ISSN No:-2456-2165

Applications of Blockchain Technology for Cloud Computing Security

Jensy Doshi
Btech Computer Science with Business Systems
SVKM'S NMIMS
Mukesh Patel School of Technology Management and Engineering, Mumbai, Maharashtra, India

Abstract:- Blockchain technology is considered a game changer. Perfect for enhancing your current computer system in many ways. As one of the network-enabled technologies, cloud computing has been widely adopted in the industry through various cloud service models. In terms of functionality and performance, the combination of blockchain technology and existing cloud systems has a great potential.
This study addresses the issue of combining blockchain and cloud computing and examines recent efforts in the technological convergence of blockchain and cloud. There are roughly two technical aspects to this work. This works and both access control and searchable encryption schemes are evaluated.

Keywords:- *Cloud Computing, Blockchain Technology, Data Security, Decentralization, Data Management.*

I. INTRODUCTION

Cloud computing is a well-defined technology that emerged from large-scale distributed computing. Cloud computing can help reduce your processing load. Benefits include reduced hardware and maintenance costs, global availability, flexibility through fully automated processes, and easy scalability. Many large companies such as IBM, Google, Amazon, and Microsoft have adopted cloud computing. Many programs such as Google App Engine, Google Cloud Platform, Amazon Cloud, and Elastic Computing Platform are prototypes. Despite the cloud's many useful services, privacy concerns have slowed companies' adoption of the cloud. Security issues and cloud challenges are significant drawbacks of cloud failure.

Blockchain technology is the way to the future for industries seeking greater security and privacy. The blockchain technology creates a decentralized network in which all network nodes actively participate in validating and verifying data. Cryptography is used to encrypt the data that will be stored in the blockchain. Every block has an encrypted hash, a timestamp, and the hash of the preceding block in the chain to which it will connect. As a result, the data in the blockchain is tamper-proof. The data is secured by blockchain, and individuals that participate in the network will be validated, removing the data's privacy concern.

To facilitate cloud computing growth, we can overcome the data's privacy and security concerns by integrating with blockchain technology. It improves data security, service availability, and it can manage cloud data.

According to our research, several recent studies are looking for ways to improve existing systems by utilising blockchain concepts. One of the primary trends in establishing trustworthiness and reliability in the interconnected networking environment is reengineering cloud datacenters using a blockchain-enabled method.

Tamper-resistant transparent governance [1], decentralization-powered security [2], [3], and creative business models [4], [5] are just a few of the widely recognised benefits of blockchain technology.

Despite the many benefits of blockchain technology, our research found that there are two prevalent difficulties in current blockchain-enabled cloud solutions.

The first type of issue is that while using blockchain in cloud applications, it frequently experiences technological challenges. The majority of the challenges stem from blockchain's technical properties, some of which are considered positives. Based on a real-world instance, our study [6] also indicates that data stored in blocks is exposed to the public, posing a threat to the consortium blockchain-based autonomous trading system. Even while consortium/private blockchain reduces the impact of decentralisation in cloud datacenters, tamper-resistance remains a barrier to developing controllable/scalable cloud systems [7], [8]. Formulating and implementing blockchain service models is another common problem. When Bitcoin was originally introduced to the public, the term "blockchain" was used interchangeably with "Bitcoin," despite the fact that blockchain technology was developed as a distributed ledger-based storage technique a few years before Bitcoin. The success of blockchain in bitcoin has sparked a wave of blockchain-based digital currencies and financial services, but the model has been seldom replicated in other industries.

ISSN No:-2456-2165

II. BLOCKCHAIN-AS-A-SERVICE

A. The idea of BaaS

BaaS is a form of blockchain service model that is based on the cloud computing concept. Blockchain systems or components are considered computing resources in this service paradigm, and can be used to support cloud systems or other applications [9]. The main goal of BaaS is to allow clients to focus on their primary business rather than dealing with the technical challenges of blockchain. A metaphor called "Cloud over Blockchain" is used in work [10] to characterise a blockchain service offering within a cloud service model. As is commonly acknowledged, the ever-increasing demand for cloud services has resulted in a plethora of service models. Apart from the three basic cloud service models (IaaS, PaaS, and SaaS), developing cloud services, such as Backend-as-a-Service, Process As-a-Service, and others, are transmitting even partial processing components or processes into a transferable manner for service demanders. Because of the variety of cloud service models. A service might be a system or a programmable network. content. In the same way, blockchain infrastructure or backend can be used.

