CHAPTER 33
An Analysis of Cloud storage service and Security Threats

Dr. M. Sivaraja
Nehru Institute of Technology, India

Dr. D. Satishkumar
Nehru Institute of Technology, India

Mr. K.Arun Patrick
Nehru Institute of Technology, India

Dr. S. Pathur Nisha
Nehru Institute of Technology, India

Dr. P. Gomathi
Study World College of Engineering, India

ABSTRACT

Cloud storage service has shown its great power and wide popularity which provides fundamental support for rapid development of cloud computing. However, due to management negligence and malicious attack, there still lie enormous security incidents that lead to quantities of sensitive data leakage at cloud storage layer. Once data is stored in the cloud, a client's sovereignty over its data is lost, leaving the data vulnerable to many security threats. From the perspective of protecting cloud data confidentiality, this project proposed a Mimic Model Code Bot that combines cloud computing with block chain that assures data integrity for homomorphic encryption schemes.

Keywords: Code bot, Cloud Technology, Block chain, Homomorphic encryption

INTRODUCTION

In general, data is a distinct piece of information that is gathered and translated for some purpose. If data is not formatted in a specific way, it does not valuable to computers or humans. Data can be available in terms of different forms, such as bits and bytes stored in electronic memory, numbers or text on pieces of paper, or facts stored in a person's mind.

ISBN: 978-93-5782-920-5, www.aetsjournal.com —Handbook of research in Big data Analytics, Artificial intelligence and Machine learning

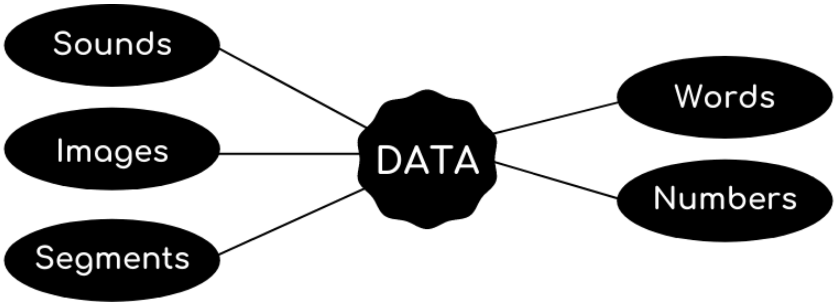

Figure 1.1: Data

Since the invention of computers, people have used the word data to mean computer information, and this information is transmitted or stored. There are different kinds of data; such are as follows:

- Sound
- Video
- Single character
- Number (integer or floating-point)
- Picture
- Boolean (true or false)
- Text (string)

In a computer's storage, data is stored in the form of a series of binary digits (bits) that contain the value 1 or 0. The information can be in terms of pictures, text documents, software programs, audio or video clips, or other kinds of data. The computer data may be stored in files and folders on the computer's storage, and processed by the computer's CPU, which utilizes logical operations to generate output (new data) form input data.

As the data is stored on the computer in binary form (zero or one), which can be processed, created, saved, and stored digitally. This allows data to be sent from one computer to another with the help of various media devices or a network connection. Furthermore, if you use data multiple times, it does not deteriorate over time or lose quality.

CLOUD STORAGE

Cloud storage allows you to save data and files in an off-site location that you access either through the public internet or a dedicated private network connection. Data that you transfer off-site for storage becomes the responsibility of a third-party cloud provider. The provider hosts, secures, manages, and maintains the servers and associated infrastructure and ensures you have access to the data whenever you need.

Figure 1.2: Cloud Storage

Cloud storage delivers a cost-effective, scalable alternative to storing files on premise hard drives or storage networks. Computer hard drives can only store a finite amount of data. When users run out of storage, they need to transfer files to an

external storage device. Traditionally, organizations built and maintained storage area networks (SANs) to archive data and files. SANs are expensive to maintain, however, because as stored data grows, companies have to invest in adding servers and infrastructure to accommodate increased demand.

