A Block Chain-Based Security Sharing Framework with Fine-Grained Access Control for Personal Data

Ashutosh Lanjewar[1], Sujata Helonde[2], Dipali Pethe[3], Ankush Sahu[4]

[1,2,3]Assistant Professor, Department of CSE J D College of Engineering & Management, Nagpur

[4]Research Scholar Department of CSE J D College of Engineering & Management, Nagpur

ABSTRACT:

Privacy protection and open sharing are important data organizations in the artificial intelligence (AI) stage. “The current solution is divided into a data management distribution platform and users upload their own data to the cloud server for storage and distribution. However, when users upload files to the server, they lose their personal data, and security and privacy become an important issue”. Data encryption and orchestration has almost solved this problem and has acquired new capabilities to protect private data on cloud servers. However, it still relies on the trust of third parties such as cloud service providers (CSPs).

“In this paper, we propose a blockchain-based personal information and security system referring to the BSSPD concept, which combines blockchain, ciphertext expert attribute-based encryption (CP-ABE) and Interplanetary File System (IPFS) to solve this problem. In this answer, the data enforcers encrypt the combined data and store it in IPFS, which by definition has many branches. The address and decryption key of the shared data will be encrypted using CP-ABE according to the instructions of the supervisor, and the data owner uses the blockchain to publish the data file and issue the key for the operator's data file. Personal data workers who control access rights can download and identify data. Data owners have full control over access to their data and BSSPD supports deletion of certain user data without affecting others.”

To protect the confidentiality of operator data, keywords in ciphertext are used when storing data. We have confirmed the credibility of BBSPD and simulated our theory on the EOS blockchain, proving that our knowledge is necessary. At the same time, we use computational analysis of storage and computational loads to determine the efficiency of BSSPD.

1. INTRODUCTION

“The development of 5G and IoT technology offers many opportunities for rapid use of artificial intelligence (AI). At the same time, data security and privacy protection have become paramount considerations in data sharing and sharing. Powerful data mining and analysis poses a threat to self-defense. Traditionally, most people choose to outsource to cloud servers to share and publish information. However, much of the data stored in the cloud is sensitive, especially those generated by IoT devices that interact with people's lives. These documents have their own characteristics and may contain personal information such as life, work, health; It will cause serious personal problems when personal information is stolen or illegally associated with the identity of the owner. Therefore, integrating data and creating value while ensuring data security and privacy has become a major challenge for all businesses today.

Today, researchers have proposed many security methods in the cloud environment [1-9]. These ideas seem to address security and privacy concerns in the data sharing process. However, these solutions share a common model: they rely on cloud service (CSP). They consider CSPs to be trusted third parties and their security models assume that CSPs are semi-trusted; this means that CSPs may want to know the information but not interact with it. This means that the following situations are always unavoidable. (1) CSP itself may use users' personal information or internal staff will keep users confidential. Although some methods, such as attribute-based encryption algorithms, may use user-centric, user-defined access rights, these methods still require a trusted third party to generate and manage user keys. The possibility of conflict between trust sites cannot be ruled out.” (2) All this will cause the data subject to fail to understand the accuracy of their data when uploading their data to the cloud server. Solar panel. Critical points of failure can often protect users who use cloud services from their data. CSP can use disaster recovery backup to improve data security and service stability. However, some clarifications, such as rules, are possible.

(3) will prevent users from using the cloud to access their data. These costs increase, as do the costs of CSPs and the construction of management platforms.

End users pay for CSP operating costs. The blockchain is a point-to-point connection that can prevent the data collected by the Internet of Things from being transmitted by third-party service providers, increasing data transmission and reducing transmission. To ensure that this data is stored and transmitted to make it fair, efficient and accurate, access control has also become an important research topic for managing the security of the sharing of IoT data.

This is why many researchers are combining blockchain technology with existing governance structures to run their research projects. Ziskind and Nathan [8] proposed a Decision Access Control (DAC) model to manage off-chain data by accessing the authority of the blockchain.

Cruz et al. [9] Using blockchain in a role-based control model (RBAC) to handle business access and perform business-wide authentication of user locations Maisa et al. [10] extended the Controlled Behavior (ABAC) process to replace traditional databases with blockchains to store code and control access to code. However, the above method is only suitable for special cases, and access control is private, so it is not suitable for one-to-many encryption in the Internet of Things.

