International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Integrity auditing for multi copy in cloud storage based on RED-BLACK tree

Ms.Aarthi Kasthuri[1], A. Shirisha[2], K. Bindhu[3], Ch. Vandhana[4], Ch. Hasika [5]
[2,3,4,5] UG Scholars, Department of CSE, ***MALLA REDDY ENGINEERING COLLEGE FOR WOMEN***, Hyderabad, Telangana, India.
[1]Assistant Professor, Department of CSE, ***MALLA REDDY ENGINEERING COLLEGE FOR WOMEN***, Hyderabad, Telangana, India.

ABSTRACT

With the rapid development of cloud storage, cloud users are willing to store data in the cloud storage system, and at the same time, the requirements for the security, integrity, and availability of data storage are getting higher and higher. Although many cloud audit schemes have been proposed, the data storage overhead is too large and the data cannot be dynamically updated efficiently when most of the schemes are in use. In order to solve these problems, a cloud audit scheme for multi-copy dynamic data integrity based on red-black tree full nodes is proposed. This scheme uses ID-based key authentication, and improves the classic Merkel hash tree MHT to achieve multi-copy storage and dynamic data manipulation, which improves the efficiency of real-time dynamic data update (insertion, deletion, modification). The third-party audit organization replaces users to verify the integrity of data stored on remote cloud servers, which reduces the computing overhead and system communication overhead. The security analysis proves that the security model based on the CDH problem and the DL problem is safe. Judging from the results of the simulation experiment, the scheme is safe and efficient .

INTRODUCTION

In the face of increasing user management and sharing needs, the emergence of cloud computing and cloud storage provides a new scheme for it. Users can obtain sufficient storage capacity at a lower price, and at the same time, highly concentrated computing resources greatly improve computing power. Usually when people use cloud storage services, they upload their data to the cloud and store it on a remote cloud server. In order to save local storage resources, the local copy will be deleted. There are two hidden dangers in this way.

One is the lack of control over the confidentiality and integrity of the data and the other is that it is difficult to recover the data if the local copy is deleted. In order to solve these problems, the researchers proposed that

users can encrypt data before outsourcing and sending it to a remote cloud server. People also think of improving the availability and recoverability of data by storing multiple copies of the original data. Suppose that part of the users' data is damaged, only one copy of the data is needed to restore the data correctly, and it remains unchanged with the data in the cloud .

Ateniese et al. proposed the concept of provable data possession (PDP). Users can effectively verify the integrity of cloud server data without retrieving the entire file, and based on homomorphic linear verification,

they proposed an effective and proved a secure PDP scheme, but the scheme it proposes is only for static data. In the case of increasing data, dynamic operation of data is also a key research point of later researchers . Wang et al. proposed a dynamic data scheme based on Merkle hash tree. Luo et al. used the Shamir secret sharing concept to improve the authentication tag based on polynomials. Barsoum et al. extended the PDP model and proposed a map-based provable multi-copy dynamic data possession (MB-PMDDP) scheme. Users can dynamically manipulate data and store fewer copies. Security is guaranteed, but any insert and delete operations will result in the need to recalculate the label and the position of the operation block, which will incur high calculation costs. Subsequently, the scheme was proposed, which greatly improved the method of dynamic update efficiency.

At the same time, Yang et al. proposed a public cloud audit scheme for dynamic update of user data and revocation of user data, but it did not solve the problem of dynamic revocation at any time. Min et al. proposed an integrity verification scheme based on spatiotemporal chaos, which supports dynamic data analysis, blinding information, and preventing third parties from leaking user data privacy. Min et al. proposed a data integrity verification scheme based on a binary balanced tree. The efficiency of data update has been greatly improved, and it also provides us with a research direction.

LITERATURE SURVEY

TITLE: ''Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium,''

ABSTRACT: To verify the integrity of cloud data, many cloud storage auditing schemes have been proposed. However, most of them incur a lot of computation overhead for users when

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
IJARST
ISSN: 2457-0362

data authenticators are generated or the data integrity is verified, which inevitably brings in heavy burdens to resource-constrained users. To overcome this problem, we propose a cloud storage auditing scheme for group users, which greatly reduces the computation burden on the user side. In our scheme, we introduce a Third Party Medium (TPM) to perform time-consuming operations on behalf of users. The TPM is in charge of generating authenticators for users and verifying data integrity on behalf of users. In order to protect the data privacy against the TPM, we blind data using simple operations in the phase of data uploading and data auditing. The user does not need to perform time-consuming decryption operations when using cloud data. We set an expiration time of the authorization to make sure only the TPM who possesses the authorization within valid period is able to upload data to the cloud and challenge the cloud data. The security proof and the performance analysis show that our proposed scheme is secure and efficient.