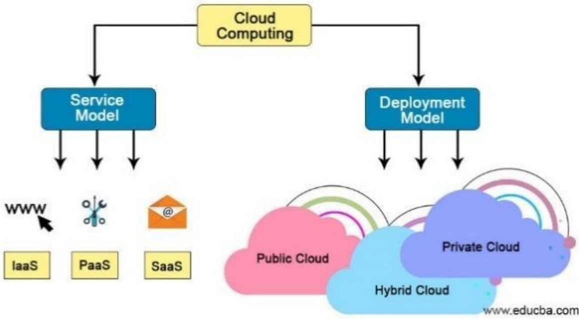

Figure 1.3: Cloud Storage

Cloud storage is available in private, public and hybrid clouds.

PUBLIC STORAGE CLOUDS

In this model, you connect over the internet to a storage cloud that's maintained by a cloud provider and used by other companies. Providers typically make services accessible from just about any device, including smartphones and desktops and let you scale up and down as needed.

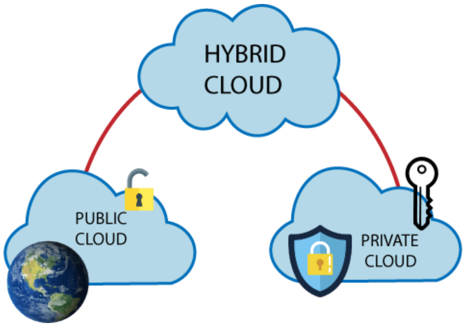

Figure 1.4: Public Cloud Storage

Private cloud storage:

ISBN: 978-93-5782-920-5, www.aetsjournal.com —Handbook of research in Big data Analytics, Artificial intelligence and Machine learning

Private cloud storage setups typically replicate the cloud model, but they reside within your network, leveraging a physical server to create instances of virtual servers to increase capacity. You can choose to take full control of an on premise private cloud or engage a cloud storage provider to build a dedicated private cloud that you can access with a private connection. Organizations that might prefer private cloud storage include banks or retail companies due to the private nature of the data they process and store.
Hybrid cloud storage:
This model combines elements of private and public clouds, giving organizations a choice of which data to store in which cloud. For instance, highly regulated data subject to strict archiving and replication requirements is usually more suited to a private cloud environment, whereas less sensitive data can be stored in the public cloud.

PROBLEMS IDENTIFICATION

A data breach is a cyber-attack in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion. Data breaches can occur in any size organization, from small businesses to major corporations.

1. Accidental Exposure: A large percentage of data breaches are not the result of a malicious attack but are caused by negligent or accidental exposure of sensitive data. It is common for an organization's employees to share, grant access to, lose, or mishandle valuable data, either by accident or because they are not aware of security policies.
2. Phishing and Other Social Engineering Attacks: Social engineering attacks are a primary vector used by attackers to access sensitive data. They involve manipulating or tricking individuals into providing private information or access to privileged accounts.
3. Insider Threats: Insider threats are employees who inadvertently or intentionally threaten the security of an organization's data. There are three types of insider threats:

Non-malicious insider: These are users that can cause harm accidentally, via negligence, or because they are unaware of security procedures. Malicious insider: These are users who actively attempt to steal data or cause harm to the organization for personal gain. Compromised insider: These are users who are not aware that their accounts or credentials were compromised by an external attacker. The attacker can then perform malicious activity, pretending to be a legitimate user. Ransomware: Ransomware is a major threat to data in companies of all sizes. Ransomware is malware that infects corporate devices and encrypts data, making it useless without the decryption key. Attackers display a ransom message asking for payment to release the key, but in many cases, even paying the ransom is ineffective and the data is lost.
Data Loss in the Cloud: Many organizations are moving data to the cloud to facilitate easier sharing and collaboration. However, when data moves to the cloud, it is more difficult to control and prevent data loss. Users access data from personal devices and over unsecured networks.
SQL Injection: SQL injection (SQLi) is a common technique used by attackers to gain illicit access to databases, steal data, and perform unwanted operations. It works by adding malicious code to a seemingly innocent database query. SQL injection manipulates SQL code by adding special characters to a user input that change the context of the query. The database expects to process a user input, but instead starts processing malicious code that advances the attacker's goals. SQL injection vulnerabilities are typically the result of insecure coding practices.