BaaS, to be precise, allows clients to receive blockchain-related services using a cloud-based approach. Alibaba Cloud BaaS, for example, offers a number of services to customers via blockchain platforms, including transaction tracking databases, smart contracts, and consortium governance. The function of BaaS varies depending on the BaaS provider. Security, cost savings, system integration, and control optimization are all frequent objective functions.

The primary concept behind BaaS is that the blockchain network/application is considered as a service offering that allows customers to customize blockchain parameters such as blockchain network types and smart contract regulations. The service provider provides the infrastructure for establishing a blockchain network, and partial blockchain codes are open source. Recent studies, such as FSBaaS [11], uBaaS [12], and NutBaaS [13], have looked into the establishment of unique BaaS. We've seen that unified BaaS is still being researched, and most previous attempts have only reached the stage of system design. The problematic thing is that technological issues with communication, consensus, and data synchronisation still persist. The absence of real-world implementations in unified BaaS is due to technical constraints.

B. Industrial Deployment of BaaS

From a performance presentation perspective, modern BaaS offerings resembled BPaaS (Business Process as a Service), both of which emphasized the connection between logical business activities and physical delivery. An emerging trend in blockchain has captured the interest of CSPs. many IT companies. B. Microsoft, IBM, and Amazon offer BaaS in mature cloud environments. IBM BaaS seeks to serve vehicle systems [16]. Oracle BaaS facilitates logistics and payment service delivery [14]. This section presents a comparison of BaaS services. Microsoft Azure [15] is a cloud he platform that provides rapid blockchain deployment and supports Ethereum, Corda and Hyperledger Fabric for the deployment and configuration of blockchain networks. Azure users only need to configure certain parameters instead of understanding all the technical details. Microsoft's solution can also automatically back up on-chain data to off-chain cloud storage. The current version of Azure primarily supports single-node configurations on Fabric, with consortium blockchain deployments under investigation. Users can benefit from IBM's data life-cycle management, which ensures dependable outsourced data management. In addition, IBM BaaS made use of secure containers. It can also let customers set up Blockchains in private clouds or on-premises environments. These features make IBM BaaS a secure and dependable cloud environment. Despite the many benefits of BaaS, the majority of existing BaaS is tied to a single cloud environment due to the blockchain system's limitations. Multi-chain technology is currently being investigated, therefore multi-cloud deployment will require additional research.

C. BaaS Exploration

A common goal for BaaS offerings is to provide a fast and secure blockchain service. Using the cloud to obtain a flexible host service becomes a viable choice. The performance differences of BaaS systems running in cloud and fog settings were studied and analysed by Samaniego and Deters [17], [18]. The findings revealed that, in the cloud, a BaaS system might have higher-level processing capability and storage resources than fog computing, despite a longer latency time.

Because of the decentralised setup in most existing blockchain systems, it was assumed that the necessity for a trustworthy third-party would be minimised. Stakeholder interactions were presumed to be secure regardless of whether the stakeholder was trustworthy. According to recent findings, this premise may be called into question when BaaS is adopted.

Concerns about trust hampered the development of BaaS services from the perspective of the service provider.

Typically, service providers had to demonstrate their data security capabilities by providing visible activities on the distributed ledger. There are four possible solutions:
(i) Improving user controllability by employing PaaS alike settings;
(ii) Minimising recentralization by constructing CSP federations;
(iii)Working on an authenticated trustful environment (e.g., ARM's trust zone);
(iv)Increasing access restrictions.

(BIDaaS) was proposed to eliminate the need for a vetted third party to maintain identification. By posting connected transactions with virtual ID and ID's signature information, this strategy provided a virtual ID registration service.

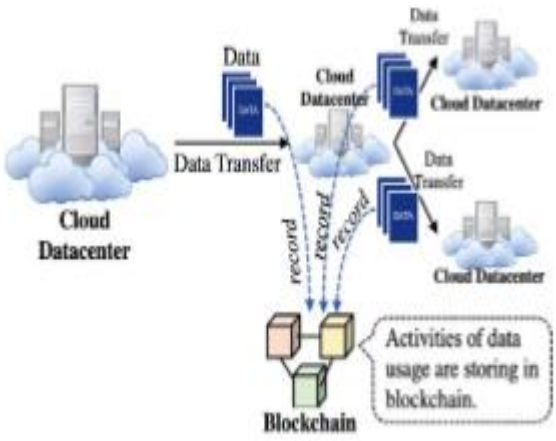
ISSN No:-2456-2165

With the support of BaaS offerings, users can concentrate on the functionality and usability of their blockchain-based apps rather than exploring blockchain network establishment. From the perspective of cost-saving, BaaS is efficient due to the easy-configuration and outsourcing-maintenance. A few tech giants had been developing various BaaS service models as the branch of their cloud services. Our investigations depicted that the industry had ambitious attempts on exploring BaaS, while limited research achievements were revealed. A wider implementation of BaaS needed to take over challenges in trust management, data security, and recentralization's.

