IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

DATA TRUST FRAMEWORK USING BLOCKCHAIN TECHNOLOGY AND ADAPTIVE TRANSACTION VALIDATION

[1]**Dr.R.JEGADEESAN** [2]**K.RISHITHA,** [3]**MD.AFREED,** [4]**K.NIKHITHA,**[54] **P. RAJESH,**
[1234]Final Year,DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
[1]Professor&HOD, Dept of CSE, Jyothishmathi Institute of Technology & Science Karimnagar,Telangana.

Abstract: This paper suggests a method for establishing data trust using blockchain, to remove obstacles to sharing data. By ensuring transparency and maintaining quality standards, it addresses the worries of both data providers and consumers. The framework evaluates data quality, controls access, and tracks data lineage. It also presents a model for assessment that considers reputation, endorsement, and condensation factors. Furthermore, it proposes an adaptive approach to selecting transaction validators based on trust metrics. Empirical findings validate the efficacy of the proposed system.

Keywords: Blockchain, Data Trust, Data Sharing, Distributed, Access Control.

1.INTRODUCTION

Data sharing is a significant concern due to privacy breaches, data misuse, and legal issues, leading to a reluctance among many data owners to share their data. This lack of transparency affects both data owners and users, highlighting the importance of trust in data sharing. Blockchain technology offers a solution by ensures transparency and security, with the potential to address key aspects of data trust such as provenance and auditing. Our proposed framework leverages blockchain to establish trust between data controllers and users, capitalizing on its distributed and secure nature. O'Hara identifies essential elements for data trust architecture, some of which are inherent to blockchain technology. Our framework includes a trust model to assess data responsibility, incorporating parameters like data owner endorsement and confidence levels. Adaptive transaction validation enhances security. Performance analysis confirms the system's efficiency in managing large transactions and meeting data trust requirements, while benefiting from transparency and reliability.

Data sharing has become a major concern due to worries about privacy, confidentiality, and ethics. Both data owners and users hesitate to share data because of trust issues. To address this, the concept of data trust aims to create transparent and dependable frameworks for sharing data.

Data trust covers legal, ethical, governance, organizational, and technical aspects needed to facilitate data sharing. Among various approaches, blockchain technology stands out for its potential to establish strong data trust frameworks. The decentralized and secure nature of blockchain can enhance trust by guaranteeing transparency and immutability in data-sharing processes.

O'Hara outlined eight key properties for data trust architecture, some of which match well with blockchain features such as provenance, auditing, and accountability. Others like discovery, access control, and impact can be tackled using smart contracts on permissioned blockchains.

In our proposed framework, we introduce a trust model that assesses the reliability of input datasets based on factors like data owner and asset endorsements, along with the confidence level of data owners in their provided data. These factors are stored on the blockchain ledger and updated with each transaction. We also implement adaptive transaction validation using Hyperledger Fabric, considering the trust value of datasets.

We conduct thorough performance analysis to showcase the system's effectiveness in handling large transaction volumes and scaling across multiple organizations. By leveraging blockchain's transparency and immutability, our framework ensures data trust while encouraging ethical and secure data usage for both data owners and users.

