2022 IEEE 8th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)

Overview of Blockchain and Cloud Service Integration

Feng Yang
School of Computer Science and Engineering
Network Informatic Center
Hunan University of Science and Technology
Xiangtan, China
15162663@qq.com

Liao Lei
Hunan Vocational College of Art
Changsha, China
3267137770@qq.com

Hangyu Zhu
School of Computer Science and Engineering
Hunan University of Science and Technology
Xiangtan, China
zhy2770848109@163.com

***Abstract*—Blockchain has unlimited possibilities to break through many application areas. Cloud service is an on-demand service paradigm that facilitates the availability of shared resources for data storage and computing. Last several years, the combination of blockchain and cloud services has attracted much attention to ensure efficiency, openness, safety and even provide better cloud services in the form of novel service models. In order to develop the all potential of blockchain and cloud integration, it is significance that have a clear comprehension of current work in this area. None of the current overviews covers blockchain cloud integration from a service-oriented perspective. This article aims to outline the service orientation of blockchain integration to fill this vacancy. This overview explores different service models that integrate blockchain. For each service model, the existing work is summarized and comparatively analyzed, and a clear and concise view is provided in each sort.**

Keywords—Blockchain, Cloud Computing, Cloud Service Model, Blockchain as a Service, Cloud Supporting Blockchain

I. INTRODUCTION

Cloud computing has become a technology for everyday use. It uses a pay-as-you-go approach to provide on-demand services. It provides fast and elastic uninterrupted network access and resource pool [1]. Cloud computing minimizes costs at an eye-catching speed and solves traditional resource management problems. Besides, it still has some deficiency, such as shared base installation issues, virtualization issues, API security, secrecy, and legal issues based on *Service Level Agreement* (SLA) [2]. Researchers are trying many different techniques to solve these problems, and blockchain technology has become one of the most commonly used in this area.

Blockchain is considered to be a fundamental technology and its emergence may bring great changes to many other application fields, including cloud computing. It provides a secure encryption method for distributed systems to store data [3], and ensures a secure transaction mechanism without involving any intermediate entities. In conclusion, this technology provides a better way of complementing many existing service platforms. Therefore, researchers are vigorously exploring how to combine blockchain and cloud computing to deal with some technical difficulties in cloud services.

To take full advantage of this approach to cloud-blockchain integration, it is critical to have a clear understanding of the impact of blockchain on the needs of various aspects of the cloud. There have been some reviews in this regard [4-6]. In particular, the comments in [6] are worth noting because the author has conducted a comprehensive and detailed survey of the different technical requirements for cloud-blockchain integration. Although most service delivery mechanisms in the cloud rely on service models, service-oriented research on blockchain-cloud integration is still scarce. The goal of this paper is to fill this gap. The goal of this article is to fill this gap.

This paper reviews some work on the intersection of blockchain and cloud, focusing on the integrated service model of blockchain following a service-oriented taxonomy. For the research in these different fields, the researchers have reviewed and comparatively analyzed the existing work to find out their advantages and limitations for further research and improvement.

The structure of the rest of this article is as follows: In Section 2, the background of cloud computing and blockchain is briefly introduced. The third section introduces the service-oriented taxonomy. Sections 4 and 5 provide an overview of each service category. Finally, the conclusion is drawn in the ninth section.

II. BACKGROUND

Cloud computing: Cloud service providers (CSPs) provide cloud data storage, virtualization, network components, and other services as third parties [1]. It mainly includes three basic service types: *Infrastructure as a Service* (IaaS), *Platform as a Service* (PAAS) and Software as a Service (SaaS). Due to the continuous improvement of existing technologies, other service models such as Blockchain as-a-service and Security-as-a-service are constantly emerging. When building a cloud computing architecture, some useful requirements should be considered [7-10]. For example, the security of user data, the applicability of services, the interoperability of technologies, and the high performance of application services are all important factors to consider [11-13].