III. DATA PROVENANCE IN CLOUD ENABLED BY BLOCKCHAIN

A. Data Provenance Issues

IDC (International Data Corporation) [19] predicted that by 2025, the global data sphere would have grown to 175 Zettabytes, with half of cloud data being housed in public clouds. Data provenance is an important aspect of traceable data consumption when it comes to assisting with the administration of such large amounts of data, both in terms of efficiency and dependability. Provenance is a sort of metadata that records and describes information about operations. A functional provenance reveals when, where, and how data is saved, accessed, modified, and deleted in a cloud datacenter, which implies CSPs are expected to provide dependable cloud-data management when a competent provenance is implemented in the cloud computing scenario.



Benefits of provenance are based on the assumption of metadata that were secure and reliable. However, provenance records still had a chance to be tempered by the threat agent, which could disable/ misused the provenance system [20]. Provenance services were subjected to accidentally shut-down and malicious attacks. It suggested that storage and analysis process be required to realize reliable provenance collections.

B. Blockchain-Enabled Cloud Data Provenance

Blockchain can protect the security of origin data, like a tamper-resistant distributed ledger. The main idea behind a blockchain-based data source is to use the traceability of a blockchain to track all activity that happens to the data in a block. Whether data is stored online or offline, smart contracts are critical to the balance between data origin, functionality, and a trusted environment.

ProvChain [21] is a private cloud network for collecting, storing and verifying source data. Hooks were responsible for monitoring changes in the cloud environment to record these operational events in this blockchain-based origin architecture. In addition, the original data was sensitive and vulnerable to data theft [22]. To protect user privacy, the user ID appears in hashed form in the ProvChain structure. A hashed value can only be mapped to a user ID by one service provider. However, some sensitive data was still recorded in plain text on the blockchain. SmartProvenance technology [23] introduced automatic verification of data origin. Unlike ProvChain, which relied on auditors for verification, SmartProvenance created a peer-to-peer, distributed verification scheme using a voting mechanism. As a result, SmartProvenance no longer requires a trusted auditor. Smart contracts were used for both source data collection and verification to fully automate the entire system. SmartProvenance stored all sensitive data offline, but kept the hash value online for privacy.

GridMonitoring used blockchain technology to create sustainable source data.Offloading of resources and tasks occurred regularly between CSPs. ProvChain and Smart Provenance were not fit for the federated cloud because they were intended for a single provider environment. To address this issue, the team of Xia et al. [60] created MeDShare, which allows for data provenance and auditing in a federated cloud context. The provenance function was created in this study to support secure data sharing among trustless service providers and to prevent malicious attacks that cause financial and reputational harm. Due to an access control-oriented smart contract and a tamper-resistant provenance system, data owners had complete control over data provenance [24].

When CSPs discovered violations or misbehaviors during the provenance phase, they were supposed to perform an automatic access control to revoke access to malicious or aberrant entities.

Some cloud services attempted to provide High Performance Computation (HPC) rather than large amounts of storage as part of a pay-as-you-go model. As a result, these cloud data centres had no hard drives and shared remote storage. Due to the substantial I/O overhead, the above blockchain provenance architectures cannot perform effectively in HPC systems. To achieve trustworthy and efficient provenance in HPC systems, Al-Mamun et al. [25] developed an in-memory blockchain. To reduce I/O overhead, distributed ledgers were kept in volatile memory and communicated using high-speed and persistence protocols in this new design. Furthermore, a neoteric consensus protocol known as Proof-of-Reproducibility (PoR) merged the concepts of PoW and PoS to achieve reliable provenance data validation and replication in a volatile environment. The proposed solution outperformed standard database and file provenance methods in experiments.

