ISSN No:-2456-2165

In the Cloud, a Review of the Access Control Framework with Privacy Protection (Supported by 5g Networks) using Blockchain

Subramanya V. Odeyar
Post Graduate Student,
Department of Computer Science and Engneering ,
Basaveshwar Engineering College, Bagalkot -587103, India

S.V.Saboji
Professor,
Department of Computer Science and Engneering ,
Basaveshwar Engineering College, Bagalkot -587103, India

Abstract:- Using the cloud, businesses may share and access computer resources on-demand from anywhere in the world, creating new opportunities for data processing and services while simultaneously lowering computing and storage costs for end users. One of the most important cloud security solutions is access control, which is used by both businesses and people to secure sensitive data. The cloud's centralised access control method makes it easier for hackers or cloud internal management to tamper with or leak critical data. As a solution to this problem, the Auto Privacy Chain, a block chain-based access control framework with privacy protection, is reviewed with generic models: Block chain based architecture for demand and supply, Block chain based Internet of medical things for healthcare services, and Bitcoin Pay architecture. Auto Privacy Chain's access control, permission, and revocation design procedures offer customers with security.

Keywords:- *Cloud, Blockchain , Access control frame work.*

I. INTRODUCTION

A cloud computing service provides on-demand access to computer system resources, such as processing power, without the need for the user to actively administer the service. Large clouds often use numerous data centres to disperse their services. For coherence, cloud computing uses a "pay as you go" paradigm, which reduces capital costs but may potentially lead to unanticipated running charges for users who aren't aware of them. Data storage and back-up apps are utilised in cloud computing for corporate purposes as well as for educational and entertainment purposes, as well as for cloud computing art applications.

Access control is supported in both standalone and networked systems by the access control framework. The system in this article refers to "the computer or set of networked computers whose resources are secured by the access control service that is invoked using the authorization API."

Decentralized and distributed ledgers record the provenance of a digital item in blockchains. People who don't trust one another should be able to transmit vital data in a safe, tamper-proof manner with the use of a Blockchain.

Using its own crypto currency, ether, Ethereum's software platform allows users to send and receive value around the globe without the need for any third-party intervention. Many more functions are possible as well. Ethereum was designed to expand the utility of crypto currencies by allowing developers to create their own special applications. Unlike traditional apps, these Ethereum-based applications, called “decentralized applications,” or dapps, are self-executing thanks to the use of smart contracts. Smart contracts are code-based programs that are stored on the Ethereum Blockchain and automatically carry out certain functions when predetermined conditions are met. That can be anything from sending a transaction when a certain event takes place or loaning funds once collateral is deposited into a designated wallet. The smart contracts form the basis of all dapps built on Ethereum, as well as all other dapps created across other Blockchain platforms.

Generally access control technology in clouds has two major issues

- An attack may happen by externals
- It is one of the most common and major issue external attacker can hack to cloud data and can temper it and he may steal the confidential data.
- An attack may happen internally
- It happens rarely but too dangerous for any clients internal administrators can steal the data and take the advantages of the privileges he has.

Our proposed model is basically designed to overcome these two main disadvantages of the cloud services.

II. RELATED WORK

The cloud is used to store encrypted data in the first paper architecture for secure data storage (without being able to decrypt them). Our model's most notable new feature is the inclusion of important distribution facilities (KDCs). An technique called DACC (Distributed Access Control in Clouds) is used to distribute keys to data owners and consumers. In certain cases, KDC may provide access to specific fields in all entries [01]. Trust Cloud is a paradigm that addresses responsibility in cloud computing using a combination of technological and policy methods [02]. View control is also included, allowing only authorised users to access the encrypted data [03]. Concerns about how to keep cloud data secure have been raised as a result of this development. There are many well-known access control models, including role-based access control (RBAC), which uses two mappings to enable flexible restrictions and administration of data object rights: users to roles and roles to privileges in those roles. RBAC