Blockchain: The data sharing of blockchain technology is a distributed fault-tolerant database. No entity can conduct transactions without a third party, and the transaction data is recorded in the distributed ledger [3]. Each node in the blockchain stores complete data according to the chain structure, and the data stored by each node is independent, relying on the consensus mechanism to ensure the consistency of data storage. Each block can encode assets and data transfers, which are then broadcast to the network, verified by special nodes and added to the existing chain or discarded

978-1-6654-8069-7/22/$31.00 ©2022 IEEE
DOI 10.1109/BigDataSecurityHPSCIDS54978.2022.00017

based on verification results [14]. The blockchain originated from Bitcoin [15], and with the development of Bitcoin, blockchain technology has attracted more and more attention. Bitcoin is not issued by a specific currency institution, but is calculated by a specific algorithm through a series of a large number of algorithms. After the Bitcoin transaction is completed, it is packaged into the block for storage [16-17]. After it is confirmed in the blockchain, the transaction is also confirmed, and each transaction is stored in the blockchain. The blockchain is slowly developing into a programmable interactive environment for building distributed and reliable applications [18].

III. Service Oriented Taxonomy

This article focuses on the integration of blockchain and cloud platform. In order to review these studies, this article created a taxonomy developed from the perspective of "as a service", called a service-oriented taxonomy. From this perspective, all research (blockchain-cloud integration) within the scope of this article is classified into four service models, as shown in Figure 1. The first group is called security as a service [19-21]. The first group is called Security as a Service, and this paper explores some blockchain-based work aimed at improving existing security services within cloud platforms.

The second group is called blockchain as a service, which provides a series of operational services such as blockchain-based search queries, transaction submissions, and data analysis. The third group is a special service model called federation as a service. Formation and management of blockchain-enabled identity federations in multiple complex cloud environments is demonstrated after extensive research work. The last group, called Management as a Service, focuses on the complete development and deployment of cloud infrastructure, with resources that enable organizations to deliver everything from simple cloud-based applications to complex cloud-enabled enterprise applications. For each category, this article outlines and compares the main influential works under different standards in order to visually compare their differences and advantages and disadvantages.

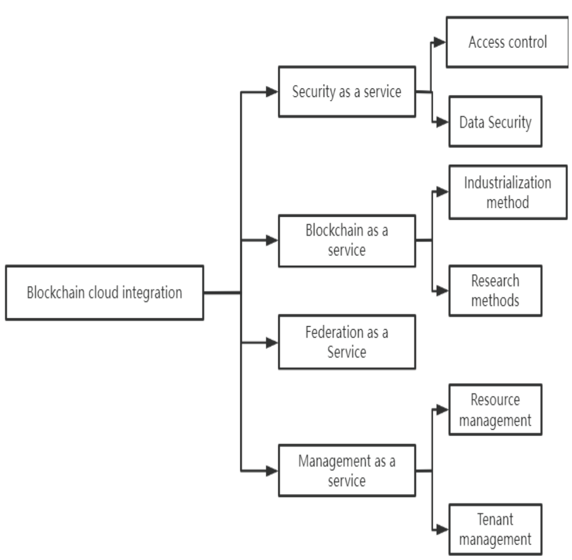

Fig. 1. The taxonomy of blockchain-cloud integration

IV. Security as a Service

The security-as-a-service model allows to provide different security services for cloud platforms [22]. This chapter mainly studies and analyzes two different types of blockchain-based cloud security services, that is, access control and data security.

A. Access control

Access control is a technology [23-25] that almost all systems need to use. It stipulates that the user's access to certain information items or the use of certain control functions is restricted according to the user's identity and a certain definition to which it belongs. a technology. The blockchain-based cloud access control model aims to address two major challenges:

• In the traditional encryption-based access control model, a trusted central server stores access policies for management and licensing obligations and generates, manages, and distributes keys that define access rights for subjects and objects, even the owner itself also have no right to modify it.

