, control, and reporting of resource utilization can ensure transparency for both the service provider and the service user..



Characteristics of cloud computing

2. LITERATURE SURVEY

1 "Oruta: Privacy-Preserving PublicAuditing for Shared Data in the Cloud,"

AUTHORS: B. Wang, B. Li, and H. Li,

Data sharing among numerous users as well as cloud storage are both prevalent with cloud data services. Sadly, there are hardware/software failures, human errors, and other factors that raise doubts about the integrity of cloud data. Several procedures have been created to make it possible for both data owners and public verifiers to effectively verify the integrity of cloud data without having to download the complete database from the cloud server. Yet, using these current systems to conduct public audits on the accuracy of shared data will eventually expose personal information to verifiers in the public domain. We suggest a novel privacy-preserving approach in this research that permits public auditing of shared data kept in the cloud..We use ring signatures in particular to compute the verification information required to audit the accuracy of shared data. With the help of our approach, public verifiers

can effectively check the integrity of shared data without having to download the full file, while the identity of the signer on each block in private data is kept secret. Additionally, rather than validating each auditing activity individually, our mechanism may carry out several auditing tasks at once. Our test findings show that our technique is effective and efficient at verifying the integrity of shared data..

2.**"Security Challenges for the PublicCloud,"**

AUTHORS:K. Ren, C. Wang, and Q. Wang,

I'll first go through some of the most important security issues facing cloud computing, such as data service outsourcing security and safe computation outsourcing. The security of data storage in cloud computing will then be my main focus. Cloud storage, one of the more basic services, enables data owners to outsource their data to the cloud because of its alluring advantages. The lack of owners' physical custody of the outsourced data, however, poses serious security questions about the storage accuracy. So, it becomes crucial and difficult to enable safe storage audits in a cloud context. In this lecture, I'll outline our technological strategies, security & performance evaluations, and our most current research initiatives towards storage outsourcing security in cloud computing..

3**. "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,"**

AUTHORS:C. Wang, Q. Wang, K. Ren, and W. Lou

The long-awaited realisation of computing as a service is cloud computing, which enables users to remotely store their data in the cloud and access high-quality applications and services from a pool of programmable computer resources on demand. Users can be spared of the responsibility of local data storage and upkeep by outsourcing their data. Yet, since users no longer physically hold the potentially vast size of outsourced data, protecting data integrity in the cloud is a highly difficult undertaking that could be extremely difficult, especially for users with limited computer resources and capabilities.Therefore, it is crucial to enable public audit capability for cloud data storage security so that customers can depend on an outside audit party to verify the accuracy of outsourced data when necessary. The following two fundamental conditions must be satisfied in order to introduce a third party auditor (TPA) in a secure manner: 1) TPA should be able to audit cloud data storage effectively without requesting a local copy of the data and shouldn't place an additional online strain on cloud users. 2) The third party auditing procedure shouldn't result in any new privacy risks for users' data..The public key based homomorphic authenticator and random masking are used in this research to create a privacy-preserving public cloud data auditing system that satisfies all of the aforementioned requirements. We further investigate the bilinear aggregate signature technique to expand our main conclusion into a multi-user setting, where TPA can carry out numerous auditing tasks concurrently, to facilitate efficient management of many auditing activities. A thorough investigation of security and performance reveals that the suggested techniques are both incredibly effective and provably secure..

4.“**Computing Encrypted Cloud Data Efficiently under Multiple Keys,”**

AUTHORS: B. Wang, M. Li, S.S. Chow, and H. Li,

Users now have a wide range of chances to use the cloud's computational capacity to process data that has been given by many people. Due to privacy considerations, these cloud data should be encrypted using several keys. Existing secure computation methods, however, are either restricted to a single key or remain somewhat impractical. In this research, we offer two effective methods for secure computing via multiple-key cloud data outsourcing. Our methods leverage two non-colluding cloud servers to jointly compute polynomial functions over encrypted cloud data from numerous users without learning the inputs, intermediate results, or final outcomes. The two cloud servers and users only need to contact seldom. We use applications in machine learning to experimentally show the effectiveness of our techniques.. Our schemes are also applicable to privacy-preserving data aggregation such as in smart metering.

