International Journal for Modern Trends in Science and Technology, 8(05):78-85, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0805012
Available online at: http://www.ijmtst.com/vol8issue05.html

Virtual Assistant Mimic Model for CloudData Security

A. Menaka[1] | S. sandhya[2] | R. Shalini[2] | I. Tehreen[2]

[1]Assistant Professor, Department of Information Technology,Adhiyamaan College of Engineering.
[2]Department of Information Technology,Adhiyamaan College of Engineering.

To Cite this Article
A. Menaka, S. sandhya, R. Shalini and I. Tehreen. Virtual Assistant Mimic Model for CloudData Security. International Journal for Modern Trends in Science and Technology 2022, 8(05), pp. 78-85. https://doi.org/10.46501/IJMTST0805012

Article Info
Received: 29 March 2022; Accepted: 27 April 2022; Published: 01 May 2022.

ABSTRACT

Cloud storage has demonstrated its immense power and widespread acceptance, providing critical support for the rapid growth of cloud computing. However, massive security events continue to occur as a result of management in competence and malevolent attacks, resulting in large amounts of sensitive data leaking at the cloud storage tier. In order to preserve cloud data secrecy, this study suggested a Mimic model of Virtual Assistant that blends cloud computing with blockchain and ensures data integrity for homomorphic encryption techniques. Apart from encrypting data homomorphically, a secure cloud service provider (CSP) platform requires a strong, tamperproof, and verifiable security architecture. A virtual assistant will be engaged to store customer data and conduct calculations on it. Each Virtual Assistant (VA) will be required to generate a master hash value for their database on a private blockchain on a regular basis. A client can compare these master hash values to see whether there has been any data tampering. Because data alterations by CSPs may be discovered by comparing master hash values kept on the blockchain, this distributed verification method meets the requirements of secrecy (homomorphic encryption will be employed for encryption) and integrity. To encourage honesty, the data sharing procedure is carried out via a smart contract, and all parties engaged must escrow. Confidentiality, integrity, privacy, non-repudiation, and anonymity are all security qualities guaranteed by data storage and sharing protocols.

KEYWORDS:Virtual Assistant, Cloud, BlockChain, KeyGeneration, Mimic Model, Data Integrity.

1. INTRODUCTION

Data, in general, is a discrete piece of information that is collected and translated for a specific purpose. Data that is not structured in a specified way is useless to computers and humans. People have used the term data to refer to computer information that is communicated or stored since the introduction of computers. Pictures, written documents, software applications, audio or video clips, and other types of data can be used to convey information. Because the data is kept on the computer in binary form (zero or one), it may be digitally processed, produced, saved, and stored. This lets data to be transmitted from one computer to another via a network connection or multiple media devices. Furthermore, data does not decay or lose quality over time when used several times.

STRUCTURE OF PAPER

The paper is organized as follows: In Section 1, the introduction of the paper is provided along with the structure, important terms, objectives and overall description. In Section 2 we discuss related work. In Section 3 we have the complete information about project how the virtual assistant works and reduse the work Data Owner. Section 4 shares information about the modules of proposed work. Section 5shares information about workflow of the project.Section 6

concludes the paper with acknowledgement and references.

OBJECTIVES

To reduces the workload of Computation to Data Owner. No need for direct communication between the data owner and cloud service providers instead of that virtual assistant will act as an intermediate. As soon as the owner added the employee. Then the employee will get a mail regarding username and password.

2. RELATED WORK

1.Cloud Manufacturing Architecture Based on Public Blockchain Technologypublished by Baran Kaynak; Sümeyye Kaynak; Özer Uygun in the year 2020. The objective of this study has enabled manufacturing resources to be leased and shared on a global scale. However, it has problems arising from its central structure and the need for a reliable 3rd party. Reliability, security, continuity, scalability, data lock-in, single point failure, data manipulation are some of the main problems. Blockchain (BC) is a decentralized and distributed technology. The data stored on the B
C network cannot be altered in any way. With these features, we believe that blockchain supported cloud manufacturing systems can overcome the aforementioned problems and eliminates the need for a reliable 3rd party. Based on this belief, in this study the agreements and communication are realized with a decentralized application using block chain based smart contracts (scs). The designed application is called the decentralized cloud manufacturing application (dcmapp). Dcmapp does not operate on a fully public block chain network, it has a hybrid structure and uses the Ethereum network as a public BC network. These features make dcmapp different from other block chain-based cloud manufacturing applications.