Data provenance technology was used to keep track of operations and manage data throughout its lifecycle. Traditional data provenance methods were centralised, complicated, and lacked protection and validation. In this area, we've compiled a list of existing projects that use blockchain to address current issues. Provenance data privacy and interoperability were also explored. In the future, the blockchain solution for cloud data provenance should rely on a smart contract-based system that rewards honest behaviour while punishing malevolent activity.

IV. CLOUDS WITH BLOCKCHAIN-BASED ACCESS CONTROL

A. Cloud Computing Access Control

Access control was a critical component of cloud data security and privacy, as it prevented unauthorised users from accessing cloud data. Other functions, including authentication, authorization, and data auditing, were affected by an unreliable access control technique. The problems of traditional access control mechanisms in clouds were highlighted in this section.

Traditional cloud access control approaches relied heavily on well-defined access control policies.

Traditional policies are divided into four categories: discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC) (ABAC).

In DAC, the legitimate user (e.g., a service provider) was in charge of deciding how other users (e.g., cloud users) might access items [26]. Because no fixed rule was required in DAC, this solution allowed for flexible access control for cloud users. In contrast to DAC, MAC relied on a specified trusting policy that could not be altered dynamically. Because the system administrator was in charge of access restrictions rather than objects, the approach emphasised confidence over integrity [27].Subjects were given access rights based on their roles and responsibilities in the system rather than their identities in the RBAC model [27]. The lack of consideration in other elements of subjects generated a downside due to the nature of RBAC. ABAC was offered as a way to address these difficulties further. It set up the access rule based on object and subject attribute analysis [28]. The importance of ABAC's full consideration during authentication was a major benefit. Despite the fact that ABAC authentication was a time-consuming operation, the computation resource it consumed in the cloud environment was low. Each technique of access restriction has advantages and disadvantages. Traditional access control systems have a common flaw in that they rely heavily on a centralised setting that lacks transparency, traceability, tamper-resistance, and multi-party governance. In the context of the application environment, a trade-off between security and efficiency exists and is difficult to resolve in nature.

B. Cloud Access Control Using Blockchain

Unlike existing access control systems, blockchain-based access control (BAC) has several advantages derived from the properties of blockchain. According to our data, there are two main advantages. First, BAC adds consensus to access control operations by allowing all stakeholders to logically participate in the process. Reaching consensus usually requires consent level approval from participating voters or decision makers, which increases security in terms of decentralization. Second, blockchain traceability provides traceable and immutable governance for access control. This feature increases the difficulty of your opponent. In this part, we will look at some of the latest BAC studies. Because of the layered structure of cloud architecture, access control in clouds primarily served two purposes. The first was the cloud service role, which managed cloud users' access to data and services in the cloud. BlockSLaaS [29], a recent study, offered a blockchain-assisted approach for providing Logging-as-a-Service (LaaS). The proposed mechanism handled cloud forensics, which served as a good example of how blockchain and access control techniques might be combined. On the other hand, it had a visual role in that it required governance for Virtual Machines (VMs) access to actual machines in the event of risks from side channel analyses [30].

A blockchain-based decentralised access control system could eliminate the risk of a single point of failure and data misappropriation by third parties. Data owners could control the access to their own data more flexibly and completely using blockchain technology [31]. According to a recent study [32], BAC can enable data transfer in an untrustworthy environment. Decentralization could mitigate the risks posed by untrustworthy third parties or participants [33].

Some implementations used blockchain transactions to guide the access control process in a cloud environment due to the tamper-resistant and transparent nature of blockchain transactions. A newly created decentralised personal data management system for off-chain storing of mobile data. In this blockchain network, there are two types of transactions. The first type of transaction, Taccess, was created to manage access control. Tdata, the other type of transaction, was in charge of data storage. By defining different policy sets in the Taccess transaction, data owners were able to modify access authentications. Tdata also works with the check policy protocol to control the read/write operations.

Users would have complete control over their data by implementing digitally-signed transactions, preventing harmful invasions (from unauthorised users) in this blockchain-enhanced DAC paradigm. To be more explicit, the protocol-based transaction provided a dynamic and fine-grained access control protocol that included compound key creation, permission check, access control, and data on/off chain protocols. As we entered the blockchain 2.0 age, smart contracts were another frequently utilised alternative that could be used to improve access control. In a telemedicine context, some works created a smart contract based access management system for sensitive health and medical data.

Access control was a critical tool for preventing unauthorised intruders from accessing user data.