ISSN No:-2456-2165

and role-based encryption (RBE) are combined in a single method called "RBE"[04]. Rather of distributing material based on specific hosts, the information centric networking (ICN) architecture holds promise for the Internet of the future. This makes the ICN a potential network architecture for the smart grid because of its congestion control and self-security features. [05] Multi-authority attribute-based encryption with quick decryption is the primary goal of this research. Allows any number of independent authorities to monitor characteristics, distribute secret keys, and decode the communication [06]. The IT industry's use of cloud computing is only getting started. Many dispersed systems are networked to supply software, hardware, and other resources through the internet in a cloud computing environment. Since this new paradigm compels people to secure the protection of their personal data, outsourced data security and privacy concerns are on the rise. Encrypting data before putting it on a cloud server is a logical technique to keep it secret [07]. Match-then-decrypt is a new approach that introduces a matching step before to the decryption phase [08]. The protection of cloud data is made possible by the use of data access control. Managing access to data stored in the cloud may be a challenge because of the vast volume of data that is outsourced [09]. In MeDShare, all activities on the MeDShare system are logged in a tamper-proof way [10]. Especially in cloud computing settings, where data owners have no control over key data characteristics, such as the physical storage of data and the restriction of its accesses, this problem is of particular concern [11]. Among other things, block chain is a remarkable technology that delivers compelling qualities regarding data integrity. It is possible to ensure the integrity and availability of data provenance by using blockchain technology [12], which may give tamper-proof records while also making cloud data responsibility more transparent. In the Internet of Things, access control poses significant issues. Due to the nature of the smart object, it is difficult to apply existing access control standards, while the inclusion of a strong and trusted third party to manage access control logic might impair user privacy [13]. In a cloud computing context, it is costly for the cloud server to secure user data access control via authentication, permission, and auditing [14]. With this in mind, we've proposed a Blockchain-based security architecture for distributed cloud storage, where users may encrypt their own files, then upload those encrypted data chunks to the P2P network nodes that provide free storage space [15]. From a contemporary security aspect, it is essential to keep data provenance in the cloud in an impenetrable, tamper-resistant way. The immutable distributed ledger service offered by block chain technology has emerged as a safe method for storing and sharing information. [16]. BPay, an outsourcing service fair payment framework based on the blockchain in cloud computing, is designed to provide safe and fair payment of outsourcing services in general without depending on any third-party, trustworthy or not. BPay's architecture, adversary model, and design objectives are initially proposed, followed by a description of the specific design elements [17]. Our solution offers an immutable record of all relevant security events, such as key creation, access policy assignment, update or revocation, access request, based on a block chain decentralised ledger. The cryptographic protocols I present [18] ensure the confidentiality of cryptographic operations using secret or personal keys.. I examined the most frequently referenced publications, most prolific nations, and most prevalent keywords using a systematic examination of literature acquired from the Web of Science service. The following five areas of research should be prioritised: "economic benefit," "block chain technology," "initial coin offerings," "fin tech revolution" and "sharing economy" [19]. Clustering analysis should also be performed. Confusion matrices in binary classification have grown so commonplace that individuals who analyse findings may not understand that alternative and more realistic methods of visualising data are available. When it comes to risk and return, this is especially true [20]. As a result of this, the need for a dedicated solution, in the form of patient-centered, personalised care - IoMT - has been expressed. IoMT helps to increase the accuracy with which diseases are identified as well as reduce errors and costs of care by utilising technology. Improves and accelerates clinician workflows and enables extreme connectedness thanks to improved automation and perceptions in the DNA of IoMT activities [21] by providing a proactive approach to health preservation. Operations Research and Mathematical measures, such as the cosine similarity index, are used in this work as well to assist us find the best way to allocate employment. These calculations are carried out using the Ethereum Block chain network's smart contracts [22]. Eventually, the transactions are validated and blocks are generated. Artificial intelligence (AI) may be utilised to perform complicated problems utilising cloud computing. It is used in a wide range of cloud-based applications that let users to share files and devices. It has a large user base. Security and protection of the system area are the main challenges in cloud computing, which have attracted a number of criminals who want to steal data or damage the system. [23] It is impossible to tamper with the data in any application that employs the block chain technology as a core foundation. A block chain is an open, decentralised, and digital ledger that stores transactional records known as blocks of the public in multiple databases known as chains across many networks [24]. We've devised a privacy-aware game model for cloud storage customers and suppliers. The replication dynamic equations are used to examine the model's evolutionary stability methods [25].