• Use flexible access control mechanisms to securely share data/resources in the cloud.

Paper [26] proposes a blockchain-based decentralized data storage and sharing framework, which combines file system, Ethereum and attribute-based ABE encryption mechanism. Data owners can encrypt shared data, enabling fine-grained access control to data. Their solution uses a multi-attribute value and wildcard AND gate access strategy to filter unauthorized search requests, and allows data owners to use a *Public Generator Key* (PKG) to secretly share data in the cloud. Similarly, the author in [27] proposed a new secure cloud storage framework with access control that combines the Ethereum blockchain with the CP-ABE encryption mechanism based on the ciphertext policy property. This solution enables data owners to assign attribute sets to resources and define access policies with expiration dates by creating and deploying smart contracts that execute strategies.

Paper [28] The proposed scheme can use Ethereum to define and implement dynamic access strategies in the cloud platform. This scheme uses the encryption feature based on the ciphertext policy attribute with dynamic attributes, and uses the decentralized ledger of the blockchain to generate a secure immutable log, but to ensure the privacy of the secret key or private key. Paper [29] proposed a blockchain-based access control framework with privacy protection, and designed the authentication and authorization revocation process with the blockchain account address as the ID. It not only prevents hackers and administrators from illegally accessing resources, but also protects authorized privacy.

Table 1 records the summary of the evaluation of this part of the work outlined in this article. In Table I, the symbols '●' and '○' are respectively used to indicate whether the fine-grained attribute is satisfied. In addition to the content listed in the table, all these works utilize public blockchain platforms such as Ethereum and EOS. Although the public blockchain platform provides better security than any private platform, there are still costs associated with storing data and smart contract execution [30]. In addition, most public blockchain systems are inherently slow and may have some scalability issues. In addition, public blockchains have great privacy security issues, so these works need to address privacy issues separately.

B. Data Security

Various solutions are designed to ensure the confidentiality, privacy, integrity and source of data using blockchain in the cloud environment [31-33].

Confidentiality and privacy of data [34-37]: In order to maintain the confidentiality and privacy of data, a certain pre-processing format or any encryption method must be used before data is stored in the cloud [38-40]. This increases the complexity when retrieving encrypted data. In fact, the user must download all the data, decrypt them, and then use the query to retrieve the required part, which requires extra time and expensive calculations to process big data [41]. In recent years, SSE (*Secure Searchable Encryption*) schemes have emerged, in which user data is encrypted using a private key and stored in a masked index table along with key pairs of encrypted messages. Both the index table and the preprocessed data are stored on the server. When searching or querying, the search token is generated directly from the client, and the encrypted data is filtered out from the server using the mask index table without decryption.

TABLE I. COMPARISON OF ACCESS CONTROL MECHANISMS IN BLOCKCHAIN-CLOUD INTEGRATION

Literature	Technology	platform	method	fine-grained	advantage	shortcoming
[12]	DAC, ABAC	Ethereum	MIRACL (ABE-80)	●	feasible, internally operable	No attribute revocation
[13]	ABAC	Ethereum	CPABE	●	No central key distributor	lack of integration
[14]	ABAC	Ethereum	ABE	○	Dynamic Access Policy	Cannot process resource with multiple owners
[15]	ID based	EOS	AES &Asymmetric	○	Authorization revocation	complex to implement

In response to the above motivation, [41] proposed a "SSEusing-BC" scheme that resists malicious attacks on data stored on public chains and accelerates the use of data, whose encrypted data is stored in a decentralized blockchain that supports data confidentiality and search efficiency in storage, the data owner can upload encrypted files and their corresponding indexes to the cloud, which is applicable to a wide range of retrieval methods.

