IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCK CHAIN BASED ACCESS CONTROL MECHANISM HEALTH CARE SYSTEM ON CLOUD

[1]Subramanya V Odeyar, [2] S.V.Saboji

[1]Post-graduate student Basaveshwar Engineering College Bagalkot,
[2]Professor, Computer Science and Engineering, Basaveshwar Engineering College Bagalkot,
[1] Computer Science and Engineering Department,
[1] Basaveshwar Engineering College, Bagalkot, India

ABSTRACT

With the help of the cloud, companies may share and use computer resources whenever they need them from anywhere in the globe, opening up new possibilities for data processing and services while also bringing down end users' computing and storage expenses. Access control, which is used by both enterprises and individuals to secure sensitive data, is one of the most crucial cloud security solutions. The centralized access control technique used by the cloud makes it simpler for hackers or within cloud administration to alter or leak crucial data.

Keywords: Cloud, Blockchain, Access control frame work.

I. INTRODUCTION

Without the customer actively managing the service, a cloud computing service offers on-demand access to computer system resources, such as processing power. Numerous data centres are frequently used by large clouds to distribute their services. A "pay as you go" model is used in cloud computing for coherence, which lowers capital costs but could result in unforeseen running costs for customers who are unaware of them. Applications for data backup and storage are used in cloud computing for business, education, and entertainment as well as for cloud computing art applications.

Both standalone and networked systems can use the access control framework to control access. Any time the term "system" is used in this document, it refers to "the computer or set of networked computers whose resources are protected by the access control service which is invoked using the authorization API."

Blockchain structure is most simply defined as a decentralized, distributed ledger that records the provenance of a digital asset. The whole point of using a Blockchain is to let people in particular, people who don't trust one another share valuable data in a secure, tamper proof way.

The software architecture of Ethereum enables users to transfer and receive value globally without the involvement of any third parties using its own cryptocurrency, ether. As well, many additional functions are possible. Ethereum was created to increase the usefulness of digital currency by enabling programmers to make their own unique applications. These Ethereum-based "decentralised applications," or dapps, are self-executing in contrast to conventional apps since they make use of smart contracts. When specific criteria are satisfied, smart contracts, which are code-based programmes recorded on the Ethereum Blockchain, automatically perform specific tasks. This could involve lending money after receiving collateral in a defined wallet or sending a transaction when a specific event occurs. All decentralised applications (dapps) developed on Ethereum and other Blockchain platforms are built on top of smart contracts.

In general, there are two main problems with access control technology in clouds.

1. External parties may launch an attack. One of the biggest problems is that an outsider can hack into cloud

   data, corrupt it, and take sensitive information.
2. Internal attacks are possible. Rarely but very dangerously, internal administrators can steal data and abuse their rights, which allows them to take advantage of any client.

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

II. RELATED WORK

The Trust Cloud framework, which addresses accountability in cloud computing through technical and policy-based approaches, is presented in this study along with a discussion of the major difficulties in attaining a trusted cloud through the application of detective controls [02]. It also offers the additional capability of access control, which limits who can decrypt the stored data to authorised users only [03]. The crucial security issue of how to regulate and stop unwanted access to data stored in the cloud has been brought up as a result. Role-based access control (RBAC), which has two mappings—users to roles and roles to privileges on data objects—provides flexible restrictions and management. It is one of the most well-known access