2.Block Chain Based Cloud Computing: Architecture andResearch Challenges published by Ch. V. N. U. Bharathi Murthy, M. Lawanya Shri, Seifedine Kadri and Sangsoon Lim in the year 2020. This survey develops the Block chain technology is the necessary technology behind Bit coin, which is a popular digital Crypto currency. Cloud computing is a practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.'' It is still facing many challenges like data security, data management, compliance, reliability. In this article, we have mentioned some of the significant challenges faced by the cloud and proposed solutions by integrating it with block chain technology.

3.Blockchain Based Data Integrity Verification for Large-Scale IoT Data published by Haiyan Wang and Jiawei Zhang in the year 2019 had proposed a Blockchain and Bilinear mapping-based Data Integrity Scheme (BB-DIS) for large-scale iot data. In our BB-DIS, iot data is sliced into shards and homomorphic verifiable tags (hvts) are generated for sampling verification. Data integrity can be achieved according to the characteristics of bilinear mapping in the form of blockchain transactions. Performance analysis of BB-DIS including feasibility, security, dynamicity and complexity is also discussed in detail. A prototype system of BB-DIS is then presented to illustrate how to implement our verification scheme. Experimental results based on Hyperledger Fabric demonstrate that the proposed verification scheme significantly improves the efficiency of integrity verification for large-scale iot data with no need of tpas.

4.Analysis of Data Management in Blockchain-Based Systems: From Architecture To Governance published by Hye-Young Paik, Xiwei Xu, H. M. N. Dilum Bandara, Sung Une Lee, and Sin Kuang Lo in the year 2019 had analyzed blockchains from the viewpoint of a developer to highlight important concepts and considerations when incorporating a blockchain into a larger software system as a data store. The work aims 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. First, we identify the common architectural layers of a typical software system with terms. Second, we examine the placement and flow of data in blockchain-based applications. Third, we explore data administration aspects for blockchains, especially as a distributed data store. Fourth, we discuss the analytics of blockchain data and trustable data analytics enabled by blockchain.

5.Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications published by MD. Abdur Rahman; M. Shamim Hossain; George Loukas; Elham Hassanain; Syed Sadiqur Rahman; Mohammed F. Alhamid; Mohsen Guizani in the year 2018 had proposed an in-home

therapy management framework, which leverages the iot nodes and the blockchain-based decentralized MEC paradigm to support low-latency, secure, anonymous, and always-available spatiotemporal multimedia therapeutic data communication within an on-demand data-sharing scenario. To the best of our knowledge, this non-invasive, MEC-based iot therapy platform is first done by our group. This platform can provide a full-body joint range of motion data for physically challenged individuals in a decentralized manner. With MEC, the framework can provide therapy diagnostic and analytical data on demand to a large portion of humanity who are either born with disabilities or became disabled due to accidents, war-time injuries, or old age. For security, the framework uses blockchain–Tor-based distributed transactions to preserve the therapeutic data privacy, ownership, generation, storage, and sharing.