Paper [42] proposed a cryptographic decentralized storage architecture that can support trusted and private keyword searches, considering the use of a *Trusted Third Party* (TTP) secure and fair payment service. The solution is compatible with ether and bitcoin, enabling the client to perform file addition on the target storage node through verifiable keyword search. Paper [43] first proposed a single sign-on scheme with both client-side and server-side verifiability, supporting cost minimization and fairness judgment. The scheme's trusted keyword search on encrypted data, without the need for a trusted third party, enables data owners to resist malicious cloud servers. By publicly verifying the digital signature, server-side verifiability is realized.

Paper [44] introduced BPay, a blockchain-based outsourcing service framework in the cloud, which solves the payment fairness problem for malicious users or service providers, achieves robustness and robustness fairness, and is comparable to Bitcoin and Ethereum Square compatible.

In paper [45], Hu et al. used Ethereum smart contracts to replace the central server, and constructed an efficient data privacy protection search scheme, where data owners can confidently receive correct search results and protect data security. The ensemble search algorithms in smart contracts mainly focus on two issues: the correctness of search results and computational overhead. On the basis of literature [20], Chen et al. [46] focused on data access control in medical data records, and constructed a blockchain-based single sign-on searchable encryption scheme through complex logical expressions. This scheme can provide fair payment services for multi-user settings.

A summary of the research work based on SSE supported by the blockchain is shown in Table Ⅱ. ('-' means not applicable). According to the table, only [42] used TTP, all of which are based on public blockchain platforms (mainly Ethereum). In addition, when applicable, the client-side authentication problem has been solved, and only server-side authentication is considered in the TKSE scheme.

Data integrity: Data integrity is the maintenance and assurance of the accuracy and reliability of data [47-50], and Data provenance typically describes the chronology of the object's custody by recording its creation to modification and deletion, and then stores this information in a verifiable audit trail. Leveraging the immutability and transparency of blockchain to record activities associated with data objects is the core idea of combining blockchain with these two approaches.

TABLE II. COMPARISON OF BLOCKCHAIN-BASED SINGLE SIGN-ON MECHANISMS IN THE CLOUD

Literature	client authentication	Server-side validation	Third Party (TTP)	Updatability	Platform
[16]	●	○	○	○	Bitcoin
[17]	●	○	●	●	Ethereum

[18]	●	●	○	○	Ethereum And Bitcoin
[19]	●	○	○	○	Ethereum and Bitcoin
[20]	-	-	○	●	Ethereum
[21]	-	-	○	●	Ethereum

Provchain of [51] provides a solution for the collection, storage and verification of source data, which achieves data transparency and enhances the privacy and availability of source data. The BlockCloud architecture [52] is similar to Provchain, but the difference is that the framework provides provenance data verification, which is bound to blockchain transactions, preventing attackers from maliciously tampering with data.

M. Qiu et al. proposed a new evaluation framework called Deepsweep for mitigating DNN backdoor attacks using data augmentation [53]. Paper [54] proposed a provenance database of data through a cloud computing platform, which reduces the computational overhead and realizes data integrity checking. Zhang et al. [55] proposed a process origin mechanism that utilizes blockchain and group signatures to provide proof of existence and privacy protection for process records.

Paper [56] proposed a two-layer blockchain in the cloud. Among them, the first layer is a blockchain based on mining rotation to improve the high latency and weak stability of processing data, while the second layer is blockchain research based on POW mechanism to ensure data integrity. Paper [57] proposed a *Certificateless Public Verification Scheme* (CPVPA), which requires the transaction of each verification result to be recorded in the blockchain without auditor verification and without certificate management issues. Table III presents a comparative summary of the works outlined under this category.