control models. The integration of cryptographic methods with RBAC is characterised as the role-based encryption (RBE) scheme[04]. A proposed design for the future Internet is information centric networking (ICN), which distributes content based on named data rather than named hosts. Congestion control and self-security make the ICN a possible network design for the smart grid by enabling more scalable, secure, collaborative, and pervasive networking [05]. This paper's fundamental idea is to support multiple authorities in attribute-based encryption while also enabling quick decryption. Any polynomial number of independent authorities may monitor attributes, disseminate secret keys, and decrypt the communication using the multi authority concept [06]. This article suggests a cutting-edge method dubbed match-then-decrypt, in which a matching phase is added before the decryption phase[08]. This problem is particularly prevalent in cloud computing environments, where data owners have little control over basic features of their data, such as how it is physically stored and who has access to it. A remarkable new technology called block chain offers, among other things, attractive characteristics regarding data integrity [11]. Data provenance powered by blockchain technology can offer tamper-proof records, enable data accountability transparency in the cloud, and improve provenance data privacy and accessibility [12]. In IoT, access control faces numerous difficulties. Unfortunately, the restricted structure of smart objects makes it difficult to apply current access control standards, and the addition of a strong and reliable third party to manage access control logic could jeopardise user privacy. [13]. To ensure authentication, authorization, and auditing for access control of the user's data in a cloud computing environment is expensive for the cloud server [14]. I offer BPay, an outsourcing service fair payment framework based on block chain in cloud computing, in order to realise secure and fair payment of outsourcing services generally without relying on any third party, trustworthy or not. I initially make suggestions for BPay's system architecture, adversary model, and design objectives before describing the specifics of the design [17]. Our system provides an immutable log of all significant security events, such as key generation, access policy assignment, change or revocation, and access request, using a block chain-based decentralised ledger. In order to guarantee the secrecy of cryptographic operations involving secret or private keys, I propose a set of cryptographic protocols [18].Two-way confusion matrices in binary classification, along with corresponding metrics like sensitivity and specificity, have become so commonplace that reviewers of findings may not be aware that there are other, more accurate methods to depict data. This is especially true when concerns of risk and return are crucial [20]. The use of mathematical metrics, such as the cosine similarity index, to assess the similarity of two or more tensors and operations research to improve task allocation are also demonstrated in this paper. The Ethereum Block chain network's smart contracts, which are used to accomplish these computations, are used. Blocks are made after the transactions have been validated [22]. One interesting technique that uses artificial intelligence to address difficult problems is cloud computing. It is used in a wide range of applications that exchange information and devices using a cloud-based system. It serves a big user base. The biggest difficulties in cloud computing are related to protecting the system area and ensuring system security in the face of numerous attracters who want to steal data or cause system harm [23]. The data is "tamper resistant" in any application that uses block chain technology as a key building element. Considering that a block chain is a decentralized, distributed, and digital ledger that keeps track of open transactional information, known as blocks, across several databases, or chains, over numerous networks. [24]. Users and providers of cloud storage participate in an evolutionary game that takes privacy into account. The replication dynamic equations-based evolutionary stability techniques of the model are examined [25].

III. ISSUES AND CHALLENGES

ISSUES

1. An outsider accesses the trusted centre, tampers with the central server's authorised database, and gains unauthorised access to or steals the resources that users have placed in the cloud.
2. Because the cloud system administrator controls the permission database and has access to and control over the resources, a dishonest cloud system administrator might abuse this privilege to gain unauthorised access to the resources or manipulate the authorization database to do so.

CHALLENGES

1. Developing a system that grants the cloud system access security to resources after confirming the authentication permission
2. Integrating a blockchain technology to create a cloud security solution.
3. User request authentication in Blockchain chains.
4. Publication of Resources.

IV. OBJECTIVES

1. Avoid the hacking activities in the clouds.
2. Avoid hacker form tempering and stealing the confidential data.
3. Bring high trust on the cloud services by implementing Block chain system to build cloud securities.
4. To create access control authentication, authorization and authorization revocation in **Auth-Privacy** chain.

V. METHODOLOGY

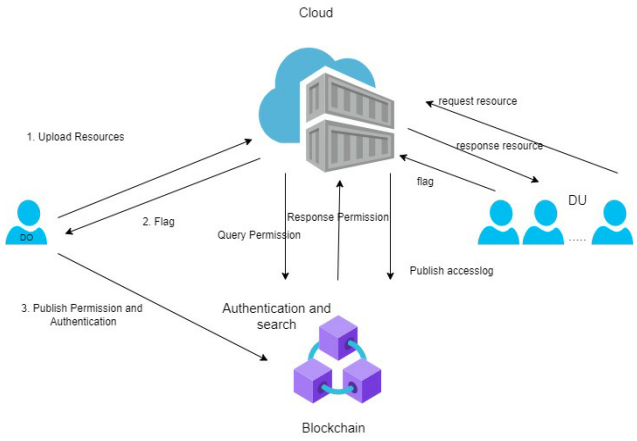

Figure 01: Structure Model.

Cloud: It gives users data storage and authentication. Blockchain is used by Cloud to determine access rights for DU or DO.