TITLE: 'Cloud and IoT based smart architecture for desalination water treatment,''

ABSTRACT: Increasing water demand and the deteriorating environment has continuously stressed the requirement for new technology and methods to attain optimized use of resources
and desalination management, converting seawater into pure drinking water. In this age, the Internet of Things use allows us to optimize a series of previously complicated processes to perform and required enormous resources. One of these is optimizing the management of water treatment. This research presents an implementable water treatment model and suggests smart environment that can control water treatment plants. The proposed system gathers data and analysing to provide the most efficient approach for water desalination operations.
The desalination framework integrates smart enabling technologies such as Cloud Portal, Network communication, Internet of Things, Sensors powered by solar energy with ancient water purification as part of seawater's desalination project. The proposed framework incorporates the new-age technologies, which are essential for efficient and effective operations of desalination systems. The implemented desalination dual membrane framework

uses solar energy for purifying saline water using ancient methods to produce clean water for drinking and irrigation. The desalination produced 0.47 m3/l of freshwater from a saline concentration of 10 g/l, consuming 8.31 KWh/m3 energy for production from the prototype implementation, which makes desalination process cost effective.

TITLE: ‘‘CGP: Cluster-based gossip protocol for dynamic resource environment in cloud,’

ABSTRACT: Since the recent past, cloud computing is developing as a solution to expansive calculation and information storage issues in the form of services. It gives a stage to ask for computational assets with "on interest payments per use arrangement". It thus opens ways to getting to boundless assets with negligible equipment and programming at the customers' end. This paper goes for the advancement of a cloud administration's provisioning structure by building up a dynamic load-balancer for the cloud. In this article, a framework and protocol for the resource environment in the cloud have proposed. Distributed Hash Table (DHT) protocol has been utilized for a service query to perform a job agreed by the user. For load balancing, gossip protocol has been used for inter/intra-cluster gossip. For inter-cluster gossip, the load is balanced among the leaders of every cluster. The proposed protocol uses the inter-cloud resource management, where a leader is selected from the cloud that interacts to other cloud and decides on virtual machine (VM) migration. The decision about job allocation is not acknowledged by a single machine, which generates the scalable architecture of the proposed protocol. The protocol considers the current load situation and decides at the time of request submission. This protocol is adaptable, reliable and scalable and supports green computing by utilizing server solidification.

TITLE: ‘Dynamic group-oriented provable data possession in the cloud,’’

ABSTRACT: As an important security property of cloud storage, data integrity has not been sufficiently studied under the multi-writer model, where a group of users work on shared files collaboratively and any group member can update the data by modification, insertion, and deletion operations. Existing works under such multi-writer model would bring large storage cost to the third-party verifiers. Furthermore, to the best of our knowledge, none of the existing works

for shared files supports fully dynamic operations, which implies that users cannot freely perform the update operations. In this paper, we propose the first public auditing scheme for shared data that supports fully dynamic operations and achieves constant storage cost for the verifiers. Our scheme, named PRAYS, is boosted by a new paradigm for remote data integrity checking. To implement the new paradigm, we proposed a specially designed authenticated structure, called blockless Merkle tree, and a novel cryptographic primitive, called permission-based signature. Extensive evaluation demonstrates that PRAYS is as efficient as the existing less-functional solutions. We believe that PRAYS is an important step towards designing practical multi-writer cloud storage systems.

TITLE: ‘‘A DE-ANN inspired skin cancer detection approach using fuzzy C-means clustering,’

ABSTRACT: As per recent developments in medical science, the skin cancer is considered as one of the common type disease in human body. Although the presence of melanoma is viewed as a form of cancer, it is challenging to predict it. If melanoma or other skin diseases are identified in the early stages, prognosis can then be successfully achieved to cure them. For this, medical imaging science plays an essential role in detecting such types of skin lesions quickly and accurately. The application of our approaches is to improve skin cancer detection accuracy in medical imaging and further, can be automated using electronic devices such as mobile phones etc. In the proposed paper, an improved strategy to detect three type of skin cancers in early stages are suggested. The considered input is a skin lesion image which by using the proposed method, the system would classify it into cancerous or non-cancerous type of skin. The image segmentation is implemented using fuzzy C-means clustering to separate homogeneous image regions. The preprocessing is done using different filters to enhance the image attributes while the other features are assessed by implementing rgb color-space, Local Binary Pattern (LBP) and GLCM methods altogether. Further, for classification, artificial neural network (ANN) is trained using differential evolution (DE) algorithm. Various features are accurately estimated to achieve better results

using skin cancer image datasets namely HAM10000 and PH2. The novelty of the work suggests that DE-ANN is best compared among other traditional classifiers in terms of detection accuracy as discussed in result section of this paper. The simulated result shows that the proposed technique effectually detects skin cancer and produces an accuracy of 97.4%. The results are highly accurate compare to other traditional approaches in the same domain.