2. LITERATURE SURVEY

Our system and user information and policies. We use JAR File sharing is an attractive service provided by cloud computing platforms as its simplicity and affordability. As a method that can provide good data sharing, behavioral encryption (ABE) has received a lot of attention. However, most of the current ABE solutions have disadvantages such as high overhead and poor data quality, which greatly affects the technical support services of the mobile service. Fine grained cloud data sharing, the high performance of the data manager at the end, as well as the problem of data model privacy is not solved.

This article talks this stimulating matter by suggesting a new system- based data distribution for mobile users with limited resources in cloud computing. The proposal removes much of the work by adding a different system as well as moving some of the encryption calculation offline. Additionally, the general ciphertext testing phase precedes the decryption time, which removes much of the computational burden from illegal ciphertexts. For information security, the chameleon hash function is used to generate real-time ciphertext, and the offline ciphertext is blindly obtained until the last online ciphertext. The future arrangement has established to be protected against modification of the chosen ciphertext attack, which is widely accepted as a security standard. performance reviews show the plan is safe and effective

Ensuring distributed accountability for data sharing in the cloud:

Cloud computing enables the easy provision of large-scale services on demand over the Internet. One of the main features of cloud services is the remote processing of user data, usually run on unknown machines or by the user. While enjoying the conveniences brought by this new technology, users are worried about managing their information, especially financial and health information, which will likely be the main problem for air use. To solve this problem, in this article, we propose a new database to track the actual usage of users' data in the cloud, which has a huge impact on accountability. Specifically, we propose an object-centric approach that both turns off programmability for the design of animated objects and ensures that access to user data is for automatic and automatic import of native JARs. To enhance user control, we also provide a distributed analytics system. We provide extensive research that demonstrates the effectiveness and efficiency of the plan.

Key-aggregate cryptosystem for scalable data sharing in cloud storage:

Data sharing is an essential part of cloud storage. In this article, we will show you how to share data in the cloud with others in a safe, efficient and flexible way. We describe a new set of public-key cryptosystems that generate ciphertexts large enough to execute code that decrypts entire sets of ciphertexts. What's new is the ability to combine secret keys into a single key, but change the function of all keys together. In other words, the administrator can still provide a key combination that facilitates the selection of ciphertexts in cloud storage, but non-light encrypted data remains confidential.

Collective data-sanitization for preventing sensitive information inference attacks in social networks:

Authours: Zhi Peng Cai, Zaobo He, Xin Guan, and Yingshu Li,

- Posting information on social networks may violate the user's privacy. User profiles and friendships are personal in nature. Unfortunately, it is likely to extrapolate delicate data from published information using data mining techniques. Therefore, network data must be deleted before sending. In this article, we explore the use of social networks to link negative attitudes and social behaviors. We map this problem to an integration problem and present the integration model. In our model, attackers use user information and networks to guess important information about victims in published social network data. To protect against these attacks, we provide an anti-virus system that manages data usage and relationships. This scheme can be used in many ways to process information and damage friendships. We show that we can easily reduce candidates' understanding of sensitive information while reducing exposure to useless information in social networking datasets.

This is the first project to integrate with various data processing and collaboration to prevent social attacks.

A Private and Efficient Mechanism for Data Uploading in Smart Cyber-Physical Systems:

Authours: Zhipeng Cai1, Xu Zheng1,2, Student Member

- Data transfer in intelligent cyber-physical systems to provide effective access to various parts of the physical world facing new challenges in energy conservation and privacy protection. It is important that participants use as little energy as possible when uploading files. However, even the mere discovery of electronic devices can reveal private information, especially if participants provided more details than before. In this paper, we propose a new mechanism for uploading information to intelligent cyber-physical systems that takes into account both energy conservation and personal protection. The system enhances the utility of scheduling for data uploads by revealing additional details, while protecting privacy by hiding the unusual behavior of participants. Deriving the optimum loading scheme has proven to be NP-hard. Therefore, we proposed a heuristic algorithm and evaluated its performance. Analyzing the results on real-world data shows that our proposed method achieves comparable results with the best results.

Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big data:

Authours: Xiaokang Zhou, Wei Liang

Education big data is a large collection of educational materials, teaching materials and collaborations that have attracted the attention of companies and education worldwide. The widespread use of social media has made it easier than ever for researchers to conduct collaborative research and share academic knowledge in collaborative learning. In this study, we focus on information recognition and multi-network analysis based on clustering of large-scale data. Teaching methods are introduced and interpreted to measure the effect of social work, social cognition and cognitive exercise action based on three relationships: researcher-researcher, researcher-text and sentence-sentence. There are many schools (eg., researchers, and equipment) in a networked network. An enhanced restart-based random walk (RWR) algorithm was developed in which time-varying learning effects are redefined and evaluated in a social setting, providing Collaborative research navigation for researchers and future research. Experiments and evaluations were conducted to demonstrate the effectiveness and efficiency of our proposed method in big data research using DBLP and ResearchGate databases.

A Differential-Private Framework for Urban Traffic Flows Estimation via Taxi Companies:

Authours: Zhipeng Cai1, Xu Zheng2, Member, Jiguo Yu3,4,5,

- Due to the remarkable progress in public transport, taxis can now serve the public in the city. Individuals, city planners and taxi companies themselves will benefit greatly from this experience. Blindly publishing these details, however, could jeopardize the privacy of taxi companies. Some of the sensitive information of the business itself, passengers and drivers can be leaked. Therefore, in this study, we present a new shared transportation system for taxi corporations that together considers the secrecy, income and integrity of participants and is kept confidential. The framework permits corporations to share the size of their taxi fleet and extract information from statistics. Since publicly available information can be retrieved by individuals and third gatherings such as the government, two algorithms have been proposed to provide shared plans in various situations. Different privacy measures are used to protect subtle data of taxi corporations. Lastly, both processes are authenticated on practical information tracked across numerous markets.

Bitcoin: A Peer-To-Peer Electronic Cash System:
“The cash-only model allows online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide a partial solution, but the benefits will be lost if a trusted third party is still required to avoid duplication. We propose a method to solve the double-spending problem using a peer-to-peer network. Network timestamps are managed by hashing them into a continuous chain of hash-based proof-of-work records, creating a record that cannot be changed without the first reboot. The longest chain not only proves the observed events, but also proves that it comes from the largest pool of CPU power. As long as most of the CPU's power is controlled by conflicting networks against the network, it will form the longest chain leading to the attacker. The network itself should have a small sample size. The most effective message is broadcast, and nodes can leave and rejoin the network at any time, accepting the longest proof-of-work as proof of what happened when they disappeared.”

3. PROPOSED SYSTEM

Over the next few years, many researchers developed and implemented blockchain management systems to protect privacy and security while sharing information. “Liang et al. A user health data sharing model [20] is used with Hyperledger Fabric, where cloud storage is used as a data storage and the blockchain ledger is designed to handle issues and updates. At the same time, use member management services provided by Hyperledger Fabric to strengthen user authentication and channel design to protect user privacy. Fan et al.
They proposed an efficient blockchain-based sharing system, focusing on mobile data sharing and privacy protection in the 5G era [21]. The main idea is to identify the types of transactions on the blockchain to represent access rights. The rules include the person requesting access, the provider, the visitor, the start and end time of the access authorization and is the access control model. Zhang et al. He proposed a blockchain-based data sharing project for AI-driven network operations [22].

The concept creates two types of connections, where DataChain is used as a data management tool and BehaviorChain is used to store input data and ensure it is not tampered with. They are divided into four levels. Zhou et al. A blockchain-based knowledge sharing system [23] has been proposed to solve the ineffectiveness of knowledge sharing during academic analysis. Schema uses Access Control Language (ALC) to control access to data stored on the chain.
It needs to define access rights on the blockchain for all users and resources. Patel proposed a blockchain-based shared image [24] that uses the blockchain as data storage and allows patients to authenticate their access rights. They point out that this approach protects information from unauthorized parties, but privacy and security have not been reviewed. Tan et al. A blockchain access control system called BacCPSS has been proposed for Big Data in Cyber-Physical Social Systems (CPSS) [25].