III. ISSUES AND CHALLENGES

A. *ISSUES*

- An external attacker interfering with the central server's allowed database and unlawfully accessing or stealing the resources saved by users in the cloud is a scenario that might occur.
- It's possible for a malevolent cloud system administrator to manipulate the authorization database in order to get unauthorised access to resources and manipulate the database to gain unauthorised access itself.

B. *CHALLENGES*

- Creating a system that give access security to the cloud system to access resources after ensuring the authentication permission

- Creating a cloud security with the integration of **Block chain** system.
- Authenticating user requests in the Blockchain chains.
- Resource Publication.

IV. METHODOLOGY

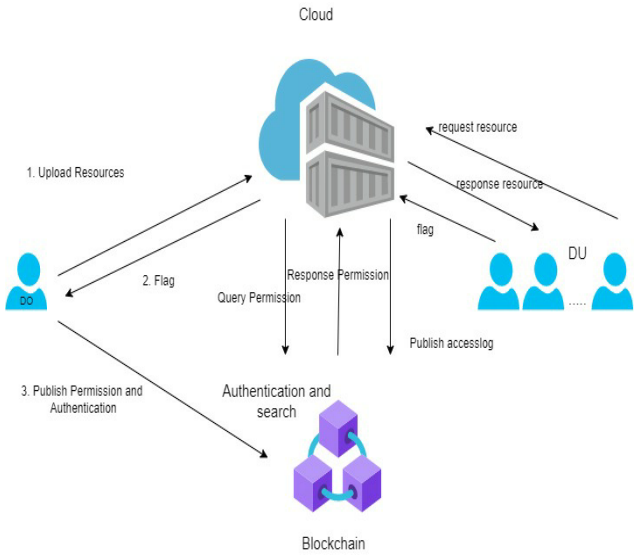

Fig. 1: Architecture Model

- **Cloud:** Authentication and data storage are provided for users via this application. By using Blockchain, the Cloud decides who has access to DU or DO.
- **Blockchain:** In the same way that we utilise the distributed database as an authorization policy database for access control, it is open, tamper-proof, and irreversible.
- **DO:** Resource access permissions are published on Blockchain when they have been uploaded to Cloud by DO.
- **DU:** If Cloud gives DU permission to access the resources, DU may do so.

It's assumed that the cloud can be trusted in terms of its software and hardware, but not in terms of its security architecture (SA), which is why we call it "semi-trusted." The trustworthiness of the blockchain is presumed. First, DO uploads the resources to the Cloud, and then publishes registration transactions in the Blockchain to verify the authenticity of the data. Sending a request to Cloud, DU searches Blockchain, and Cloud returns a response based on whether the request has been granted permission.

V. SYSTEM MODEL

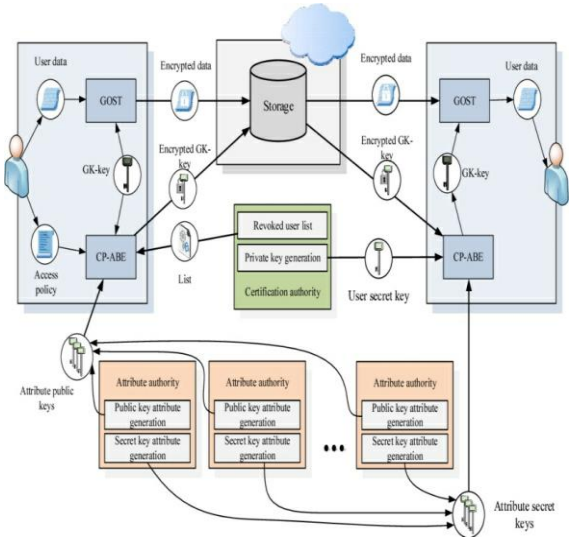

Fig. 2: System Model.