DATA BREACHES IN CLOUD COMPUTING

Data breaches in cloud computing maintain their status as one of the top cybersecurity threats in 2021. Today, organizations are placing more data as well as infrastructure in the public cloud. The public cloud has made it possible for organizations to be much more efficient, agile, and to integrate new technologies much more quickly

In today’s world, a cloud solution is essential for enterprises and individuals. Cloud infrastructures like AWS and Microsoft Azure have transformed the way businesses and hobbyists use storage and computing. Traditional cloud storage solutions are centralized. A single business entity controls the infrastructure, raising questions about privacy and security. This dependability on a third party to keep the data secured is a disadvantage for cloud storage.

BLOCKCHAIN TECHNOLOGY

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the “chain,” in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a ‘digital ledger. ‘Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure.

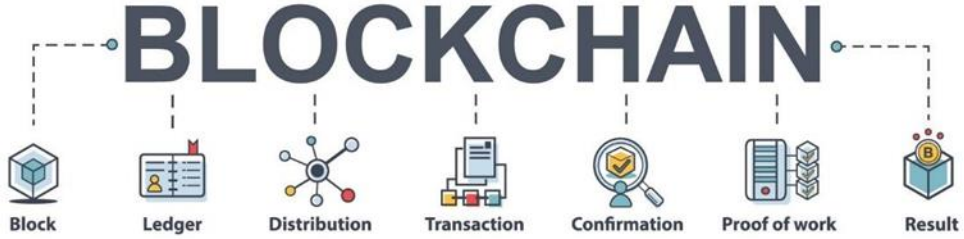

Figure 1.5: Blockchain Technology

Security is not the only benefit of blockchain technology. Blockchain technology makes sure the owner of the data is anonymous. All the sensitive information about identity is protected. Whenever a user tries to obtain the data, all the sections are validated to check for alterations. If any alteration is found, the miner responsible for that is eliminated from the network. From big tech corporations to entrepreneurs, several companies have jumped to the blockchain cloud storage market, transforming their businesses digitally. Blockchain provides not only secure but also a cheap way to get cloud storage because many small organizations collaborate to share the computing power and space to store data.

HISTORY OF BLOCKCHAIN

Satoshi Nakamoto, whose real identity still remains unknown to date, first introduced the concept of blockchains in 2008. The design continued to improve and evolve, with Nakamoto using a Hashcash-like method. It eventually became a primary component of bitcoin, a popular form of cryptocurrency, where it serves as a public ledger for all network transactions. Bitcoin blockchain file sizes, which contained all transactions and records on the network, continued to grow substantially. By August 2014, it had reached 20 gigabytes, and eventually exceeded 200 gigabytes by early 2020.

KEY ELEMENTS OF A BLOCKCHAIN

1. Distributed ledger technology: All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that’s typical of traditional business networks.
2. Immutable records: No participant can change or tamper with a transaction after it’s been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.
3. Smart contracts: To speed transactions, a set of rules — called a smart contract is stored on the blockchain and executed automatically.

TYPES OF BLOCKCHAIN:

ISBN: 978-93-5782-920-5, www.aetsjournal.com ―Handbook of research in Big data Analytics, Artificial intelligence and Machine learning

All types of blockchains can be characterized as permissionless, permissioned, or both. Permissionless blockchains allow any user to pseudo- anonymously join the blockchain network and do not restrict the rights of the nodes on the blockchain network. The identities of the users of a permissioned blockchain are known to the other users of that permissioned blockchain. Blockchain Buzzwords Permissionless blockchains tend to be more secure than permissioned blockchains, because there are many nodes to validate transactions, and it would be difficult for bad actors to collude on the network.