6.Enhanced Security in Cloud Computing using Neural Network and Encryption published by Muhammad Usman Sana, Zhanli Li, Fawad Javaidi, Hannan Bin Liaqat and Muhammad Usman Ali in the year 2021 had developed the functionality of the NN network model by using the homomorphic properties of the more schemes to complete the work of coding data. The proposed workflow on homomorphic encryption and NN is shown in Fig. 4. In the processing stage, the trained data is encoded using a secret key that is not shared. Finally, it directly supports floating-point calculation with the help of the homomorphic function of the more encrypting scheme, and all the processes achieved on the Attributes. Network is able to train directly on the encrypted text information. This creates a model that gives an encoded prediction that merely the holder of the secret key can decrypt. When the training stage is complete, use the encoded model to predict new cipher instances. Here the input sample is encoded using the same key used in the training stage. More encryption schemes rely on symmetric keys to encrypt plain-text data and decrypt cipher-text data.

7.Medshare: Trust-Less Medical Data Sharing Among Cloud Service Providers Via Blockchain published by Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani in the year 2017 had proposed medshare, a system that addresses the issue of medical data sharing among medical big data custodians in a trust-less environment. The system is blockchain-based and provides data provenance, auditing, and control for shared medical data in cloud repositories among big data entities. In medshare, data transitions and sharing from one entity to the other, along with all actions performed on the tamper-proof manner. The design employs smart contracts and an access control mechanism to effectively track the behavior of the data and revoke access to offending entities on detection of violation of permissions on data. By implementing medshare, cloud service providers and other data guardians will be able to achieve data provenance and auditing while sharing medical data with entities such as research and medical institutions with minimal risk to data privacy.

8.Using Block Chain in Cloud Computing to Enhance Relational Database Security published by RubaAwadallah and Azman Samsudin in the year 2021 had provided an optimal solution based on encrypting data using homomorphic encryption cryptosystems and simulating block chain technology in the cloud RDB structure.The design of block chain over cloud-RDB is based on simulating block chain security components over the RDB stored and processed in cloud servers. It provides a client self-verification system that detects and restricts internal threats applied to data computations in the cloud.

9.A Secre Cloud Storage Framework with Access Control Based on Blockchain published by Shangping Wang; Xu Wang; Yaling Zhang in the year 2019 had proposed a new secure cloud storage framework with access control by using the Ethereum blockchain technology. Our new scheme is a combination of Ethereum blockchain and ciphertext-policy attribute-based encryption (CP-ABE). The proposed cloud storage framework is decentralized, that is, there is no trusted third party in the system. Our scheme has three main features. First, as the Ethereum blockchain technology is used, the data owner can store ciphertext of data through smart contracts in a blockchain network. Second, the data owner can set valid access periods for data usage so that the ciphertext can only be decrypted during valid access periods.

10 Decentralized and Privacy-Preserving Public Auditing for Cloud Storage based on Blockchain published by Ying Miao, Qiong Huang, Meiyan Xiao,

And Hongbo Li in the year 2020 had proposed a decentralized and privacy preserving public auditing scheme, which is secure against the procrastinating third-party auditor and malicious cloud server. Our scheme utilizes two components to generate unpredicted challenge messages. One is generated by the auditor, and the other is a series of decentralized block hashes. Our scheme could resist against the procrastinating auditor, and a malicious cloud server could not retrieve or guess the challenge message ahead of the audit time. Furthermore, our scheme provides better protection of user privacy during the process of verification of the audit response from the cloud server.

3. PROPOSED SYSTEM

This project suggests a method for ensuring data integrity in the cloud by combining cloud computing and blockchain. For data secrecy in cloud computing, the suggested solution in this research combines HE and BC in a cohesive way. A virtual assistant with a mimic model that combines cloud computing and a blockchain network to ensure data integrity for completely homomorphic encryption. The blockchain network and smart contracts are designed to record information on a cloud-based file and verify its integrity. A smart contract that lets the data owner to create data users and access control policies for those users. A virtual assistant will be engaged to store customer data and conduct calculations on it. Using open-source services and APIs, it creates a smart assistant. It can carry out tasks or provide services for an individual depending on the data owner's orders. The saved data will be encrypted and decrypted using fully homomorphic encryption. It enables for an endless amount of ciphertext arithmetic operations while still providing a valid result. For key generation, integrity check services are employed.