TABLE III. COMPARISON OF CLOUD DATA TRACEABILITY MECHANISMS BASED ON BLOCKCHAIN

Literature	Extensibility	customizability	Interoperability	Access control	surroundings	platform	monitoring tool
[22]	●	●	○	●	Google drive	Ethereum	Event listener module
[23]	●	●	○	●	OwnCloud	bitcoin	Hooks API
[24]	●	●	○	●	OwnCloud	PoS blockchain	Hooks and listeners
[25]	●	○	●	●	Federated cloud	-	Hooks and listeners
[26]	○	○	●	○	Cloud forensic	-	User
[27]	●	○	●	●	Distributed DB	-	Database
[28]	○	●	○	●	Public cloud	-	Auditor

V. Blockchain as a Service Area

Blockchain-as-a-Service (BAAS) allows consumers to develop, use and maintain blockchain applications using cloud-based services; acting as a bridge between companies and platforms, BAAS brings simpler and more secure technology to some organizations, so the more and more industries are beginning to adopt this service [58-60]. Researchers are starting to improve research in this area.

A. Industrialization method

In recent years, technology giants across the country have begun to provide BAAS services in their internal platforms, and Microsoft was considered a pioneer in this field when it introduced EBaaS; IBM provides a public cloud service on which customers can develop more advanced services. A secure blockchain network; Amazon AWS also released Hyperledger Fabric to make it easier for developers to create environments; Hewlett-Packard also introduced a distributed ledger with Corda-backed BAAS.

B. Research methods

A serverless architecture of FBaas [61] is proposed, which provides running speed and more concise logic level. FSBaaS provides transparency in the deployment of blockchain services in cloud computing networks [62-64] and seeks a more detailed evaluation method. NutbaaS [65] proposes some more advanced technical services for the shortcomings of Baas, such as identity chain technology and smart contract security vulnerability detection. uBaas [6] includes Deployment and Services, Design-as-a-Service, and Ancillary Services to avoid lock-in to a specific cloud platform and address issues such as scalability and security. Most of these frameworks are similar, but are improving step by step.

VI. Conclusion

This article introduced the use of service-oriented taxonomy and reviews some of the influential research results in the field of blockchain and cloud service integration. Below are some of the conclusions that emerged in conducting this survey. Research in blockchain cloud service integration focuses on the use of blockchain to mitigate or improve one or more security issues. Due to the immutability or integrity of the blockchain, there are many security advantages in the form of no single point of failure. Blockchain platform: the privacy and limited scalability problems that exist on the blockchain public chain, and the calculation and data storage of such platforms will incur huge costs. Nonetheless, it is surprising that most deployments utilize public blockchain platforms. It may be that there is no stable private blockchain platform like Hyperledger Fabric in previous years, so researchers can only use public blockchain platforms for research experiments. However, as more and more private blockchain platforms appear on the market, this aspect is expected to change in the future.

REFERENCES

[1] Judith Hurwitz, Daniel Kirsch. "Cloud computing for dummies," John Wiley & Sons, 2020.

[2] Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb. "A taxonomy and survey of cloud computing systems," 2009 Fifth International Joint Conference on INC, IMS and IDC. IEEE, 44–51, 2009.

[3] Daniel Drescher. "Blockchain basics," Apress, Berkeley, CA, 276, 2017.

[4] Fei Han, Jing Qin, Jiankun Hu. "Secure searches in the cloud: A survey," Future Generation Computer Systems, 62: 66-75, 2016.

[5] Jin Ho Park and Jong Hyuk Park. "Blockchain security in cloud computing: Use cases, challenges, and solutions," Symmetry, 9(8): 164, 2017.

[6] Keke Gai, Jinnan Guo, Liehuang Zhu, Shui Yu. "Blockchain meets cloud computing:A survey," IEEE Communications Surveys & Tutorials, 2009–2030, 2020.

[7] Z. Lu, N. Wang, et al. "IoTDeM: An IoT Big Data-oriented MapReduce performance prediction extended model in multiple edge clouds," Journal of Parallel and Distributed Com., 118, 316-327, 2018.

[8] G. Wu, H. Zhang, et al. "A decentralized approach for mining event correlations in distributed system monitoring," JPDC, 73(3): 330-340, 2013.