Blockchain: Similar to a distributed database, it is open, transparent, tamper-proof, and irreversible. We use it as an authorization policy database for access control.

DO: DO publishes the resource access rights to Blockchain and uploads the resources to the cloud.

DU: If DU has authorization from the Cloud, DU may access the resources.

While the cloud is expected to be trustworthy in terms of its software and hardware but not in terms of its security architecture, the blockchain is meant to be reliable (SA). DO initially uploads the resources to the Cloud before publishing registration transactions in the Blockchain to verify the accuracy of the data. DU makes a request to the Cloud and queries the Blockchain. Cloud chooses whether to answer with a yes or no.

SYSTEM MODE

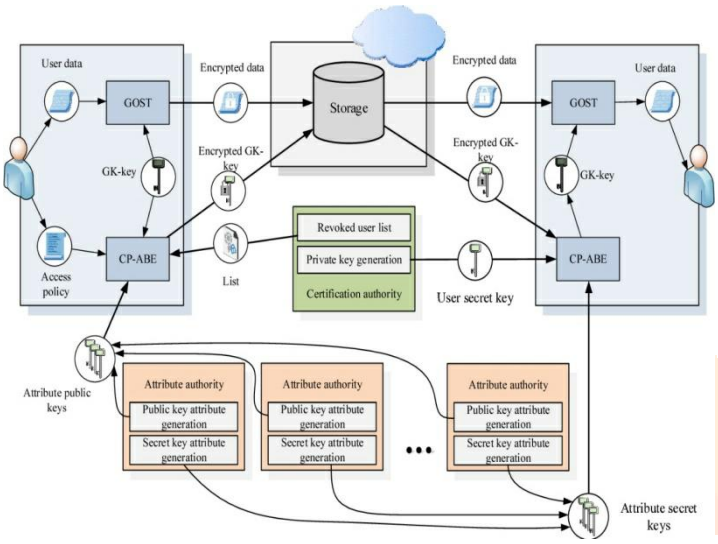

Figure 02: System Model.

Access or share control is designed into the system paradigm using cloud and Blockchain services. The data owner will upload the file, provide access to the user, and then store the access information on a blockchain. The encrypted file will be kept on a cloud server. Only legitimate users have access to Blockchain data, and using those details, users can ask GOST for file access.

Access to the aforementioned model can be made in both DIRECT and INDIRECT ways. Direct access to a file means the owner of the data has given some users permission to access it, whereas indirect access occurs when individuals who have access can provide it to others. The owner of the data has the right to cancel or delete access at any time. No one can access a user's file after revocation.

The author of the proposed paper is creating the following modules.

1) Initialization: There are three users in this module: the data owner, the data user, and the cloud server.

2) Registration: All users will be able to maintain their personal data on the Blockchain using the ISAVE Smart Contract feature. You can use Blockchain to keep track of who has access to what resources once you've registered. Blockchain creates a distinct identification key for each user.

3)Blockchain will receive a registration request from the cloud in step three.

4) User to Blockchain: The owner of the data will grant permission for users to upload/publish files and to execute revoke.

The centralised access control mechanism of the cloud makes it easier for hackers or employees of cloud administration to change or leak important data. Auth-Privacy Chain, a Blockchain-based access control architecture with privacy protection, is the suggested solution to this problem. Using a block chain account address as a means of identification, access control constraints for cloud-encrypted data are also redefined. Auth-Privacy Chain employs a variety of access control techniques, including authorization, permission revocation, and an Internet of Medical Things powered by a block chain.

ADVANTAGES

1. Creating a system that, after validating authentication permission, provides the cloud system access security to resources.
2. Integrating a blockchain technology to create a cloud security solution.
3. User request authentication in Blockchain chains.
4.This application is cost-effective in comparison to other applications

VI. RESULTS

To avoid the hacking activities in local server, I introduced etherium along with smart contracts integrated with block chain.