4. PROPOSED WORK

1. Cloud Server API

The Cloud Server API is a programming interface that gives you quick access to all of the Cloud Server's features. This programming interface is based on the Flask API. Cloud apps may be made smaller by-passing data to API-based back-end services for processing or analytics calculations, and then returning the results to the cloud application. Authorized users receive instant access to the data on cloud services. Cloud apps provide fine-grained, centralized control over users and data.

Cloud Service Provider(csp):

The cloud service provider has a lot of storage space and a lot of processing power. It earns money by offering diverse customers with storage and computing services, allowing them to upload and download data at any time and from any location. The cloud service provider, on the other hand, is just responsible for data storage and does not guarantee data security.

Data Owner (DO):

Because the data owner owns the data files and has limited local storage space, the data owner decides to entrust the information to the cloud service provider. The data owner will periodically examine the integrity of the uploaded data for the benefit of cloud data security. The admin interface allows the data owner to manage all accounts, add, alter, and remove accounts, unsuspend or suspend websites, change passwords, and more. Unauthorized personnel cannot control or see data because of the data owner's access control policy.

Data Upload:

A user can use this technique to outsource data to a cloud service provider. The data owner creates encrypted files and tags all data blocks before sending them to the cloud server. The cloud server should also verify that the data uploaded is accurate.

Integrity Verification:

This method necessitates the data owner auditing the integrity of cloud data on a frequent basis, as well as the data owner verifying the conduct of data users over a longer period of time. The data owner transmits the challenge information to the blockchain, which creates a data integrity proof, which the data owner validates. Furthermore, the data owner must create a log file that captures the data user's verification information and allows the data owner to audit the data user's conduct by validating the log file's authenticity and accuracy. Managing a Cloud Server, as well as a user account for data, are all tasks that must be completed. Purchasing more resources, logging, resource usage statistics, uploading files, and maintaining integrity.

Receive Request.:

Receive the requested file from the virtual assistant and decrypt it using the data user's private key. Also, play about with the file. If a data user wishes to upload a file

back to the cloud, encrypt it with the data owner's private key and upload it to the IPFS cloud storage server. The Blockchain keeps track of all data users' transactions

2. Block Cloud Integration

Our approach includes blockchain as a key component. During the data integrity verification process, a third-party audit platform between the data user and the cloud service provider is responsible for relaying and documenting the data user and cloud service provider interactions. When a data owner has a disagreement with a cloud service provider, the blockchain records can be submitted as legitimate proof to an arbitration organization. The blockchain network is cooperatively maintained by all members, and user and cloud service provider behavior is collectively monitored to guarantee the system's regular functioning.

Smart Contract:

Data owners use IPFS smart contracts for data storage and data sharing, which we call data storage and data sharing. When this process defines numerous contract variables, it is called smart contract initialization.

1) The mapping type "authorized user" variable is a Boolean value that establishes a mapping collection from an authorized user address.

2) A mapping type uses a mapping variable to specify an index of encrypted keyword indexes to related data. The data owner can add, update, and remove data collects using smart contracts. Smart contract interfaces allow the authorized data user to access the data.

Data storage and sharing:

Only log events are provided by Block cloud smart contracts to identify the return value of nonconstant functions. To begin the digital data exchange process, the Degenerates the original file metadata. The file name, type, size, and description are all examples of metadata. As a result, the search results given by the search function are only accessible through events in the aforesaid data sharing contract. A entire encrypted file (CEF) is posted to IPFS in addition to the metadata. The first algorithm for uploading files to IPFS is shown below. It keeps track of DO Meta mask account addresses and rewards storage nodes. The IFPS generates the hash, which is then placed on the Block cloud blockchain.

Add User (new user account address):

This procedure is conducted by the contract's creator (DO), who passes the user's identity (registration data) as an input to the function. The system verifies the user's identity through the registration page and creates a unique private key for each user.