[9] L. Qiu, K. Gai, M. Qiu. "Optimal big data sharing approach for tele-health in cloud computing," IEEE SmartCloud, 184-189, 2016.

[10] J. Wang, M. Qiu, B. Guo. "Enabling real-time information service on telehealth system over cloud-based big data platform," Journal of Systems Architecture 72, 69-79,2017.

[11] K. Gai, Z. Du, M. et al. "Efficiency-aware workload optimizations of heterogeneous cloud computing for capacity planning in financial industry," IEEE 2nd CSCloud, 2015.

[12] M. Qiu, W. Dai, A. Vasilakos. "Loop parallelism maximization for multimedia data processing in mobile vehicular clouds," IEEE Transactions on Cloud Computing, 7(1): 250-258, 2019.

[13] J. Wang, M. Qiu, B. Guo, Z. Zong, "Phase-reconfigurable shuffle optimization for Hadoop MapReduce," IEEE Trans. on Cloud Computing 8 (2), 418-431, 2020

[14] Imran Bashir. "Mastering blockchain," Packt Publishing Ltd, 2017.

[15] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[16] W. Pan, M. Qiu. "Application of blockchain in asset-backed securitization," IEEE 6th Conf. BigDataSecurity, 2020.

[17] M. Qiu, H. Qiu. "Review on image processing based adversarial example defenses in computer vision," IEEE 6th Conf. BigDataSecurity, 2020.

[18] Florian Tschorsch, Björn Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, 18(3): 2084–2123, 2016.

[19] M. Qiu, K. Gai, Z. Xiong. "Privacy-preserving wireless communications using bipartite matching in social big data," FGCS, 87, 772-781,2018.

[20] Wei Liang, Yin Huang, Jianbo Xu and Songyou Xie. "A distributed data secure transmission scheme in wireless sensor network," International Journal of Distributed Sensor Networks, 2017.

[21] H. Qiu, M. Qiu, Z. Lu. "Selective encryption on ECG data in body sensor network based on supervised machine learning," Information Fusion, 55: 59-67, 2020.

[22] Vijay Varadharajan, Udaya Tupakula. "Security as a service model for cloud environment," IEEE Transactions on network and Service management, 11(1): 60–75, 2014.

[23] Z. Shao, C. Xue, Q. Zhuge, et al. "Security protection and checking for embedded system integration against buffer overflow attacks via hardware/software," IEEE Transactions on Computers, 55(4): 443-453, 2006.

[24] M. Qiu, L. Zhang, Z. Ming, et al. "Security-aware optimization for ubiquitous computing systems with SEAT graph approach," J. of Comp. and Sys. Sci., 79(5): 518-529, 2013.

[25] K. Gai, M. Qiu, S. Elnagdy. "A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance," IEEE BigDataSecurity, 2016.

[26] Shangping Wang, Yinglong Zhang, Yaling Zhang. "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE Access, 6: 38437–38450, 2018.

[27] Shangping Wang, Xu Wang, Yaling Zhang. "A secure cloud storage framework with access control based on blockchain," IEEE Access, 7: 112713–112725, 2019.

[28] Ilya Sukhodolskiy, Sergey Zapechnikov. "A blockchain-based access control system for cloud storage," IEEE Conf. of Russian Young Researchers in Electrical and Electronic Eng., 1575–1578, 2018.

[29] C. Yang, L. Tan, N. Shi, et al. "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," IEEE Access, 8: 70604–70615, 2020.

[30] Mohammad Jabed Morshed Chowdhury, MD Sadek Ferdous, Kamanashis Biswas, Niaz Chowdhury, A. S. M. Kayes, Mamoun Alazab, Paul Watters. "A comparative analysis of distributed ledger technology platforms," IEEE Access, 7: 167930–167943, 2019.