TITLE: ‘‘Efficient certificateless multi-copy integrity auditing scheme supporting data dynamics,’’

ABSTRACT: To improve data availability and durability, cloud users would like to store multiple copies of their original files at servers. The multi-copy auditing technique is proposed to provide users with the assurance that multiple copies are actually stored in the cloud. However, most multi-replica solutions rely on Public Key Infrastructure (PKI), which entails massive overhead of certificate computation and management. In this article, we propose an efficient multi-copy dynamic integrity auditing scheme by employing certificateless signatures (named MDSS), which gets rid of expensive certificate management overhead and avoids the key escrow problem in identity-based signatures. Specifically, we improve the classic Merkle Hash Tree (MHT) to achieve batch updates for multi-copy storage, which allows the communication overhead incurred for dynamics to be independent of the replica number. To meet the flexible storage requirement, we propose a variable replica number storage strategy, allowing users to determine the replica number for each block. Based on the fact that auditors may frame Cloud Storage Servers (CSSs), we use signature verification to prevent malicious auditors from framing honest CSSs. Finally, security analysis proves that our proposal is secure in the random oracle model. Analysis and simulation results show that our proposal is more efficient than current state-of-the-art schemes.

TITLE: ‘‘A bio-inspired privacy-preserving framework for healthcare systems,’’

ABSTRACT: Wireless computing has revolutionized our life with the technological advancement from the traditional networking into a new epoch for communication in ad hoc

decorum. An energy efficient network of sensors based on wireless communication and networking principles can enhance the effectiveness of computing during unpredictable circumstances. If a computable required resource is readily available within the reachable region and it is identified to be idle and it is ready to share the corresponding information from its end without affecting the normal behavior of the device or the node, then there exists an opportunity to utilize those resources for computing. Opportunistic computing has a great potential of growth in the field of wireless ad hoc network computing. In traditional network computing technology, mobile computing, grid computing, distributed computing, ubiquitous computing and cloud computing, formerly ensues the communication with minimal resources currently available at the terminal point. This paper proposes a novel framework for an effective utilization of sharable resources, which are available within the reachable region, by creating an opportunity to frame an opportunistic computing while preserving the user's privacy. The proposed framework adopts a bio-inspired technique for identifying and collecting resources information, and thereby recognizes which resource is ready to participate in the opportunistic computing. Experimental results of a system that implements the bio-inspired technique along with the natural behavior of the bee colony approach was analyzed and found that the proposed system shows comparatively high performance in terms of computation resource searching, identifying, emergency data transfer, and participative node privacy preserving.

TITLE: ''Audit cloud: Ensuring data integrity for mobile devices in cloud storage,''

ABSTRACT: One of the promising field sectors of service provision turns out to be Cloud Computing. It involves storing the user's data to be able to use the applications and services that the cloud introduces. One of these risks that can attack the cloud computing is the integrity of the data stored in the cloud. Data Integrity Verification is one of the massive responsibilities of cloud data to reduce the participation in activities which manipulates the data of cloud users and providers. There are many ways to address this problem. Using Encryption and Decryption process for the data can solve the

problem but it requires huge computing time and functional overheads. Applying data auditing can solve this problem. The main approach of this system is variant Paillier Homomorphic Cryptography (PHC) system with Homomorphic tag and combinatorial batch codes. Data Auditing consists of Provable Data Possession (PDP) and Proof of Retrievability (POR) techniques but these techniques have the limitations of queries. The Integrity Verification using the Third Party Auditor in the Proposed Scheme states the solution for the manipulation of data. The experimental results show the effectiveness and efficiency of the proposed system.