Integrity Verification

Miners are the participants on the blockchain who verify the transaction's integrity. Proof-of-Work (PoW), commonly known as 'mining,' is this technique. The transaction with this nonce is published on the blockchain system by the first miner who finds it. Other miners check if nonce is a good answer to this challenging challenge, and if so, they add a new block to their network. If a large number of miners verify and approve a transaction, it can be recorded on the blockchain. request the blockchain to verify the file's integrity. Block cloud produces the verification link and sends it to the DO, who validates the file's integrity.

3. KEY GENERATION CENTRE (KGC).

The KGC creates the system's public and private keys. It's regarded to be semi-reliable. The KGC is only allowed to look at the data owner's data objects, access control policies, and constraint policies while it is performing valid responsibilities given to it by other entities.

Homomorphic Key Generation:

DO receives the system security parameter as an input and begins the system configuration operation. The system's public parameter PK and the master key K will be returned as outputs. DO publishes PK in public media, such as websites and public databases, because it is public and accessible to all users. DO embeds K to VA and deploys smart contracts on the Block cloud at the same time. This algorithm is conducted by the DO. The system receives the master key MK, the public parameter PK, and the user attribute set S as inputs. S = att1, att2, attn is the DU's attribute list from which the associated private key SKDU was acquired. DO determines SKDU ∈ R Z* Q for each user. Then for {1 ≤ i ≤ n}, DO computes

$$\overline{\sigma_i} = \sigma_{i,k} = g^{\mathrm{H}_1(y||i||k)} \times \mathbb{H}_2 SK_{DU}^{\mathrm{H}_1(x||i||k)}$$

Finally, it generates the DU private key and public key, as well as the related attribute set S. DO provide the necessary DU private key and PKDO to the DU through

email. To the VA, add all of the PKDU and MKDO public keys.

Homomorphic Encryption and Decryption:

The process of converting data into ciphertext in which the process may operate on encrypted data without having access to the private decryption key; the owner of the data should be the only one with access to the private key. When arithmetic operations are applied to encrypted data, the same results should be obtained as when the data is unprocessed. The data owner produces the public-key pair in the first step of the HE processes, which is called KeyGen (a public key puk and a private key prk). The encryption procedure Enc is the next step, which entails applying an encryption algorithm to the data C = Encpuk (P) before transmitting it to the cloud server. The puk and encrypted data are kept in a database on the cloud server. The cloud server conducts the desired computation on the encrypted data when prompted by the client before returning the result to the client in its encrypted form. This is referred to as the Eval (evaluation) procedure. The client can use the associated prk to perform the Dec decryption function to retrieve the plaintext. To summaries, HE has four primary operations: KeyGen, Enc, Eval, and Dec. Despite the benefits of a homomorphic cryptosystem, all designs are not IND-CCA2 safe due to their malleability. This may result in incorrect outsourced computations. It's worth noting that same issues can arise even if the data isn't encrypted.

4.AUTHENTICATIONS:

This module contains the primary entrance to the application, as well as the login and registration pages. To utilize the programme, both the data owner and the data user must first register. After registering, the data owner and data user can log in using his unique user's name and password. Here, the data owner must register for both key creation and login. The data owner will set up authentication for the data user, and the user will get an email with the username and password. After logging in, the user will see a welcome screen with several functions. Md5 encryption is used for security. MD5 (Message Digest Technique 5) is a cryptographic hash algorithm that may be used to generate a 128-bit text value from a string of any length. The most prevalent method for verifying the integrity of files is MD5. Other security protocols and applications, such as SSH, SSL, and IPsec, use it as well.

5.VIRTUAL ASSISTANT

Data Retrieval Request.:

Data collection is requested by the service provider. We wish to gather data by building a legitimate trapdoor using the connection keyword, according to the user's labelling. Meanwhile, a data state channel is established. The operation is brought up to date and then documented off-chain.