5.**“Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,”**

AUTHORS: S. Yu, C. Wang, K. Ren, and W. Lou,

An emerging paradigm of computing is cloud computing, in which resources from the computing infrastructure are made available as online services. As exciting as it is, this paradigm also presents a number of fresh difficulties for access control and data security when users share critical information on cloud servers, which are outside of the trusted network of data owners. Existing solutions often employ cryptographic techniques by granting access to data decryption keys to only authorised users in order to protect sensitive user data against untrusted services. Unfortunately, when fine-grained data access control is required, these methods often impose a significant computing overhead on the data owner and as a result do not scale effectively..In reality, there is still no solution to the issue of obtaining fine-grainedness, scalability, and data secrecy of access control. This paper tackles this difficult open problem by, on the one hand, defining and enforcing access policies based on data attributes, and, on the other hand, enabling the data owner to outsource the majority of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We accomplish this by taking advantage of and specifically fusing attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption approaches. Other noteworthy features of our suggested system are user secret key accountability and user access privilege confidentiality. Our proposed approach is very effective and provably secure under the current security models, according to extensive analysis..

6.“PORs: Proofs of Retrievability for Large Files”.
AUTHORS:A.Juels and B. S. Kaliski,

We discuss retrievability proofs and define them (POR). A POR technique allows an archive or backup service (prover) to quickly demonstrate that a user (verifier) can restore a target file F, i.e., that

the archive dependably stores and sends file data necessary for the user to fully recover F. A POR can be thought of as a specific type of cryptographic proof of knowledge (POK) that is made to deal with huge files (or bit strings), or F. Here, we examine POR protocols where the user's (verifier) storage needs, the prover's memory accesses, and the communication costs are all tiny quantities that are virtually independent of the length of F. Along with suggesting new, We investigate implementation issues and optimizations that affect previously investigated, related schemes in the context of practical POR structures. Unlike a POK, neither the prover nor the verifier must really be familiar with F in a POR. Another addition of our work is the creation of the security concept that PORs lead to, which is novel and unusual.

PORs are crucial for semi-trusted online archives, in our opinion. Users can guarantee the confidentiality and integrity of files they retrieve using existing cryptographic mechanisms. Nonetheless, it is also normal for users to want to make sure archives don't remove or change files before retrieval. A POR's objective is to carry out these checks without requiring users to download the files directly. PORs can also guarantee quality of service., i.e., show that a file is retrievable within a certain time bound.

7 .“Scalable and Efficient Provable Data Possession”.

AUTHORS: G. Ateniese, R. D. Pietro,

The authors of this paper present a concept for proven data possession (PDP), which enables a client who has saved data at an untrusted server to confirm that the server actually has the original data without having to retrieve it. The model significantly lowers I/O costs by generating probabilistic proofs of possession from samples of random sets of server-side blocks. To validate the proof, the client keeps a consistent quantity of metadata. The challenge/response protocol minimises network communication by transmitting a small, constant quantity of data. Consequently, big data sets in widely dispersed storage systems are supported by the PDP paradigm for remote data validation. A dynamic verifiable data possession protocol based on cryptographic hash functions and symmetric key encryption was created by Ateniese et al. to assist the dynamic auditing..Their plan is to pre-calculate a specific number of metadata during setup, limiting and fixing the number of modifications and challenges in advance.