[31] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi, M. Qiu. "Adversarial attacks against network intrusion detection in IoT systems," IEEE Internet of Things Journal, 8(13): 10327-10335, 2020.

[32] Xie Songyou, Liang Wei, Xu Jianbo, Tang Mingdong, Weng Tien-Hsiung, Li Kuan-Ching. "A Novel Bidirectional RFID Identity Authentication Protocol," 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovations, 2018.

[33] Y. Li, Y. Song, L. Jia, et al. "Intelligent fault diagnosis by fusing domain adversarial training and maximum mean discrepancy via ensemble learning," IEEE Trans. on Industrial Informatics, 17(4): 2833-2841, 2020.

[34] H. Qiu, M. Qiu, R. Lu. "Secure V2X communication network based on intelligent PKI and edge computing," IEEE Network, 34(2): 172-178, 2019.

[35] Mingdong Tang, Wei Liang, Buqing Cao and Xiangyun Lin. "Predicting Quality of Cloud Services for Selection," International Journal of Grid Distribution Computing, 2015.

[36] Chunyan Diao, Dafang Zhang, Wei Liang, Kuan-Ching Li, Yujie Hong, Jean-Luc Gaudiot. A Novel Spatial-Temporal Multi-Scale Alignment Graph Neural Network Security Model for Vehicles Prediction. IEEE Transactions on Intelligent Transportation Systems, 2021

[37] H. Qiu, M. Qiu, M. Liu, Z. Ming. "Lightweight selective encryption for social data protection based on EBCOT coding," IEEE Trans. on Compu. Social Systems, 7(1):205-214, 2019.

[38] Jing Wang, Wei Luo, Wei Liang, Xiangyang Liu, Xiaodai Dong. "Locally Minimum Storage Regenerating Codes in Distributed Cloud Storage Systems," China Communications, 2017.

[39] K. Gai, M. Qiu, M. Liu, Z. Xiong. "In-memory big data analytics under space constraints using dynamic programming," FGCS, 83: 219-227, 2018.

[40] M. Qiu, Z. Chen, J. Niu, et al. "Data allocation for hybrid memory with genetic algorithm," IEEE Trans. on Emerging Topics in Computing, 3(4): 544-555, 2015.

[41] Huige Li, Fangguo Zhang, Jiejie He, Haibo Tian. "A searchable symmetric encryption scheme using blockchain," arXiv preprint arXiv:1711.01030, 2017.

[42] Chengjun Cai, Xingliang Yuan, Cong Wang. "Towards trustworthy and private keyword search in encrypted decentralized storage," International Conference on Communications, 1–7, 2017.

[43] Yinghui Zhang, Robert Deng, Jiangang Shu, Kan Yang, Dong Zheng. "TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain," IEEE Access, 6: 31077–31087, 2018.

[44] Yinghui Zhang, Robert Deng, Ximeng Liu, Dong Zheng. "Outsourcing service fair payment based on blockchain and its applications in cloud computing," IEEE Transactions on Services Computing, 1152–1166, 2018.

[45] Shengshan Hu, Chengjun Cai, Qian Wang, Cong Wang, Xiangyang Luo, Kui Ren. "Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization," IEEE INFOCOM 2018, 792–800, 2018.

[46] Lanxinag Chen, Wai-Kong Lee, Chin-Chen Chang, Kim-Kwang Raymond Choo, Nan Zhang. "Blockchain based searchable encryption for electronic health record sharing," Future Generation Computer Systems, 95: 420–429, 2019.

[47] F. Hu, S. Lakdawala, et al. "Low-power, intelligent sensor hardware interface for medical data preprocessing," IEEE Trans. on Information Technology in Biomedicine, 13(4): 656-663, 2009.

[48] M. Qiu, L. Chen, Y. Zhu, J. Hu, X. Qin. "Online data allocation for hybrid memories on embedded tele-health systems," IEEE Conf. HPCC, 2014.