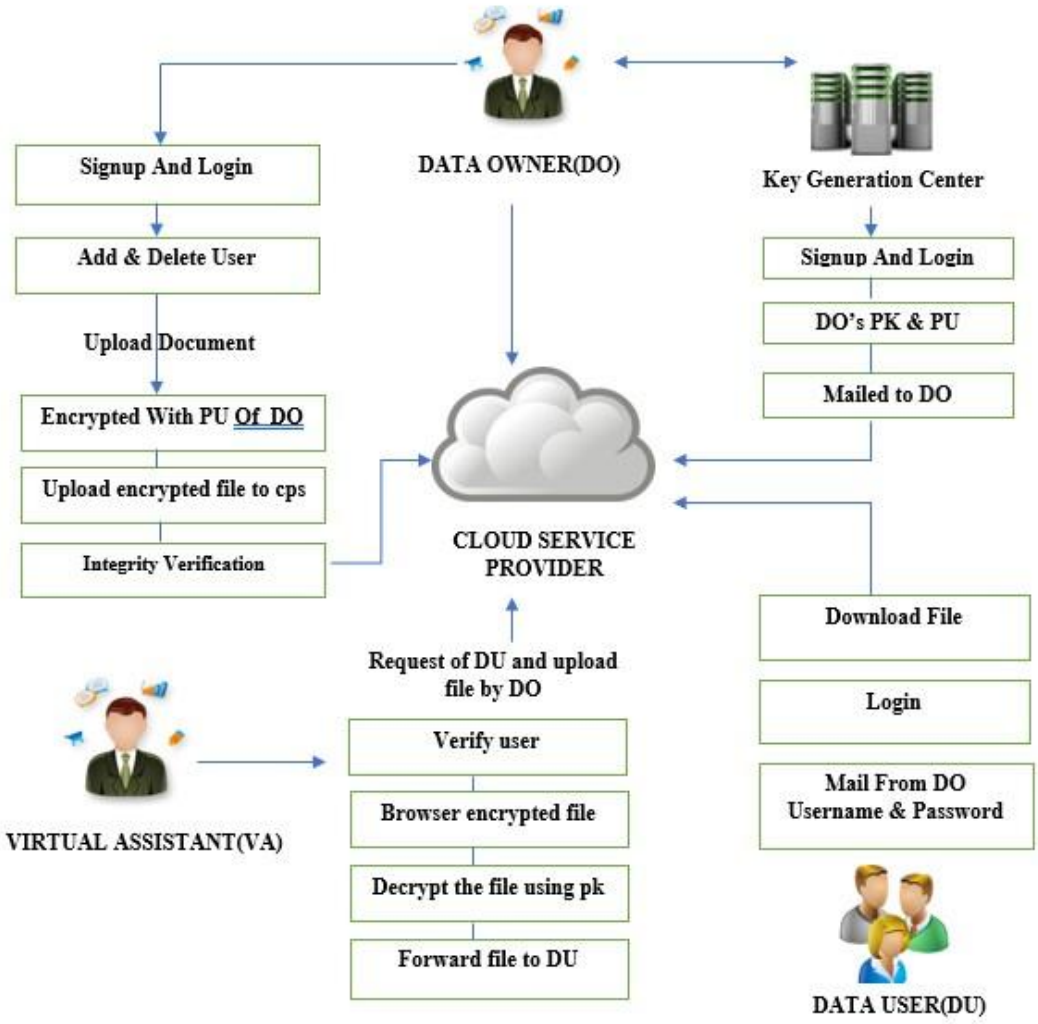
Data Retrieval and Response.:

The informant verifies the request's legitimacy. The data access token is distributed to the node service provider once VA confirms that the request's trapdoor is in the data connection keyword set. The final state is distributed as a transaction on the blockchain. The file is then decrypted with MKDO and re-encrypted with PKDU before being sent to the requested DU.