TITLE: ''A lightweight identity-based remote data auditing scheme for cloud storage,'

ABSTRACT: Cloud storage enables data owners to use any device to store and access data anytime, anywhere. In a data auditing scheme, the data owner can entrust a third party auditor (TPA) to verify that the outsourced data remains unchanged. A secure data auditing scheme not only detects whether cloud service providers (CSP) maintain data integrity, but also prevents TPA from stealing data. In this paper, a new identity-based data auditing (IBDA) scheme for cloud storage systems is proposed. In the scheme, the data owner generates the tags using its private key and data blocks, and then uploads the data blocks along with the tags to CSP. In the challenge-proof phase, before returning the proof information, CSP performs the addition operation between the hash function value and the data block to hide the data, thereby preventing TPA from stealing the data. This scheme is proved to be secure in the random oracle model. Analysis of efficiency shows that it is more efficient than other schemes.

TITLE: Identity-based public multi replica provable data possession,''

ABSTRACT: Cloud storage has been gaining tremendous popularity, which provides facilitative data storage and sharing services for distributed clients. To maximize the availability and reliability, some customers may store multiple replicas of critical data on cloud servers. However, cloud servers may collude to make it look like they are storing multiple copies of data, whereas in fact they only store a single copy. Currently, several multi-replica provable data possession schemes have

been proposed to provide verifications to ensure that all the outsourced copies are actually stored and maintained intact. For these schemes with third-party verifications, correctly choosing public keys of data owners relies on the public key infrastructure (PKI), which is complicated and resource consuming. In this paper, we propose a novel identity-based public multireplica provable data possession scheme (IDPMR-PDP) to provide third-party verification of outsourced data with multiple replicas without PKI. We also introduce a formal security model of identity-based public multi-replica PDP schemes and prove that the IDPMR-PDP is secure against malicious cloud servers and privacy-preserving against curious verifiers under this model. Meanwhile, our analyses and simulation results demonstrate that the IDPMR-PDP realizes efficient integrity verification

MODULES

There are 4 modules:

1. TPA
2. PKG
3. User
4. Cloud

TPA:-

- Login
- T-RBT Details
- Audit Request
- Download Request
- Logout

User:-

- Register
- Login
- Upload Files
- My Files
- My Profile
- Audit Files
- Logout

Cloud:-

- Login
- C-RBT Details
- Audit Challange
- Logout

PKG:-

- Login
- User Details
- User Request
- Logout

PROPOSED SYSTEM

A. DYNAMIC STORAGE STRUCTURE RED-BLACK TREE

In order to establish a more complete cloud storage service system, we use the red-black tree data structure for data storage. Compared with the balanced

binary tree, although the red-black tree algorithm has the same time complexity, its statistical performance is higher. For dynamic data update, the traditional tree storage structure requires a lot of queries and adjustment operations in the worst case. If the data is stored in the data structure of the red-black tree, because it is not strictly balanced, its query ability is slightly weaker, but its insertion and deletion capabilities are completely stronger than the balanced binary tree. In our scheme, each copy corresponds to a red-black tree with a complete node and is stored in the CSP, and the data block copy in each copy corresponds to a node value, which is stored in the TPA. According to the node value of the binary tree, the location of the data block can be verified, which greatly reduces the verification path and improves the system efficiency. Here, the red-black tree stored in the CSP is abbreviated as C-RBTree, and the red-black tree stored in the TPA is abbreviated as T-RBTree.