Signal point failure, unreliable trusted third parity, and a lack of user control are all issues that traditional access control mechanisms face. Users could have complete control over their data by deploying blockchain technology, which eliminates the risk of a single point of failure.

Smart contracts also allowed for automatic access management and the identification and punishment of misbehaviors.

Furthermore, all of these access control approaches were used to safeguard cloud storage. Cloud VMs, on the other hand, required an access control mechanism to prevent side-channel attacks. To the best of our knowledge, there hasn't been any research on the use of blockchain in VM access management.

V. SEARCHABLE ENCRYPTION IN CLOUDS WITH BLOCKCHAIN

A. Current Searchable Encryption Issues

Due to concerns about losing control over personal data that is outsourced, users might encrypt data before uploading it to the cloud to avoid exposing plain-texts. The honest-but-curious service provider was unable to exquisite and analyse personal sensitive data as a result of this endeavour. This type of protection solution may degrade service availability due to the trade-off between security and availability. One of the most typical difficulties was finding encrypted outsourced data.

To address this issue, searchable encryption was offered as a way for users to get the search result without having to download all of the encrypted material stored in the cloud.

There were two types of searchable encryption techniques that existed at the time: Symmetric Encryption that can be searched (SSE)and searchable Public Key Encryption (PKE).

Song et al. [34] introduced a two-layered searchable encryption technique based on symmetric encryption, which was known as a representative approach of the first generation search encryption. Boneh et al. [35] proposed public key based asymmetric searchable encryption as an extension of Song et al work. To achieve multi keyword search, the work [36] suggested a conjunctive keyword search approach. All of the strategies outlined above, on the other hand, were based on exact matching in order to reduce availability performance. To address this issue further, Li et al. [37] used a fuzzy keyword search instead of precise matching, which produced the result with the highest similarity.

All of the work presented above was based on the premise that CSPs followed the honest-but-curious model [38]. However, due to different insider threats, this assumption proved to be unreliable in practise. Under the guise of energy conservation and fault coverage, dishonest servers may return fraudulent results. It meant that in a searchable encryption scheme, a verification mechanism was desired.

Although various attempts [39–41] were made to check the integrity of returned values, without a trusted party, no punishment could be used to incentivize honest behaviour. Furthermore, verifications were not well-researched, from the server side to against rogue users.

B. Searchable Encryption on the Blockchain

Recent research has centred on resolving existing blockchain-based mechanisms. Chen et al. [42] conducted research on using blockchain to improve encrypted keyword search.

When employing a distributed hash table protocol to merge encryption with keyword search, hostile nodes could sabotage search results, according to the research. Because the majority of nodes follow a self-determining approach, the proposed system might discover and eliminate rogue nodes. Zhang et al. [43] developed a blockchain-assisted PKE called a SEPSE to combat Keyword Guessing Attacks (KGAs).

This paper proposes a few strategies for reducing the likelihood of KGA success, such as screening key encryption, key renewal on a regular basis, and key request monitoring. In order to address the major leakage problem, the work[44] devised a CPA-resistant key aggregation searchable encryption technique.

With the help of broadcasted transactions, some approaches had confirmed the search result. For example, Searchchain [45] was one of the techniques that took this technical route, using a privacy-preserving public key encryption mechanism on top of the Obvious Keyword Search with Authentication (OKSA) mechanism. The unique OKSA mechanism solved the limitations of traditional Oblivious Keyword Search (OKS) by providing key word search authorisation. When CSPs evaluated users' access authentication by a specified term, Searchchain was proposed to reinforce privacy preservation. Without acknowledging any keyword information, data retrieval information was recorded in the block and broadcast to all nodes for verification through a consensus.

Zhang et al. [46] developed a blockchain-based time commitment approach that made use of various transaction types. Without the use of a Trusted-Third Party, dishonest parties would be penalised with bitcoin recompense (TTP). TKSE initially proposed two-sided verification in a searchable encryption system in a follow-up study. Both the harmful service provider and the malicious data owner may face legal consequences. The authors built a merkle tree with ciphertext leafs to validate the search result, then checked the results by its root.