BacCPSS uses blockchain addresses as user identifiers and controls user access to smart contracts to ensure that only authorized transactions can be executed in the matrix. The access control method from the instructions above requires multiple access rights on the chain, otherwise there will be no effective control. Neither access control matrices nor RBAC are suitable for distributed environments such as blockchains.”

ABE is recognized as the most suitable tool for solving data security and privacy issues in a distributed environment. Therefore, researchers recently managed to access information about the blockchain using ABE. Jemel and Serhrouchni proposed an access control system [26]. For the first time, researchers have used the CP-ABE algorithm using blockchain nodes to verify the authenticity of user codes. The program creates two types of operations: SetPolicy and GetAccess. However, it does not use smart contracts and in fact this solution does not meet the increasing demand. Sun et al.

A secure and unified electronic medical record system is built on ABE and blockchain [27], enabling better management. Physicians use ABE to encrypt patients' medical records and store them in IPFS. However, it does not use smart contracts either. It only reports a limited number of ABE stores on the exchange and cannot recognize more complex transactions. Wang et al.
proposes a shared method where users share secret keys [28]. It gives data owners more control over their data. At the same time, the Ethereum smart contract is used to return the ciphertext content. However, it requires a lot of communication from the user and most importantly, it does not use permission to delete. Pournaghi et al. proposed a secure and efficient sharing strategy based on blockchain and ABE called MedSBA to collect and store medical information [29]. It enforces renewal and cancellation policies by issuing new policies that reflect previous changes, but this makes it equivalent to users who don't want to revoke keys.

4. SYSTEM ARCHITECTURE

Architecture is a graphical representation of data from information systems that models processes. It is used as a preliminary step in the development of the process and does not require further explanation. The architecture specifies how the data is accessed and output from the system, how the information is processed by system, where the information is kept. Unlike standard scheduling, which focuses on flow control, it does not show information about the timing of the process or how well the process is performing or stabilizing. Logical data flowcharts can be drawn using four simple symbols i. for example, it represents process and data storage. We use these symbols as Gain and Sarson symbols. Boxes indicate external locations, curved boxes indicate processes, rectangular boxes indicate data storage, and arrows indicate data flow.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, Journal Volume 11 , Iss 11, Nov 2022