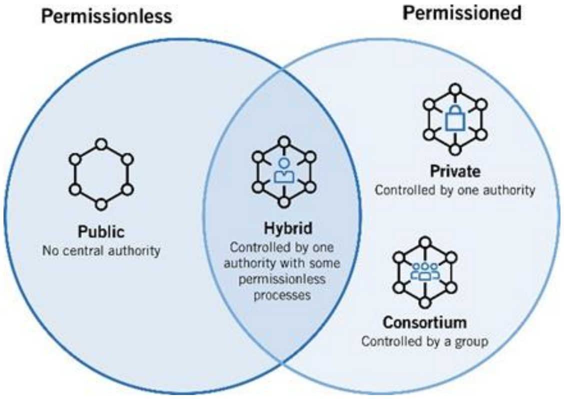

Figure 1.6: Three types of blockchain

1. Public blockchain: A public, or permission-less, blockchain network is one where anyone can participate without restrictions. Most types of cryptocurrencies run on a public blockchain that is governed by rules or consensus algorithms.
2. Permissioned or private blockchain: A private, or permissioned, blockchain allows organizations to set controls on who can access blockchain data. Only users who are granted permissions can access specific sets of data. Oracle Blockchain Platform is a permissioned blockchain.
3. Federated or consortium blockchain: A blockchain network where the consensus process (mining process) is closely controlled by a preselected set of nodes or by a preselected number of stakeholders.

BENEFITS OF BLOCKCHAIN

1. Greater trust: With blockchain, as a member of a members-only network, you can rest assured that you are receiving accurate and timely data, and that your confidential blockchain records will be shared only with network members to whom you have specifically granted access.
2. Greater security: Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently.
3. More efficiencies: With a distributed ledger that is shared among members of a network, time-wasting record reconciliations are eliminated.

TOP BLOCKCHAIN USE CASES FOR CYBERSECURITY

Due to its nature, the blockchain offers promising cybersecurity options to startups and enterprises operating in different fields. The list of sectors that can benefit the most from applying the blockchain for cybersecurity includes.

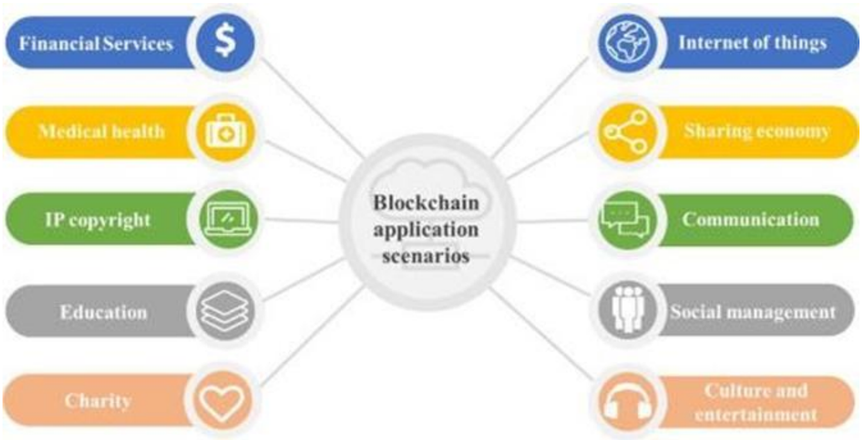

Figure 1.7: Benefits of blockchain

1.4. CRYPTOGRAPHY:

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. It includes techniques such as microdots, merging words with images and other ways to hide information in storage or transit.

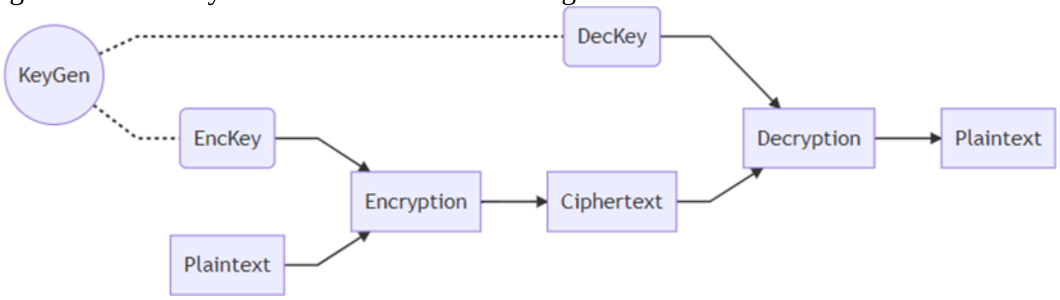

Figure 1.8: Cryptography

From the diagram, we can see the overall composition of an encryption scheme:

There is a KeyGen algorithm that generates the key used for both encrypting and decrypting. Notice that in a symmetric scheme both keys are the same, and in an asymmetric scheme the keys are different. (One is called Public Key and the other is called Private Key)

The Encryption algorithm applies encryption to a given plaintext using the encryption key. Then it produces the ciphertext, which is the encrypted plaintext.