6.MIMIC MODEL:

The Mimic Model is nothing more than a DO replacement. When a user submits a request for data access, the blockchain's metadata is queried. The signatures of the data owner and the VA are used to verify the data's validity. If authentication is successful, a date is inserted, and the signed data is forwarded to the VA in a request for the real data. The data's associated metadata is obtained from the cache, and the ciphertext is retrieved from the CSP.The VA re-encrypts the ciphertext and provides the result to the user. With his private key, the user may now decrypt the ciphertext. By employing the user's signature, the blockchain confirms the user's legitimacy in advance. For auditing reasons, the timestamp is checked, and the request is logged on the blockchain.

5. WORK FLOW DIAGRAM



6. FUTURE SCOPE AND CONCLUSION

To track data updates, cloud databases should include a trustworthy authority control security mechanism. Cloud databases, in particular, are troublesome since they may be modified without the data owner's awareness. We present a secure homomorphic-based FHE data-sharing mechanism in a cloud computing environment to ensure data confidentiality, integrity, and privacy. The FHE technology enables secure data sharing by allowing data owners to store encrypted data in the cloud and share it with legitimate users quickly.Due to resource restrictions, a Virtual Assistant was used as a stand-in for the DO position to conduct the demanding calculations. The method also combines Cloud capabilities to efficiently distribute cached material and quick responses, hence boosting service quality and maximising network capacity. Then, we provide a blockchain-based system concept for flexible encryption data authorisation. It is possible to implement fine-grained access control, which can assist data owners in achieving acceptable privacy protection. The suggested model's study and results demonstrate how efficient our scheme is in comparison to other schemes. Furthermore, Blockcloud makes it possible for blockchain systems to adapt to changing networks with greater efficiency and scalability.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] B. Kaynak, S. Kaynak and Ö. Uygun, "Cloud Manufacturing Architecture Based on Public Blockchain Technology," in IEEE

Access, vol. 8, pp. 2163-2177, 2020, doi: 10.1109/ACCESS.2019.2962232.

[2] C. V. N. U. B. Murthy, M. L. Shri, S. Kadry and S. Lim, "Blockchain Based Cloud Computing: Architecture and Research Challenges," in IEEE Access, vol. 8, pp. 205190-205205, 2020, doi: 10.1109/ACCESS.2020.3036812.

[3] H. Wang and J. Zhang, "Blockchain Based Data Integrity Verification for Large-Scale IoT Data," in IEEE Access, vol. 7, pp. 164996-165006, 2019, doi: 10.1109/ACCESS.2019.2952635.

[4] H. -Y. Paik, X. Xu, H. M. N. D. Bandara, S. U. Lee and S. K. Lo, "Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance," in *IEEE Access*, vol. 7, pp. 186091-186107, 2019, doi: 10.1109/ACCESS.2019.2961404

[5] M. A. Rahman et al., "Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications," in IEEE Access, vol. 6, pp. 72469-72478, 2018, doi: 10.1109/ACCESS.2018.2881246.

[6] M. U. Sana, Z. Li, F. Javaid, H. B. Liaqat and M. U. Ali, "Enhanced Security in Cloud Computing Using Neural Network and Encryption," in IEEE Access, vol. 9, pp. 145785-145799, 2021, doi: 10.1109/ACCESS.2021.3122938.

[7] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," in IEEE Access, vol. 5, pp. 14757-14767, 2017, doi: 10.1109/ACCESS.2017.2730843.

[8] R. Awadallah and A. Samsudin, "Using Blockchain in Cloud Computing to Enhance Relational Database Security," in IEEE Access, vol. 9, pp. 137353-137366, 2021, doi: 10.1109/ACCESS.2021.3117733.

[9] S. Wang, X. Wang and Y. Zhang, "A Secure Cloud Storage Framework With Access Control Based on Blockchain," in IEEE Access, vol. 7, pp. 112713-112725, 2019, doi: 10.1109/ACCESS.2019.2929205.

[10] Y. Miao, Q. Huang, M. Xiao and H. Li, "Decentralized and Privacy-Preserving Public Auditing for Cloud Storage Based on Blockchain," in IEEE Access, vol. 8, pp. 139813-139826, 2020, doi: 10.1109/ACCESS.2020.3013153.