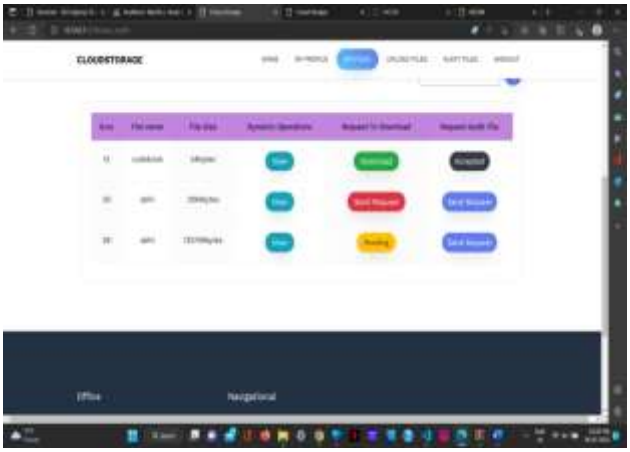
B. CONSTRUCTION OF OUR PROPOSAL

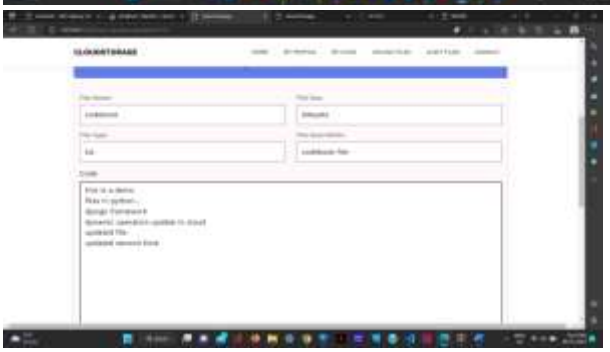
In the program, the review process is divided into two phases: the setup phase and the verification phase. The previous phase is some preparations, including: KeyGen, ReplicaGen and TagGen. The system setting is mainly for the user. The user generates a public key and a private key pair through the KeyGen algorithm, and then performs other pre-processing tasks through ReplicaGen and TagGen. The latter phase includes three algorithms: ChalGen, ProofGen and VerifyProof. At this stage, users, CSP, and TPA will participate to perform data verification. In the ChalGen algorithm, the TPA sends verification challenge information to the CSP, and then the CSP responds in the ProofGen algorithm to prove the integrity of the stored data. In the final Verify Proof algorithm, TPA audits the proof and sends the audit results to the user by TPA.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362

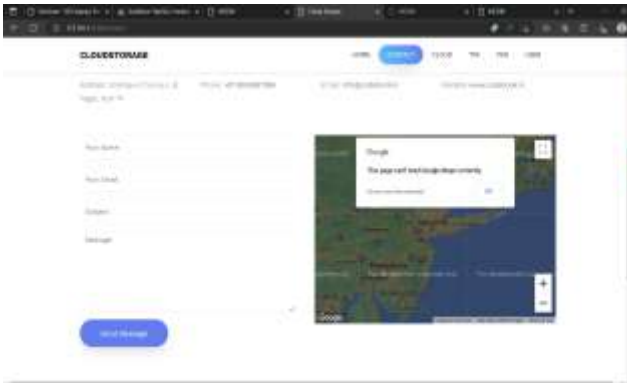
C. DYNAMIC OPERATION VERIFICATION

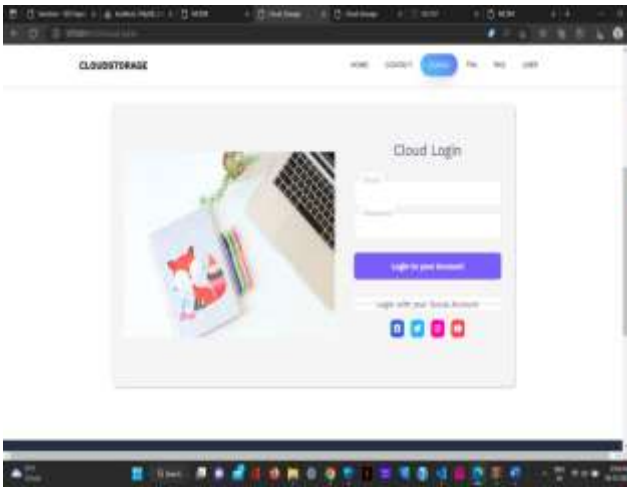
For each data change operation, the user will send a request to the CSP to run the dynamic operation. After receiving the request, the CSP will dynamically update the data. According to the user's request, it will implement operations such as modification, insertion, and deletion.

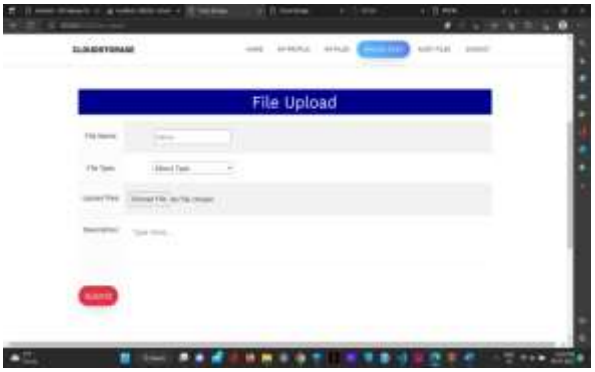




Results







CONCLUSION

This paper proposes an effective multiple copies data integrity verification scheme based on red-black tree in cloud storage. It supports dynamic operations on multiple copies, which can improve efficiency. In terms of data storage, the red-black tree data

structure storage is adopted to effectively improve data storage efficiency and simplify data update operations. The theoretical analysis of our scheme also proves the security of the scheme. The experimental results also show that our scheme is superior to other comparative schemes in terms of computational cost, storage cost, and communication cost. The experimental analysis demonstrate that our scheme achieves desirable security and efficiency.