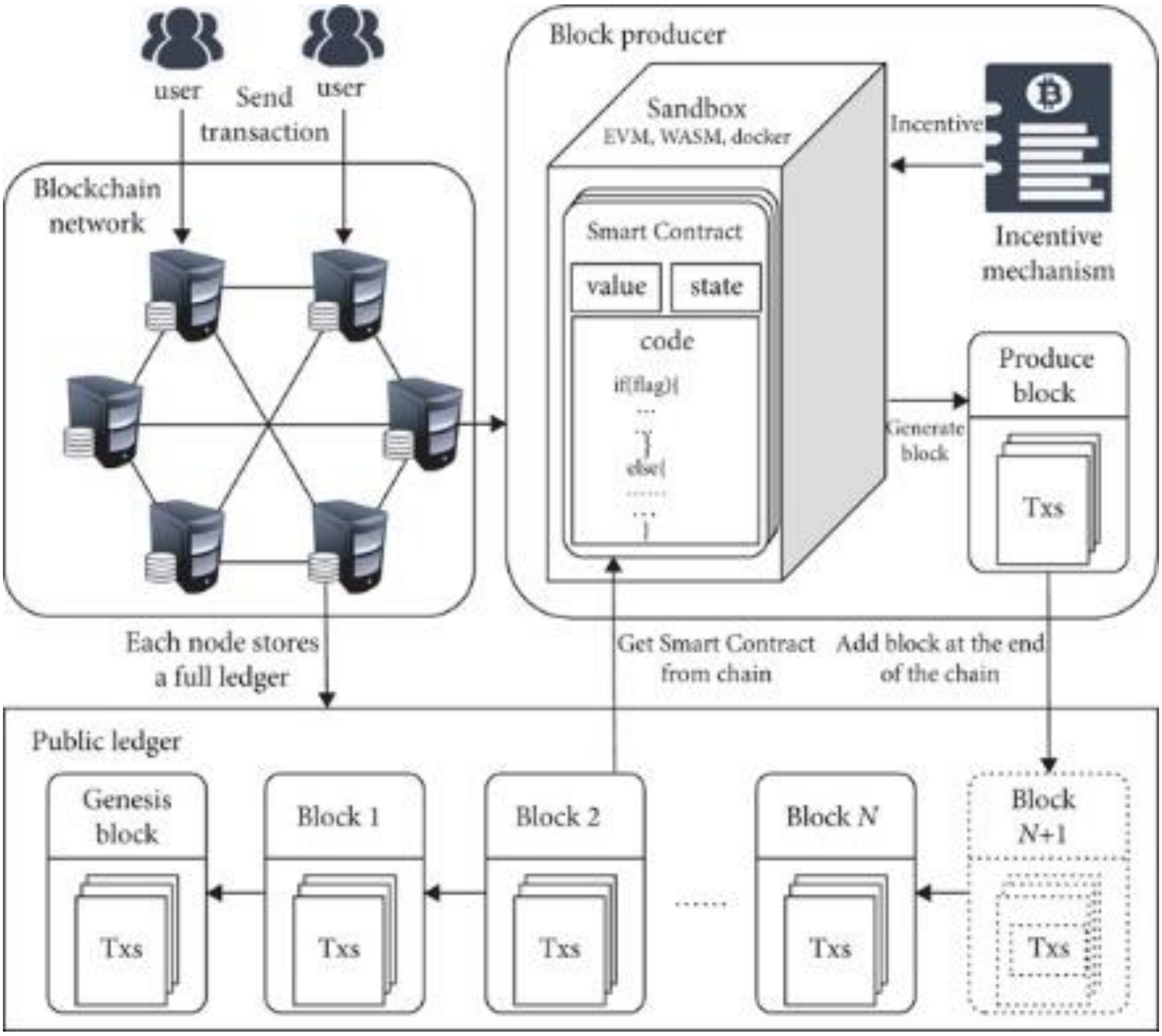

Fig-1 Proposed Architecture Framework

In the blockchain, smart contracts are the rules based on the trust environment of the blockchain to be executed while enabling blockchain to be used in many transactions. The working mechanism of smart contracts founded on the Blockchain is shown in Figure 1. From a higher perspective, the blockchain can be thought of as a state machine of transactions and the information population is the state of the world, starting with the Genesis Block. Users can create a transaction and publish it via any part of the blockchain net. All block generators will do the same job after receiving the change.

Because of the deal, each of the ends will the evaluation framework ensures that every collaboration meets the prerequisites. Accuracy and consistency of test procedures. An example of a testing framework is an integration testing framework. Presentation and efficiency-based assessment framework that includes planning and integration

ALGORITHM

Algorithm: Validating a Data Query Request and Updating Token Ledger according to:
Input: string token, User details as UD, server as SV
Output: create user and login details

```
Start
Initialization: rec ← null, out ← rejected
Enter user details.
S ← user verification function
D ← SaveTheDetails(S)
if  S-success at that time:
    rec ← token ledger(Token)
    if rec.(DO_ID )= UD and rec.(AC_ID) = UD at that time:
        rec[UD]==SV
        Read and share data
        Token_Ledger[Token].Expires In = Time.Now()
    else:
        Out← Return(string Token)
Return Out
```

Algorithm 1. Proposed Algorithm

5. CONCLUSION AND FUTURE SCOPE

Conclusion

Currently, cloud storage will render users' data unusable due to energy majeure (Natural Disasters, Government censorship, etc..). (ABE) Technology and ciphertext discovery encryption technology were imperative Technologies for Solving Data secrecy and effective admittance controller issues. However, traditional ABE solutions require a reliable private generator (PKG). The private key generates by (PKG) for user non supple sufficient, which can lead to key misuse, leakage of user information, etc. may cause. Old-style exploration encoding systems need Cloud servers to Perform an honest exploration, but practical use, Cloud servers can yield invalid or even useless results to conserve resources.

Future Scope

As future studies, different designs will be compared to measure performance with different BC platforms. Here, the distribution of the chain, where some storage will be wrong, must be occupied into accounts. Extra Efforts should be made to address the dearth of trust in the systems in all decentralized systems. Controlling the use of fine-grained objects, where SC uses an intelligent power creator in a context-sensitive manner, is a auspicious area of investigate. Finally, since the data query is only about storing thoughts (CRUD-Operations Only), (BC) may be used for computing power, which means BC nodes keep track of the safety of the number of workers counting, processing and processing data. I return it. Application data instead of raw data.