Cloud customers can search their own outsourced data thanks to searchable encryptions. Because CSP(s) may be trustworthy but suspicious or malevolent, encrypted search

results may be inaccurate and misleading. The transaction verification and smart contract were employed with the help of blockchain to ensure the authenticity of the search results. In addition, timely payment was critical. Malicious users may refuse to pay money after receiving accurate information. When the payment system was not properly built, users might still pay for the erroneous search results. The time commitment that was encoded in either transactions or smart contracts was used to implement fair remuneration. Until date, the bulk of blockchain-based searchable encryption solutions have addressed SSE's aforementioned concerns. More investigation into blockchain in PEKS was required.

VI. CONCLUSION

This paper looks at a few technical aspects of leveraging blockchain technology to reengineer cloud computing. The effort encompasses two technical dimensions: service and security. This study explains current research in blockchain-enabled cloud datacenter reengineering through the following aspects: BaaS service model, blockchain-enabled cloud access control, blockchain-enabled cloud data provenance, blockchain-based cloud searchable encryptions. The main conclusions of this study give a theoretical reference for future work in the subject of blockchain-enabled cloud datacenter reengineering.

REFERENCES

[1]. F. S. Hardwick, R. N. Akram, and K. Markantonakis, "Fair and transparent blockchain based tendering framework—A step towards open governance," in Proc. 17th IEEE Int. Conf. TrustCom, 2018, pp. 1342–1347.
[2]. N. Fabiano, "Internet of Things and blockchain: Legal issues and privacy. The challenge for a privacy standard," in Proc. IEEE Int. Conf. IoT, 2017, pp. 727–734.
[3]. W. Meng, E. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," IEEE Access, vol. 6, pp. 10179–10188, 2018.
[4]. K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," IEEE Trans. Ind. Informat., vol. 15, no. 6, pp. 3548–3558, Jun. 2019.
[5]. I. Eyal, A. Gencer, E. Sirer, and R. V. Renesse, "Bitcoin-NG: A scalable blockchain protocol," in Proc. 13th USENIX Symp. Netw. Syst. Design Implement., 2016, pp. 45–59.
[6]. L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," Future Gener. Comput. Syst., vol. 91, pp. 527–535, Feb. 2019
[7]. E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in Proc. Int. Conf. Financ. Cryptography Workshops, 2016, pp. 43–60.
[8]. N. Herbaut and N. Negru, "A model for collaborative blockchain-based video delivery relying on advanced network services chains," IEEE Commun. Mag., vol. 55, no. 9, pp. 70–76, Sep. 2017.
[9]. M. Samaniego and R. Deters, "Blockchain as a service for IoT: Cloud versus fog," in Proc. IEEE Int. Conf. IoT, 2016, pp. 433–436.
[10]. K. Gai, K. Choo, and L. Zhu, "Blockchain-enabled reengineering of cloud datacenters," IEEE Cloud Comput., vol. 5, no. 6, pp. 21–25, Nov./Dec. 2018.
[11]. Y. Chen, J. Gu, S. Chen, S. Huang, and X. S. Wang, "A full-spectrum blockchain-as-a-service for business collaboration," in Proc. IEEE Int. Conf. Web Services, 2019, pp. 219–223.
[12]. Q. Lu, X. Xu, Y. Liu, I. Weber, L. Zhu, and W. Zhang, "uBaaS: A unified blockchain as a service platform," Future Gener. Comput. Syst., vol. 101, pp. 564–575, Dec. 2019.
[13]. W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "NutBaaS: A blockchain-as-a-service platform," IEEE Access, vol. 7, pp. 134422–134433, 2019.
[14]. Oracle. (2019). Oracle Blockchain Blog. [Online]. Available: https://blogs.oracle.com/blockchain/blockchain-use-cases
[15]. Microsoft. (2019). Microsoft Azure. [Online]. Available: https://azure. microsoft.com
[16]. Blockchain. [Online]. Available: https://developer.ibm.com/technologies/blockchain/
[17]. M. Samaniego and R. Deters, "Blockchain as a service for IoT: Cloud versus fog," in Proc. IEEE Int. Conf. IoT, 2016, pp. 433–436.
[18]. M. Samaniego and R. Deters, "Using blockchain to push softwaredefined IoT components onto edge hosts," in Proc. ACM Int. Conf. BDAWT, 2016, p. 58.
[19]. D. Reinsel, J. Gantz, and J. Rydning, "The digitization of the world: From edge to core," Int. Data Corporat., Framingham, MA, USA, White Paper, 2018.
[20]. S. Zawoad, R. Hasan, and K. Islam, "SECProv: Trustworthy and efficient provenance management in the cloud," in Proc. IEEE Conf. Comput. Commun., 2018, pp. 1241–1249.
[21]. X. Liang, S. Shetty, D. K. Tosh, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,"
[22]. M. Reddy and M. Seltzer, "Provenance as first class cloud data," ACM SIGOPS Oper. Syst. Rev., vol. 43, no. 4, pp. 11–16, 2010.
[23]. A. Ramachandran and M. Kantarcioglu, "SmartProvenance: A distributed, blockchain based dataprovenance system," in Proc. 8th ACM Conf. Data Appl. Security Privacy, 2018, pp. 35–42.
[24]. T. McGhin, K. Choo, C. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," J. Netw. Comput. Appl., vol. 135, pp. 62–75, Jun. 2019
[25]. A. Al-Mamun, T. Li, M. Sadoghi, and D. Zhao, "In-memory blockchain: Toward efficient and trustworthy data provenance for HPC systems," in Proc. IEEE Int. Conf. Big Data, 2018, pp. 3808–3813
[26]. J. Lopez and J. Rubio, "Access control for cyber-physical systems interconnected to the cloud," Comput. Netw., vol. 134, pp. 46–54, Apr. 2018