The author develops a PDP method that is both extremely effective and symmetric key cryptographically safe, without the need for mass encryption. Furthermore, unlike its forerunners, this PDP approach enables outsourcing of dynamic data and effectively supports operations like block modification, deletion, and append

3. PROBLEM STATEMENT

Public auditing is a term used to describe a number of technologies that enable both the data owner and a third party to easily undertake integrity checks without downloading all of the data from the cloud. These algorithms retrieve a random combination of the blocks rather than the entire data during integrity checking. Data is separated into numerous small blocks, each of which is independently signed by the

owner. A data user (such as a researcher) who wishes to use the owner's data via the cloud or a third-party auditor (TPA) who can offer knowledgeable integrity checking services could both be considered public verifiers. Wang et al. created an enhanced auditing method as a further step..in order to prevent any public verifiers from learning the contents of private data belonging to a personal user during public auditing on cloud data. Sadly, the aforementioned public auditing tools are solely concerned with cloud-based personal data. One of the most interesting elements that encourages cloud storage, in our opinion, is the ability to share data between numerous users. Thus, it is equally essential to guarantee the accuracy of shared data integrity in the cloud. In fact, shared data integrity can be confirmed by extending the capabilities of current public auditing tools. Yet, the disclosure of identity privacy to public verifiers has emerged as a new, serious privacy concern in the context of shared data when using existing procedures..

LIMITATION OF SYSTEM:

If identity privacy on shared data is not maintained during public auditing, critical confidential information will be made available to public verifiers. 2. Protecting this personal information is crucial if you want to maintain your privacy when having your identification checked by the public during public auditing..

4. PROPOSED SYSTEM

In this research, we present Oruta, a unique privacy-preserving public auditing system, to address the aforementioned privacy problem on shared data. More specifically, we build homomorphicauthenticators in Oruta using ring signatures, which allows a public verifier to check the integrity of shared data without having to download the entire file while keeping the signer's identity hidden from the public verifier. Furthermore, we expand our method to accommodate batch auditing, which can carry out several auditing activities at once and enhance the effectiveness of verification for numerous auditing tasks..Random masking, which has been used in WWRL and can protect data privacy from outside verifiers, is compatible with Oruta. To enable dynamic data, we also use index hash tables from a previous open auditing solution. Oruta and existing mechanisms are compared on a high level..

ADVANTAGES OF PROPOSED SYSTEM:

A public verifier can accurately assess the integrity of shared data. Throughout the auditing process, a public verifier cannot tell who signed each block in the shared data.

The generated ring signatures can support blockless verifiability as well as the preservation of identity privacy.

5. SYSTEM ARCHITECTURE

The cloud server, the third party auditor (TPA), and users are all involved in the architecture.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 3, March : 2023

The initial user and various group users are the two different categories of users in a group. Members of the group include both the original user and the group users. According to access control policies, group members are permitted to see and edit shared data that was created by the original user. The cloud server houses both the shared data and the verification data (i.e. signatures) associated with it. On behalf of the group members, the third party auditor is able to confirm the accuracy of shared data in the cloud server. Our system paradigm includes users, a cloud server, and an outside auditor..Before outsourcing data to the cloud, the user is in charge of determining who has access to her data. An auditing request must first be sent to the TPA by the user who wants to verify the accuracy of supplied data. The TPA generates an auditing message to the cloud server after receiving the auditing request, and then retrieves an auditing proof of shared data from the cloud server. The TPA then confirms that the auditing proof is accurate. Ultimately, based on the verification's outcome, the TPA delivers the user an auditing report..