The Decryption algorithm inverts the encryption done on a ciphertext using the decryption key. It restores the ciphertext back to the original plaintext.

LITERATURE SURVEY

2.1. Enhanced Security in Cloud Computing using Neural Network and Encryption Author: Muhammad Usman Sana, Zhanli Li, Fawad Javaidi, Hannan Bin Liaqat and Muhammad Usman Ali. Year: October 26, 2021. Link: https://ieeexplore.ieee.org/document/9585614.

This article proposed to protect privacy and provide high accuracy in a reasonable amount of time when compared to other state-of-the-art techniques. This article provides detailed information about the neural network model developed for the application under study also show their runtime performance and model accuracy results.

2.2. Using Block Chain in Cloud Computing to Enhance Relational Database Security Author: Ruba Awadallah and Azman Samsudin Year: September 11, 2021. Link:

https://ieeexplore.ieee.org/document/9558818 Objective: This article provides an optimal solution based on encrypting data using FHE cryptosystems and simulating BC technology in the cloud RDB structure.

2.3. Block Chain Based Cloud Computing: Architecture and Research Challenges Author: Ch. V. N. U. Bharathi Murthy, M. Lawanya Shri, Seifedine Kadri and Sangsoon Lim Year: November 23, 2020.

Link: https://ieeexplore.ieee.org/document/9252909 In this survey developed an architecture integrating block chain with cloud revealing the communication between block chain and cloud.

2.4. Cloud Manufacturing Architecture Based on Public Blockchain Technology Author: Baran Kaynak; Sümeyye Kaynak; Özer Uygun Year: January 6, 2020.

Link: https://ieeexplore.ieee.org/document/8943230

This study is the use of BC technology in cloud manufacturing is attempted to be explained with an example application and it is aimed to shed light on the future studies. For future work, designed sacs may be developed and other services, such as machining as a service, will be directly integrated into the system.

2.5. Decentralized and Privacy-Preserving Public Auditing for Cloud Storage based on Blockchain Author: Ying Miao, Qiong Huang , Meiyan Xiao, And Hongbo Li Year: July 30, 2020

Link: https://ieeexplore.ieee.org/document/9152981 This article try to solve the problem that the cloud server may guess challenge messages ahead of time in decentralized public auditing schemes, and in the meanwhile, to guarantee that the TPA does not know extra information of user data for the sake of privacy protection.

2.6. A Secure Cloud Storage Framework with Access Control Based on Blockchain Author: Shangping Wang; Xu Wang; Yaling Zhang. Year: 23 July 2019.

Link: https://ieeexplore.ieee.org/document/8770246 This article is based on the cloud storage platform; the cloud storage platform is semi-honest. Therefore, the program also lacks research data integrity which ensures that data owner to upload the document has not been tampered with. In the future, cloud storage platforms may be replaced with decentralized storage platforms, such as Inter Planetary File Systems.

2.7. Analysis of Data Management in Blockchain-Based Systems: From Architecture To Governance Author: Hye-Young Paik, Xiwei Xu, H. M. N. Dilum Bandara, Sung Une Lee, and Sin Kuang Lo

Year: December 23, 2019 Link: https://ieeexplore.ieee.org/document/8938787 This article proposes to increase the level of understanding of blockchain technology as a data store and to promote a methodical approach in applying it to large software systems for examine the data governance issues in blockchains in terms of privacy and quality assurance.

2.8. Blockchain Based Data Integrity Verification for Large-Scale IoT Data Author: Haiyan Wang and Jiawei Zhang Year: November 11, 2019.