[27]. T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 858–880, 1st Quart., 2019.
[28]. M. Qiu, K. Gai, B. Thuraisingham, L. Tao, and H. Zhao, "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry," Future Gener. Comput. Syst., vol. 80, pp. 421–429, Mar. 2018.
[29]. S. Rane and A. Dixit, "BlockSLaaS: Blockchain assisted secure logging-as-a-service for cloud forensics," in Proc. Int. Conf. Security Privacy, 2019, pp. 77–88.
[30]. Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contractbased access control for the Internet of Things," IEEE Internet Things J., vol. 6, no. 2, pp. 1594–1605, Apr. 2019.
[31]. S. Rouhani and R. Deters, "Blockchain based access control systems: State of the art and challenges," 2019. [Online]. Available: arXiv:1908.08503.
[32]. I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," in Proc. IEEE EIConRus, 2018, pp. 1575–1578.
[33]. S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," IEEE Access, vol. 7, pp. 112713–112725, 2019.
[34]. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy (S&P), 2000, pp. 44–55.
[35]. [35] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Annu. Int. Conf. Theor. Appl. Cryptol. Techn., 2004, pp. 506–522.
[36]. P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Int. Conf. Appl. Cryptography Netw. Security, 2004, pp. 31–45.
[37]. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. IEEE INFOCOM, 2010, pp. 1–5.
[38]. G. Poh, J. Chin, W. Yau, K. Choo, and S. M. Mohamad, "Searchable symmetric encryption: Designs and challenges," ACM Comput. Surveys, vol. 50, no. 3, p. 40, 2017.
[39]. X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Trans. Depend. Secure Comput., vol. 12, no. 5, pp. 546–556, Sep./Oct. 2015.
[40]. Z. Fu, J. Shu, X. Sun, and N. Linge, "Smart cloud search services: Verifiable keyword-based semantic search over encrypted cloud data," IEEE Trans. Consum. Electron., vol. 60, no. 4, pp. 762–770, Nov. 2014.
[41]. R. Cheng, J. Yan, C. Guan, F. Zhang, and K. Ren, "Verifiable searchable symmetric encryption from indistinguishability obfuscation," in Proc. 10th ACM Symp. ICCS, 2015, pp. 621–626.
[42]. L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," Future Gener. Comput. Syst., vol. 95, pp. 420–429, Jun. 2019.
[43]. Y. Zhang, C. Xu, J. Ni, H. Li, and X. S. Shen, "Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage," IEEE Trans. Cloud Comput., early access, Jun. 17, 2019, doi: 10.1109/TCC.2019.2923222.
[44]. J. Niu, X. Li, J. Gao, and Y. Han, "Blockchain-based anti-key-leakage key aggregation searchable encryption for IoT," IEEE Internet Things J., vol. 7, no. 2, pp. 1502–1518, Feb. 2020. [45] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, "Searchain: Blockchainbased private keyword search in decentralized storage," Future Gener. Comput. Syst., vol. 107, pp. 781–792, Jun. 2020.
[45]. Y. Zhang, R. Deng, X. Liu, and D. Zheng, "Outsourcing service fair payment based on blockchain and its applications in cloud computing," IEEE Trans. Services Comput., early access, Aug. 7, 2019, doi: 10.1109/TSC.2018.2864191.