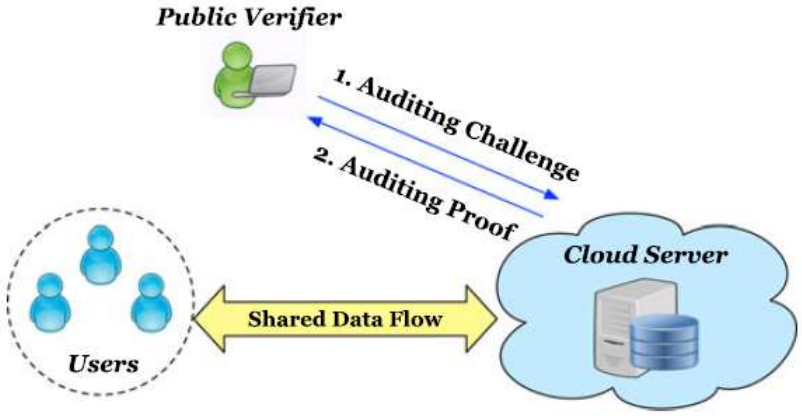


FIG: 5.1 SYSTEM ARCHITECTURE

6. IMPLEMENTATION

6.1 Cloud server

We create our system using a cloud server in the first module, where data is kept on an international scale. The following qualities should be attained by our system, Oruta: (1) Public Auditing: Without downloading the complete database from the cloud, a public verifier can publicly vouch for the accuracy of shared data. Correctness: A public verifier can successfully check the integrity of shared data. Unforgeability: The only user who can produce legitimate verification metadata (i.e., signatures) on shared data is a member of the group. Identity Privacy: Throughout the auditing process, a public verifier cannot determine the identity of the signer on each block of shared data..

6.2 Group of users

The initial user and various group users are the two different categories of users in a group. Shared data is initially created in the cloud by the original user and distributed to group users. Members of the group include both the original user and other users. Everyone in the group has access to and permission to edit shared data. The cloud server houses both the shared data and the verification information (i.e., signatures) for it. The integrity of shared data stored on the cloud server can be publicly verified by a public validator, such as a third-party auditor providing expert data auditing services or a data user outside the group planning to use shared data.Owner Registration: Before uploading any files in this module, the owner must first register. Only then can he or she accomplish it. He must complete the registration form's details in order to do that. A database contains these specifics. Owner Login: To access this module, owners must first log in using their email address and password. User Registration: In this module, users must first register their information in order to access the data that is saved in the cloud. These particulars are kept in a database. User Login: If the user is a permitted user, he or she may download the file using the file id that the data owner has recorded when it was uploading.

6.3 Public verifier

A public verifier must first submit an auditing challenge to the cloud server in order to verify the accuracy of shared data. The cloud server responds to the public verifier after receiving the auditing challenge by providing an auditing evidence of the presence of shared data. The accuracy of the auditing evidence is then confirmed by this public verifier, who then examines the accuracy of the full dataset. Public auditing is essentially a challenge-and-response protocol between a public verifier and a cloud server.

6.4 Auditing Module

If a third-party auditor is used in this module, TPA (the cloud maintainer) must first register. Under this system, only cloud service providers are permitted. Once logged in, the third party auditor can see how many data owners have uploaded their files to the cloud. Here, we offer TPA to keep the clouds maintained. We only think about using static groups to audit the consistency of shared data in the cloud. It denotes that the group has already been established before shared data is created in the cloud and that its membership is maintained throughout data sharing. The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud. Another interesting problem is how to audit the integrity of shared data in the cloud with *dynamic groups* — a new user can be added into the group and an existing group member can be revoked during data sharing — while still preserving identity privacy.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 3, March : 2023

7. OUTPUT RESULTS

REMOVING A FILE:

After updating a file if unnecessary data present in the group then remove a file using delete command.

PUBLIC VERIFIER:

Here public verifier enter their username and password and check whether file is updated or not.

8. CONCLUSION

In this paper, I tend to suggest Oruta, a public auditing system for cloud-based shared knowledge that protects anonymity. We like to use ring signatures to build homomorphic authenticators, allowing a public protagonist to audit shared knowledge integrity without getting all of the information but still unable to discriminate. The signer on each block is a representative of the United Nations. We tend to further improve our technique to facilitate batch auditing to increase the effectiveness of collateral numerous auditing tasks.We'll continue to research two exciting themes for our upcoming work. One of them is traceability, which denotes the cluster manager's (i.e., the first user's) ability to disclose the identity of the signer supported verification data in specific unique circumstances. Our design doesn't support traceability because Oruta is based on ring signatures, where the signer's identity is flatly protected [21]. According to the most accurate data we have, there is still room for improvement in the planning of a cheap public auditing system with support for traceability and the ability to protect identify privacy..