REFERENCES

[1] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, ‘‘Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium,’’ J. Netw. Comput. Appl., vol. 82, pp. 56–64, Mar. 2017.

[2] M. Alshehri, A. Bhardwaj, M. Kumar, S. Mishra, and J. Gyani, ‘‘Cloud and IoT based smart architecture for desalination water treatment,’’ Environ. Res., vol. 195, Apr. 2021, Art. no. 110812, doi: 10.1016/ j.envres.2021.110812.

[3] S. Srivastava, S. Saxena, R. Buyya, M. Kumar, A. Shankar, and B. Bhushan, ‘‘CGP: Cluster-based gossip protocol for dynamic resource environment in cloud,’’ Simul. Model. Pract. Theory, vol. 108, Apr. 2021, Art. no. 102275, doi: 10.1016/j.simpat.2021.102275.

[4] K. He, J. Chen, Q. Yuan, S. Ji, D. He, and R. Du, ‘‘Dynamic group-oriented provable data possession in the cloud,’’ IEEE Trans. Dependable Secure Comput., early access, Jul. 2, 2019, doi: 10.1109/TDSC.2019.2925800.

5] M. Kumar, M. Alshehri, R. AlGhamdi, P. Sharma, and V. Deep, ‘‘A DE-ANN inspired skin cancer detection approach using fuzzy C-means clustering,’’ Mobile Netw. Appl., vol. 25, no. 4, pp. 1319–1329, Aug. 2020, doi: 10.1007/s11036-020-01550-2.

[6] L. Zhou, A. Fu, G. Yang, H. Wang, and Y. Zhang, ‘‘Efficient certificateless multi-copy integrity auditing scheme supporting data dynamics,’’ IEEE Trans. Dependable Secure Comput., early access, Aug. 4, 2020, doi: 10. 1109/TDSC.2020.3013927.

[7] C. Dhasarathan, M. Kumar, A. K. Srivastava, F. Al-Turjman, A. Shankar, and M. Kumar, ‘‘A bio-inspired privacy-preserving framework for healthcare systems,’’ J. Supercomput., early access, Mar. 19, 2021, doi: 10.1007/ s11227-021-03720-9.

[8] L. Krithikashree and S. Manisha, ‘‘Audit cloud: Ensuring data integrity for mobile devices in cloud storage,’’

IEEE Trans. Depend. Sec. Comput., pp. 1–5, Sep. 2018, doi: 10.1109/ICCCNT.2018.8493963.

[9] L. Deng, B. Yang, and X. Wang, ‘‘A lightweight identity-based remote data auditing scheme for cloud storage,’’ IEEE Access, vol. 8, pp. 206396–206405, 2020, doi: 10.1109/ACCESS.2020.3037696.

[10] S. Peng, F. Zhou, Q. Wang, Z. Xu, and J. Xu, ‘‘Identity-based public multireplica provable data possession,’’ IEEE Access, vol. 5, pp. 26990–27001, 2017, doi: 10.1109/ACCESS.2017.2776275.

[11] A. Bhardwaj, S. B. H. Shah, A. Shankar, M. Alazab, M. Kumar, and T. R. Gadekallu, ‘‘Penetration testing framework for smart contract blockchain,’’ Peer-Peer Netw. Appl., early access, Sep. 5, 2020, doi: 10. 1007/s12083-020-00991-6.

[12] P. Shen, C. Li, and Z. Zhang, ‘‘Research on integrity check method of cloud storage multi-copy data based on multi-agent,’’ IEEE Transl. Content Mining, vol. 4, no. 8, pp. 17170–17178, 2020, doi: 10.1109/ACCESS. 2020.2966803.

[13] Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, ‘‘Efficient integrity auditing for shared data in the cloud with secure user revocation,’’ in Proc. IEEE Trustcom/BigDataSE/ISPA, Aug. 2015, pp. 434–442, doi: 10.1109/ Trustcom.2015.404.

[14] R. Rabaninejad, S. M. Sedaghat, M. Ahmadian Attari, and M. R. Aref, ‘‘An ID-based privacy-preserving integrity verification of shared data over untrusted cloud,’’ in Proc. 25th Int. Comput. Conf., Comput. Soc. Iran (CSICC), Jan. 2020, pp. 1–6, doi: 10.1109/CSICC49403.2020.9050098.