[49] X. Wei, H. Guo, et al. "Reliable Data Collection Techniques in Underwater Wireless Sensor Networks: A Survey," IEEE Comm. Surveys & Tutorials, 24(1): 404-431, 2021.

[50] H. Qiu, Q. Zheng, G. Memmi, et al. "Deep residual learning-based enhanced JPEG compression in the Internet of Things," IEEE Trans. on Industrial Informatics, 17(3): 2124-2133, 2020 .

[51] Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, Laurent Njilla. "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," 17th International Symposium on Cluster, Cloud and Grid Computing, 468–477, 2017.

[52] Sachin Shetty, Val Red, Charles Kamhoua, Kevin Kwiat, Laurent Njilla. "Data provenance assurance in the cloud using blockchain," Disruptive Technologies in Sensors and Sensor Systems, 10206, International Society for Optics and Photonics, 102060I, 2017.

[53] M. Qiu, S.Y. Kung, K Gai. "Intelligent security and optimization in Edge/Fog Computing," Future generation computer systems, 107: 1140-1142, 2020.

[54] Deepak Tosh, Sachin Shetty, Xueping Liang, Charles Kamhoua, Laurent L. Njilla. "Data provenance in the cloud: A blockchain-based approach," IEEE Consumer Electronics Magazine, 8(4): 38–44, 2019.

[55] Yong Zhang, Songyang Wu, Bo Jin, Jiaying Du. "A blockchain-based process provenance for cloud forensics," 2017 3rd IEEE International Conference on Computer and Communications, 2470–2473, 2017.

[56] Edoardo Gaetani, Leonaedo Aniello, Roberto Baldoni, Federico Lombardi, Andera Margheri, Vladimiro Sassone. "Blockchain-based database to ensure data integrity in cloud computing environments," Proceedings of the First Italian Conference on Cybersecurity, 2017.

[57] Yuan Zhang, Chunxiang Xu, Xiaodong Lin, Xuemin Shen. "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," IEEE Transactions on Cloud Computing, 2019.

[58] M. Liu, S. Zhang, et al. "H infinite State Estimation for Discrete-Time Chaotic Systems Based on a Unified Model," IEEE Trans. on Systems, Man, and Cybernetics (B), 2012.

[59] M. Qiu, E. Khisamutdinov, et al. "RNA nanotechnology for computer design and in vivo computation," Philosophical Transactions of the Royal Society A, 2013.

[60] Wei Liang, Jing Long, Aijiao Cui, Li Peng. "A New Robust Dual Intellectual Property Watermarking Algorithm Based on Field Programmable Gate Array," Journal of Computational and Theoretical Nanoscience, 2016.

[61] Huan Chen, Liang-Jie Zhang. "Fbaas: Functional blockchain as a service," International Conference on Blockchain. Springer, 243–250, 2018.

[62] H. Qiu, H. Noura, et al. "A User-Centric Data Protection Method for Cloud Storage Based on Invertible DWT," IEEE Trans. Cloud Comput. 9(4): 1293-1304, 2021.

[63] K. Gai, M. Qiu, H. Zhao. "Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing," IEEE Trans. Big Data, 7(4): 678-688, 2021.

[64] Yaoliang Chen, Jingxiao Gu, Shi Chen, Sheng Huang, Xiaoyang Sean Wang: "A full-spectrum blockchain-as-a-service for business collaboration," 2019 IEEE International Conference on Web Services (ICWS), 219–223, 2019.

[65] K. Gai et al. "Cost-Aware Multimedia Data Allocation for Heterogeneous Memory Using Genetic Algorithm in Cloud Computing," IEEE Trans. Cloud Comput. 8(4): 1212-1222, 2020.

[66] Weilin Zheng, Zibin Zheng, Xiangping Chen, Kemian Dai, Peishan Li, Renfei Chen. "Nutbaas: A blockchain-as-a-service platform," IEEE Access, 7: 134422–134433, 2019.