System model is designing access or share control by using cloud and Blockchain services. Data owner will upload file and then give access to Data user and this access details will be stored at Blockchain and encrypted file will be stored at Cloud Server. Only genuine users can request access details from Blockchain and by using those details Data user can request to GOST for file access.

The above model access can be provided via DIRECT and INDIRECT way. Direct means data owner authorizing some users to access his file and indirect means authorized users can give access to other users. Any time data owner can revoke or remove access from his file. After revoke no user can access his file.

In propose paper author is designing following modules

- Initialization: this module consist of 3 users such as data owner, data user and Cloud server
- Registration: Using the ISAVE Smart Contract feature, all users will be able to keep their personal information on the Blockchain. After registering, you may use Blockchain to record information about who has access to what resources. For each user, Blockchain generates a unique identification key.
- Cloud to Blockchain: Blockchain will get a registration request from the cloud.
- User to Blockchain: data owner will authorized data users to Blockchain, can upload/publish files and can performrevoke.

The cloud's centralised access control method makes it easier for hackers or cloud internal management to tamper with or leak critical data. Auth-Privacy Chain, a Blockchain-based access control architecture with privacy protection, is proposed as a solution to resolve this problem. An account address in block chain is used as a form of identification, and access control permissions for cloud-encrypted data are also re-defined in this process. Auth-Privacy Chain's access control methods include

ISSN No:-2456-2165

authorisation, revocation of permission, and a block chain-based Internet of Medical Things.

VI. BLOCK CHAIN BASED SOLUTION

The popular security solutions are related to the supply and demand, Internet of Things and Payment systems . These security solutions are very essential in real time applications. The following sections explore the authentication using block chain technology.

BLOCK CHAIN ARCHITECTURE FOR DEMAND AND SUPPLY

The architecture and functioning of the Blockchain may be broken down into two basic modules: supply and demand. For the most part, this module is intended for use by the workers themselves. Using an application interface, workers may access "Solidity" smart contracts and complete transactions. As soon as a transaction is complete, smart contracts are used by platform users to subjectively assess the building developers' projects. Workers' transactions and evaluations are entered into the ledger throughout this procedure. As a result, the job assignment procedure is implemented by the Demand Module. An aggregator's demand module implements the task allocation and is built particularly for that function. Supply module creates and stores the worker task allocation in the ledger. In order to keep tabs on the information, aggregators will examine the ledgers on a regular basis. In order to track worker information, smart contracts on the Blockchain are used by Aggregators to access the workers' personal ledgers. Finally, the system creates the outputs of the task allocation model and sends them back to the aggregator for further processing. Job allocation model findings are all recorded in a ledger.

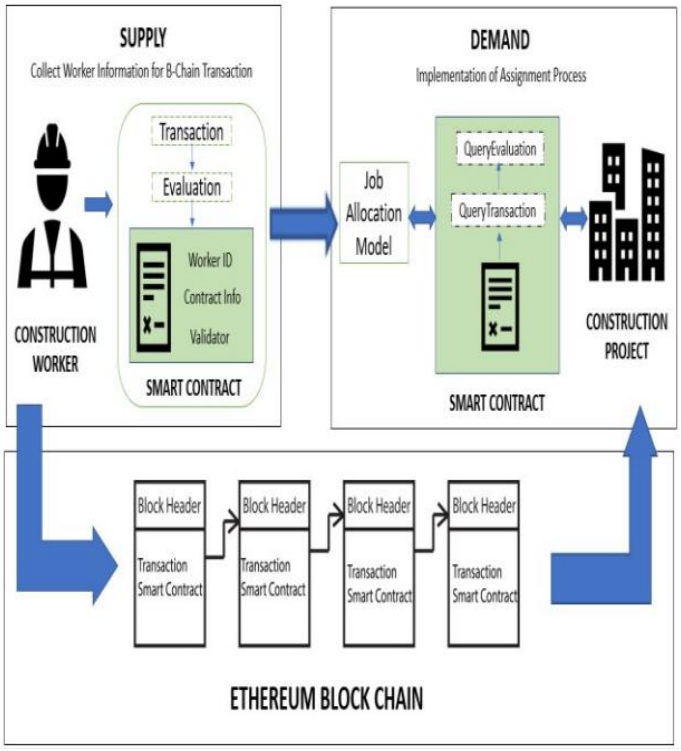

Fig. 3: Block chain Architecture.