Link: https://ieeexplore.ieee.org/document/8895808 This article proposes a prototype system with an edge computing to process the IoT data. Experimental results finally demonstrate that the proposed BB-BIS outperforms existing blockchain based methods in terms of computational cost and communication overhead for large-scale IoT data

2.9. Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications

Author: MD. Abdur Rahman; M. Shamim Hossain; George Loukas; Elham Hassanain; Syed Sadiqur Rahman; Mohammed F. Alhamid; Mohsen Guizani . Year: 14 November 2018

Link: https://ieeexplore.ieee.org/document/8534320 This article proposes a novel mobile edge network that uses blockchain, an anonymous Tor tier, and a secure distributed DB to make therapy applications immutable, always available with service quality, and interoperable. To the best of our knowledge, this therapy application is one of the first to propose a secure mobile edge network solution.

2.10. Medshare: Trust-Less Medical Data Sharing Among Cloud Service Providers Via Blockchain

Author: Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. Year: July 24, 2017 Link: https://ieeexplore.ieee.org/document/7990130

This article proposed a blockchain based solution for sharing medical data among cloud service providers while providing data access control, provenance and auditing. Actions of data beneficiaries are constantly monitored through mechanisms mentioned later in the paper and breaches are addressed accordingly by revoking access to the data.

CONCLUSION

A technology known as "cloud computing" makes use of the internet and centralized remote servers to maintain data and applications. The use of apps without installation and access to personal files from any computer thanks to cloud computing using the internet. Using this technology's centralization, computers may be significantly more effective. bandwidth, computing, and data storage . Ramnath Chellapa, a professor at Emory University and the University of South Cloud computing was described as the "new computing paradigm where the boundaries are fluid" in California. rather than just technical constraints, economic logic will govern the future of computing. This has evolved into the foundation of how we talk about clouds today.

REFERENCES

Al Mamun. A, Jahangir. M. U. F, Azam. S, Kaiser. M. S, and Karim. A, “A combined framework of interplanetary file system and blockchain to securely manage electronic medical records,” in Proceedings of International Conference on Trends in Computational and Cognitive Engineering. Springer, 2021, pp. 501–511.

Benisi. N. Z, Aminian. M, and Javadi. B, “Blockchain-based decentralized storage networks: A survey,” Journal of Network and Computer Applications, vol. 162, p. 102656, 2020.

Chen. C, Yang. J, Tsaur. W. J, Weng. W, Wu. C, and Wei. X, “Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in iiot’s application,” Sensors, vol. 22, no. 3, p. 1146, 2022

Chi. J, Li. Y, Huang. J, Liu. J, Jin. J, Chen. C, and Qiu. J, “A secure and efficient data sharing scheme based on blockchain in industrial internet of things,” Journal of Network and Computer Applications, vol. 167, p. 102710, 2020.

Faruk. M. J. H, Shahriar. H, Valero. M, S. Sneha, Ahamed. S. I, and Rahman. M, “Towards blockchain-based secure data management for remote patient monitoring,” in 2021 IEEE International Conference on Digital Health (ICDH). IEEE, 2021, pp. 299–308.

Hemamalini. V, Zayaraz. G, and Vijayalakshmi. V, “Bspc: blockchainaided secure process control for improving the efficiency of industrial internet of things,” Journal of Ambient Intelligence and Humanized Computing, pp. 1– 14, 2022.

Lobo. P. A and Sarasvathi. V, “Distributed file storage model using ipfs and blockchain,” in 2021 2nd Global Conference for Advancement in Technology (GCAT). IEEE, 2021, pp. 1–6.

Lu. X, Fu. S, Jiang. C, and Lio. P, “A fine-grained iot data access control scheme combining attribute-based encryption and blockchain,” Security and Communication Networks, vol. 2021, 2021.

Naz. M, Al-zahrani. F. A, Khalid. R , Javaid. N, Qamar. A. M, Afzal. M. K and Shafiq. M, “A secure data sharing platform using blockchain and interplanetary file system,” Sustainability, vol. 11, no. 24, p. 7054, 2019.

Niu. S, Chen.L, Wang. J, and Yu. F, “Electronic health record sharing scheme with searchable attribute-based encryption on blockchain,” IEEE Access, vol. 8, pp. 7195–7204, 20190.