9. FUTURE ENHANCEMENT

We improve the Oruta system in two intriguing problems that we will keep researching for our upcoming work. One of them is traceability, which refers to the group manager's (i.e., the original user's) capacity to, in some exceptional circumstances; divulge the identity of the signer based on verification information. Our current architecture does not provide traceability because Oruta is built on ring signatures, which unconditionally safeguard the signer's identity. To the best of our knowledge, there is still work to be done on creating a reliable public auditing system that can assist traceability while protecting identity privacy. How to demonstrate data freshness will be a further challenge for our future efforts (prove the cloud possesses the latest version of shared data) while still preserving identity privacy.

10 .REFERENCES

1. B. Wang, B. Li, and H. Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,” Proc. IEEE Fifth Int’l Conf. Cloud Computing, pp. 295-302, 2012.

2. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,” Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

3. K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

4. D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud Data Protection for the Masses,” Computer, vol. 45, no. 1, pp. 39-45, 2012.

5. C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” Proc. IEEE INFOCOM, pp. 525-533, 2010.

6. B. Wang, M. Li, S.S. Chow, and H. Li, “Computing Encrypted Cloud Data Efficiently under Multiple Keys,” Proc. IEEE Conf. Comm. and Network Security (CNS ’13), pp. 90-99, 2013.

7. R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems,” Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

8. The MD5 Message-Digest Algorithm (RFC1321). https://tools. ietf.org/html/rfc1321, 2014.

9. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-610, 2007.

10. H. Shacham and B. Waters, “Compact Proofs of Retrievability,” Proc. 14th Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT ’08), pp. 90-107, 2008.

11. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, “Dynamic Provable Data Possession,” Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09), pp. 213-222, 2009.

12. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing,” Proc. 14th European Conf. Research in Computer Security (ESORICS’09), pp. 355-370, 2009.

13. C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. 17th Int’l Workshop Quality of Service (IWQoS’09), pp. 1-9, 2009.

14. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Remote Data Checking for Network Coding-Based Distributed Storage Systems,” Proc. ACM Workshop Cloud Computing Security Workshop (CCSW’10), pp. 31-42, 2010.

15. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau, “Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds,” Proc. ACM Symp. Applied Computing (SAC’11), pp. 1550-1557, 2011.

16. N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, “LT Codes-Based Secure and Reliable Cloud Storage Service,” Proc. IEEE INFOCOM, 2012.

17. B. Wang, B. Li, and H. Li, "Certificateless Public Auditing for Data Integrity in the Cloud," Proc. IEEE Conf. Comm. and Network Security (CNS'13), pp. 276-284, 2013.

18. C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

19. B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp. 2904-2912, 2013.

20. B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Trans. Services Computing, 20 Dec. 2013, DOI: 10.1109/TSC.2013.2295611.

21. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT'03), pp. 416-432, 2003.
22. B. Wang, H. Li, and M. Li, "Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics," Proc. IEEE Int'l Conf. Comm. (ICC'13), pp. 539-543, 2013.

23. B. Wang, S.S. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS'13), pp. 124-133, 2013.

24. D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," Proc. 24th Ann. Int'l Cryptology Conf. (CRYPTO'04), pp. 41-55, 2004.

25. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS'12), pp. 507-525, June 2012.

26. E. Brickell, J. Camenisch, and L. Chen, "Direct Anonymous Attestation," Proc. 11th ACM Conf. Computer and Comm. Security (CCS'04), pp. 132-145, 2004.

27. D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 514-532, 2001.

R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 552-565, 2001.