BLOCK CHAIN BASED INTERNET OF MEDICAL THINGS FOR HEALTH CARE SERVICES

Service and Cloud providers' relationships with one other are likewise controlled by the Block Chain (see Figure 04). Data acquired by sensors, actuators, and tags will be accessible. Every piece of information pertaining to a patient is generated through gateways, which act as publishers. Permission levels (read/write/modify) are specified by the Publishers (using smart contracts). Access to the data created by publishers in the Cloud is granted to subscribers who are authorised to do so. Ethereum is a decentralised, open-source Blockchain platform enabling the development of new apps. The Blockchain validates and records every state transition that occurs on each node. It is possible to construct apps using EVM, the Ethereum Virtual Machine. Customizable consensus on the Ethereum platform (permissioned or unpermissioned) is used to design medical formats, rules, and state transition functions for medical transactional transactions. The uniformity and ease of use that Ethereum's smart contract framework provides make it the platform of choice. Solidity is the standard programming language for smart contracts, making it easier to create them. Two or more parties may engage into an agreement using digital contracts in a "smart contract". There are six ways that a blockchain-based Internet of Medical Things (IoMT) might benefit its users: by providing uninterruptible health care services that are available anywhere and are easy to use.

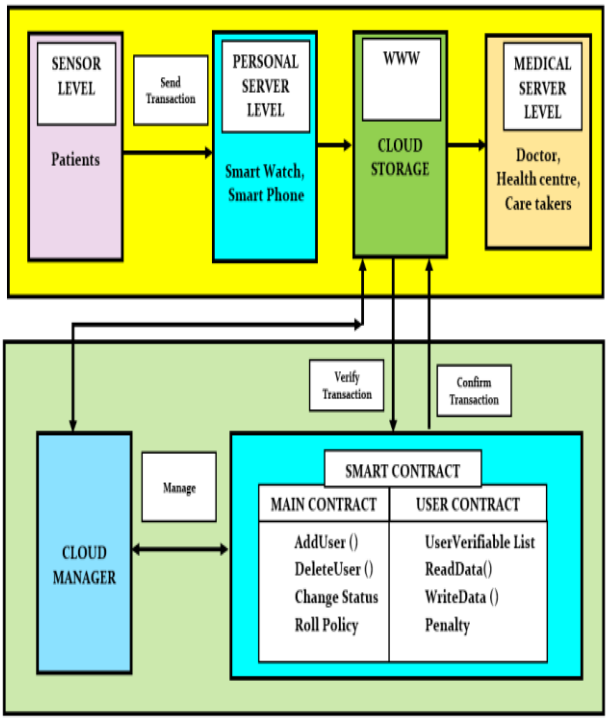

Fig. 4: Block chain based Internet of Medical Things for Health Care Services (BC IoMT U6 HCS).

ISSN No:-2456-2165

VII. THE SYSTEM ARCHITECTURE OF BPAY

Customers (i.e., users), servers (i.e., outsourced service providers) and a Blockchain make up the BPay system architecture shown in Figure 05. The terms "client" and "server" will be used interchangeably throughout the remainder of this work. Assume that C intends to use a S outsourcing service sv. Figure 05 shows just the most important aspects of BPay, so that the presentation may be kept to a minimum. The following are the specifics:

- Client C: C subscribes to sv through S as a user. S may provide a Blockchain-based preliminary service confirmation to C after enforcing sv. C issues a challenge to S in order to verify that sv has been implemented properly before making the payment. First, S guarantees that if S is evil, C will get adequate compensation in the form of deposits. Next, C and S work together to describe certain technical criteria in order to begin the service proof. By failing to offer a service evidence that matches the standards within a certain time limit, C might claim sufficient deposits from S. Keep in mind that repeated processes, including partial service implementation verification and proof, are used to achieve the proof start and service payment.
- Server S: Regulation enforced by S as an outsourced service provider is intended to generate service fees for C. S completes the Blockchain-based enforcement of sv and delivers a preliminary confirmation message to C after receiving the service subscription request from C. After receiving a challenge from C, S commits to the claim. To receive the service charge from C in the service payment phase before the specified time, S must complete the joint proof initiation process by providing a valid service proof.
- Blockchain: For example, the Bitcoin and Ethereum blockchains have been extensively embraced in practise as public Blockchains.

VIII. ADVANTAGES

- Creating a system that give access security to the cloud system to access resources after ensuring the authentication permission.
- Creating a cloud security with the integration of **Block chain** system.
- Authenticating user requests in the Blockchain chains.
- Cloud computing art apps, business applications, data storage and backup applications, educational applications, and entertainment applications all employ these model applications.
- As compared to other applications this application is economical.

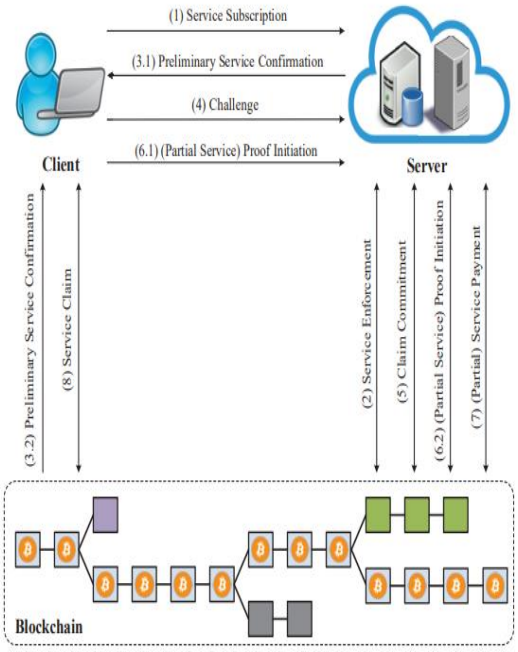

Fig. 5: The system architecture of BPay

IX. CONCLUSION

Internal and external assaults on standard cloud access control systems are quite possible since most of them use trusted centres and trusted administrators. Attackers can no longer get access to cloud resources illegally. To avoid assaults, a cloud-based access control architecture with privacy protections has to be improved. The user posts all transactions relevant to authorisation to the block chain. As a further definition of block chain transactions, we suggested the framework model connected to access permission and hash information. In cloud storage systems, data access control becomes a challenge due to the massive volume of data that is outsourced. As resources and services in the cloud are shared across many businesses, ensuring the security of these resources is a critical component of the cloud computing process. To safeguard cloud storage services from hackers, a higher emphasis on privacy protection and data security is essential. Customers no longer have to depend on third parties to verify the authenticity of the products they buy because of the advent of block chain technology.

ACKNOWLEDGEMENT

This work was supported by Funding for Design and Implementation of Security services in 5G Wireless Networks" by Karnatak State Council for Science and Technology under project CySek with Principal Investigator(PI) Dr. S. V. Saboji and Co-PI. Dr. S. M. Hatture.

REFERENCES

[1.] R. Sushmita, N. Amiya and S. Ivan, "DACC: Distributed Access Control in Clouds," in *International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11*, Canada, 2011.

[2.] K. L. K. Ryan, J. Peter, M. Miranda, P. Siani, K. Markus and Qianhui, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," in *2nd IEEE Cloud Forum for Practitioners*, Washington DC, 2011.

[3.] R. Sushmita, S. Milos and N. Amiya, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," in *12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, Canada, 2012.

[4.] Z. Lan, V. Vijay and H. Michael, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," in *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 12*, Australia, 2013.