6. REFERENCES

1. G. Venkatadri, A. Andreou, Y. Liu, A. Mislove, K. P. Gummadi, P. Loiseau, and O. Goga, “Privacy risks with facebook’s pii-based targeting: Auditing a data broker’s advertising interface,” in 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018, pp. 89–107.
2. G. Zyskind, O. Nathan et al., “Decentralizing privacy: Using blockchain to protect personal data,” in 2015 IEEE Security and Privacy Workshops. IEEE, 2015, pp. 180–184.
3. H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards blockchain-based auditable storage and sharing of iot data,” in Cloud Computing Security Workshop. ACM, 2017, pp. 45–50.
4. R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, “Blockchain for large-scale internet of things data storage and protection,” IEEE Transactions on Services Computing, 2018.
5. L. A. Linn and M. B. Koo, “Blockchain for health data and its potential use in health it and health care related research,” in ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, 2016.
6. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “Medrec: Using blockchain for medical data access and permission management,” in 2016 2nd International Conference on Open and Big Data (OBD). IEEE, 2016, pp. 25–30.
7. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
8. N. B. Truong, T.-W. Um, B. Zhou, and G. M. Lee, “Strengthening the blockchain-based internet of value with trust,” in 2018 IEEE International Conference on Communications (ICC). IEEE, 2018, pp. 1–7.
9. V. Gramoli, “From blockchain consensus back to byzantine consensus,” Future Generation Computer Systems, 2017.
10. W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, “A survey on consensus mechanisms and mining strategy management in blockchain networks,” IEEE Access, 2019.
11. A. Gervais, G. O. Karame, K. Wust, V. Glykantzis, H. Ritzdorf, ¨ and S. Capkun, “On the security and performance of proof of work blockchains,” in Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, 2016, pp. 3–16.
12. A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in Annual International Cryptology Conference. Springer, 2017, pp. 357–388.
13. A. Miller and J. LaViola, “Anonymous byzantine consensus from moderately-hard puzzles: A model for bitcoin,” nakamotoinstitute.org/research/anonymous-byzantine-consensus, 2014.
14. V. Buterin, “White paper: A next-generation smart contract and decentralized application platform,” April. https://www. ethereum. org/pdfs/Ethereum Whitepaper. pdf, 2014.
15. G. Wood, “Ethereum: A secure decentralized generalized transaction ledger,” Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.
16. T. Lodderstedt, M. McGloin, and P. Hunt, “Oauth 2.0 threat model and security considerations,” Tech. Rep., 2013.

17. N. Hackius and M. Petersen, “Blockchain in logistics and supply chain: trick or treat?” in Proceedings of the Hamburg International Conference of Logistics (HICL). epubli, 2017, pp. 3–18.
18. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, “Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,” in Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing. IEEE Press, 2017, pp. 468–477.
19. N. Herbaut and N. Negru, “A model for collaborative blockchain-based video delivery relying on advanced network services chains,” IEEE Communications Magazine, vol. 55, no. 9, pp. 70–76, 2017.
20. M. Ali, J. Nelson, R. Shea, and M. J. Freedman, “Blockstack: A global naming and storage system secured by blockchains,” in Annual Technical Conference (USENIX/ATC-16), 2016, pp. 181–194.
21. Dr.Venkata Kishore Kumar Rejeti, J. Gera, A. R. Palakayala, and T. Anusha, "Blockchain Technology for Fraudulent Practices in Insurance Claim Process," 2020 5th International Conference on Communication and Electronics Systems (ICCES) in IEEE, 2020, pp. 1068-1075, doi: 10.1109/ICCES48766.2020.9138012.
22. Dr.Venkata Kishore Kumar Rejeti, "Effective Routing Protocol in Mobile ADHOC Network Using Individual Node Energy", International Journal Advanced Research Engineering a Technology (IJARET), Volume 12, Issue 2, February 2021, pp.445-453, ISSN Print: 0976-6480 and ISSN Online: 0976-6499, DOI: 10.34218/IJARET.12.2.2020.042.