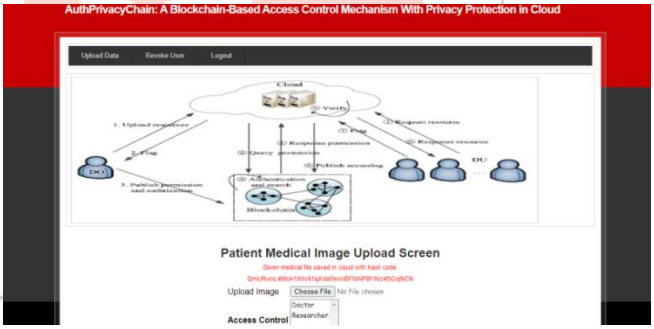

Figure 03(a): Data owner allow the access to the doctor 1

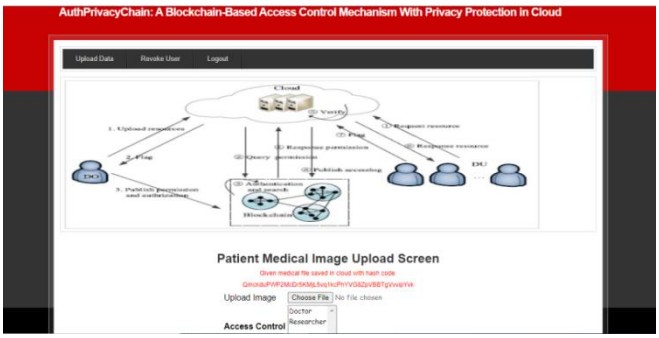

Figure 03(b): Data owner allow the access to the doctor

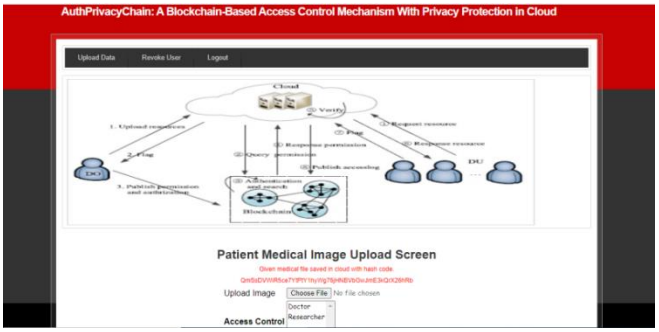

Figure 03(c): Data owner allow the access to the doctor 3

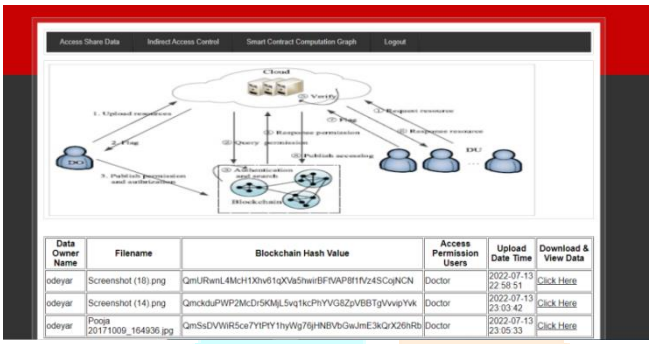

Figure 04: Data owner allow access permission for data users

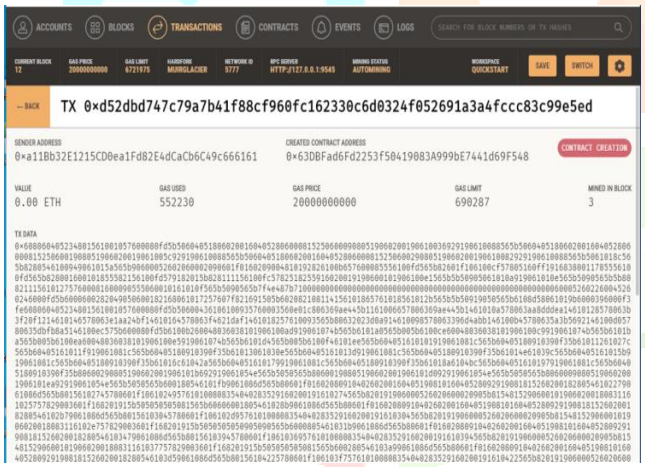

Figure 05: Contract is created in block chain through access control mechanism

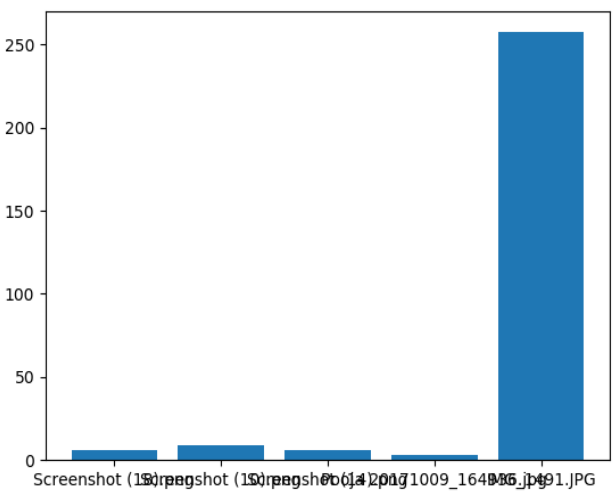

Figure 06: Block chain Total computation Time for Storage and access permission from data owner

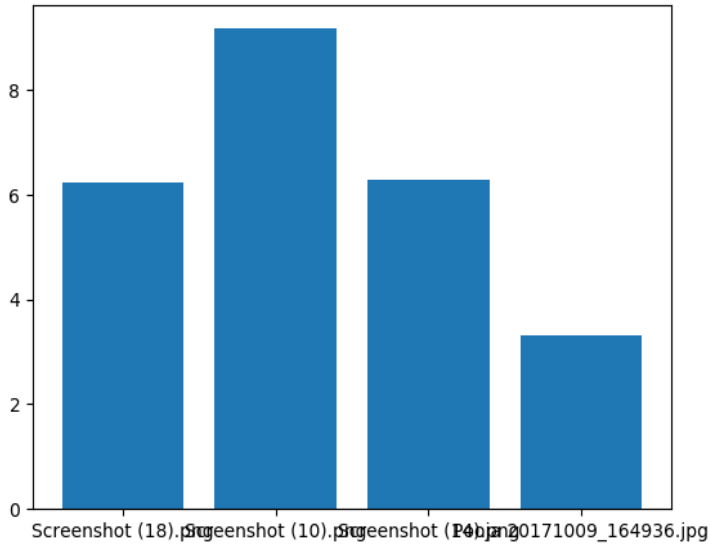

Figure 07: Block chain Total computation Time for Storage and access permission from data user

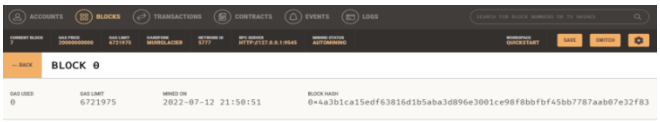

Figure 08: Smart contract and block chain in initial stage

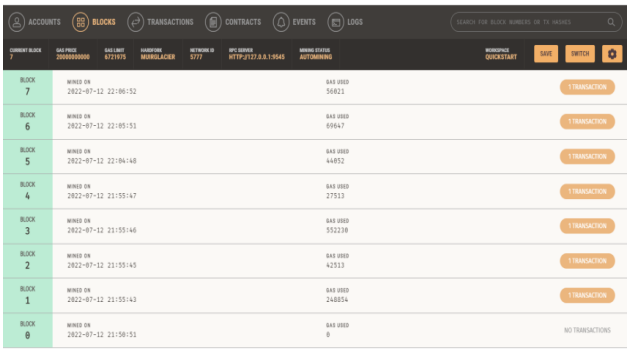

Figure 10: Smart contract and block chain in final stage

VII. CONCLUSION

Since the majority of typical cloud access control solutions use trusted centers and trusted administrators, internal and external attacks are very likely. Attackers can no longer gain unauthorized access to cloud resources. Cloud-based access control architecture with privacy protections has to be developed to prevent attacks. All transactions necessary for authorization are posted to the block chain by the user. We offered the framework model coupled to access authorization and hash data as an additional definition of block chain transactions. Data access management in cloud storage systems is difficult because of the enormous amount of data that is outsourced. The security of these resources is a crucial step in the cloud computing process because cloud resources and services are shared by numerous enterprises. A greater focus on privacy protection and data security is necessary to secure cloud storage services from hackers. Due to the development of block chain technology, consumers are no longer required to rely on other parties to confirm the legitimacy of the goods they purchase.

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.

] C. 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] I. 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] A. 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.