[5.] Y. Keping, A. Mohammad, W. Zheng, Z. Di and S. Takuro, "A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid," in *IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT*, Tokyo, 2015.

[6.] G. R. Nikita,Dr.Nishant Joshi and R. Jay, "Improving Security in Multi Authority Attribute Based Encryption with Fast Decryption," in *7th International Conference on Communication, Computing and Virtualization*, Rajkot, 2016.

[7.] N. Suyel and R. Pinki, "Secure and efficient data access control in cloud computing environment: A survey," in *Multiagent and Grid Systems – An International Journal 12*, Silchar, 2016.

[8.] Z. Yinghui, C. Xiaofeng, L. Jin, S. W. Duncan, L. Hui and Y. Ilsun, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," in *ASIACCS*, Beijing, 2016.

[9.] R and A. M, "Survey on Access Control Issues in Cloud Computing," in *IEEE*, Pondicherry, 2016.

[10.] X. Qi, B. ,. Emmanuel, O. A. Kwame, G. jianbin, D. Xiaojiang and G. Mohsen, "MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain," in *IEEE Access*, Chengdu, 2017.

[11.] G. Edoardo, A. Leonardo, B. Roberto, L. Federico, M. Andrea and S. Vladimiro, "Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments," in *European Commissions H2020 Programme*, Southampton, 2017.

[12.] L. Xueping, S. Sachin, T. Deepak, K. Charles, K. Kevin and N. Laurent, "ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," in *17th IEEE/ACM International Symposium*, Rome, 2017

[13.] O. Aafaf, A. E. Anas and A. O. Abdellah, "Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT," in *Springer International Publishing AG* , Europe, 2017.

[14.] G. Jiale, Y. Wenzhuo, Y. ,. Kwok and Y. Xun, "Using Blockchain to Control Access to Cloud Data," in *Springer Nature Switzerland AG*, Switzerland, 2018

[15.] L. Jiaxing, W. Jigang and C. Long, "Block-Secure: Blockchain Based Scheme for Secure P2P Cloud Storage," in *Information Sciences*, Guangzhou , 2018.

[16.] K. T. Deepak, S. Sachin, F. Peter, C. A. Kamhoua and N. Laurent, "CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud," in *IEEE 11th International Conference*, Norfolk, 2018.

[17.] Z. Yinghui, H. D. Robert, L. Ximeng and Z. Dong, "Outsourcing Service Fair Payment based on Blockchain and its Applications in Cloud Computing," in *IEEE*, Beijing, 2018.

[18.] S. Ilya and Z. Sergey, "A Blockchain-Based Access Control System for Cloud Storage," in *IEEE*, Moscow, 2018.

[19.] X. Min, C. Xingtong and K. Gang, "A systematic review of Blockchain," in *Financial Innovation* , Chengdu, 2019.

[20.] W. LESLIE, "Information Theory, Kelly Betting, Risk, Reward,Commission, and Omission: An Example Problem in Breast Cancer," in *IEEE*, Austin, 2019.

[21.] J, S. ACHYUT, R. G. MUHAMMAD, G. J, H. QIAOZHI, W. ZHENG and Q. XIN, "Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly,Unflappable, Unblemished, Unlimited Health Care Services," in *IEEE*, Noida, 2020.

[22.] M. Hrishikesh, S. Mayur, L. ,. Hemadri, R. ,. B and N. S. D. V, "Design of Blockchain Aggregator for Benefit of Rural Workers using I.E Techniques," in *International Conference*, Bengaluru, 2020.

[23.] Sahar, A. Areej, A. Shahad, A. Moudi and A. Saad, "A Survey on Cloud S e curity Issues and Solution," in *International Conference* , Tabuk, 2020.

[24.] J. M, S. V, S. M and Dr.Sujatha , "A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain," in *IEEE Third International Conference*, Thiruvarur, 2021.

[25.] Z. Jianguo and C. Jinming, "Users' Payment Intention considering Privacy Protection in Cloud Storage: An Evolutionary Game-Theoretic Approach," in *Hindawi Complexity*, Shanghai, 2021.