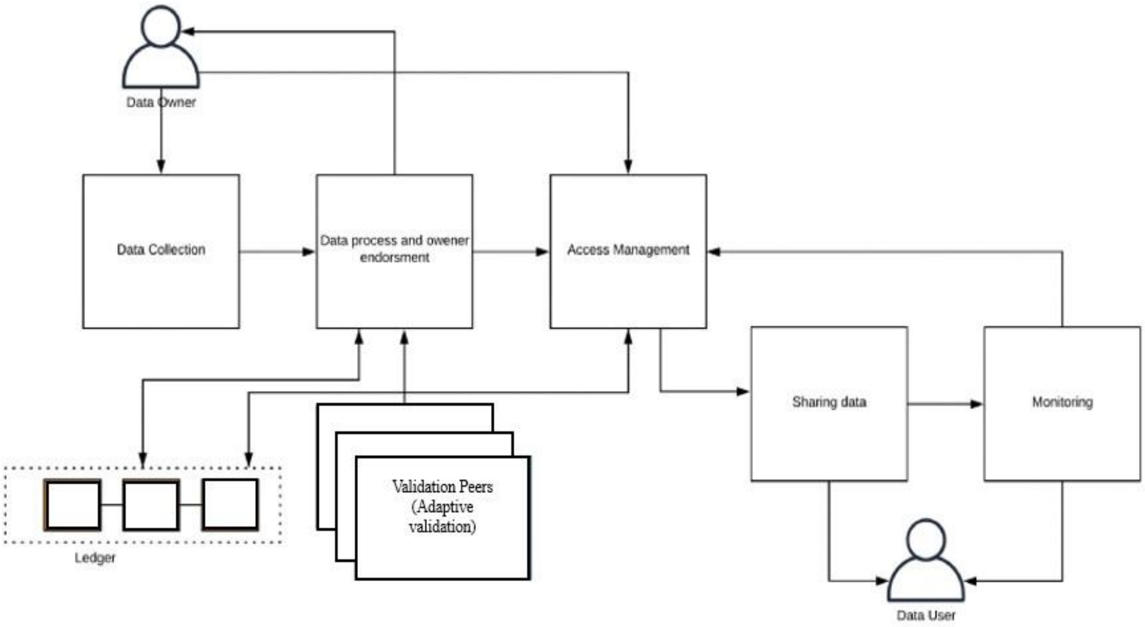


Figure 1.System architecture

2.PROBLEM DEFINITION

The problem with data sharing lies in concerns over privacy, misuse, and legal issues due to a lack of transparency and trust. Traditional methods often fail to ensure data integrity, leading to a reluctance among data owners. To tackle this, a data trust framework leveraging blockchain technology is proposed. Blockchain's transparency and immutability offer a solution by recording transactions securely. However, challenges like scalability, privacy, and regulatory compliance must be addressed. Adaptive transaction validation is crucial, adjusting validation criteria dynamically. The framework needs to be interoperable and compliant with regulations while promoting transparency and trust.

3.LITERATURE SURVEY

Shala et al. devised a reward system to incentivize IoT network peers with low trust scores to improve them. This system utilizes control loops with a target trust score. Service providers with low trust ratings are offered incentives such as discounts on other services to encourage them to enhance their service quality.

Wang et al. proposed an incentive-based strategy to motivate medical data owners to share their high-quality data and receive income, along with incentivizing miners who confirm transactions. This system aims to protect anonymity while generating high-quality crowdsensing contributions, rewarding participants with Bitcoin or Monero for their accurate sensing data.

Zavolokina et al. introduced a financial incentive for joining the network and offering top-notch information for automobile dossiers. They employ smart contracts to automatically calculate and implement incentives, with penalties for bad behavior to reduce errors.

Shrestha and Vassileva utilized blockchain and smart contracts to incentivize data owners to contribute their research data while retaining ownership. A subjective logic model was employed to evaluate the reputation of nodes for ensuring high-quality data exchange in vehicular networks.

Dedeoglu et al. proposed a trust model for evaluating the accuracy of data collected by IoT sensor nodes. This model considers the credibility and reputation of the data source, supplemented by evidence from neighboring sensor nodes. Blockchain is used to monitor data accuracy by detecting incorrect or suspicious data.

Choudhury et al. maintained data privacy while ensuring data quality by having regulatory bodies evaluate the accuracy of the data. They established private channels for specific activities to protect data privacy.

An et al. introduced Delegated Proof of Reputation (DPoR), a lightweight consensus technique, to address computing challenges in managing data quality for crowd-sensing nodes. This is achieved through smart contract verification procedures.

Su et al. devised a two-tier incentive scheme based on reinforcement learning to promote the sharing of high-quality data in edge computing layers. Casado-Vara et al. introduced a cooperative approach based on game theory to support data quality and detect false data in crowdsensing networks.

Research Through Innovation

4. EXISTINGWORKS

The current data trust framework employing blockchain and adaptive transaction validation relies on fundamental components to ensure its functionality. It commences with a robust blockchain infrastructure, commonly utilizing platforms such as Ethereum or Hyperledger Fabric, which securely store data in a decentralized ledger. Smart contracts play a pivotal role in automating transactions and enforcing rules within the network, offering the flexibility to adjust validation criteria as necessary. Data validation mechanisms are essential for maintaining the integrity of shared data, employing cryptographic techniques and consensus algorithms for verification.

Adaptive validation mechanisms further bolster the framework's efficacy by dynamically adjusting validation criteria based on factors like data trustworthiness and network conditions. Privacy measures are also incorporated to safeguard sensitive data while maintaining transparency, often utilizing technologies like zero-knowledge proofs. Interoperability features facilitate seamless data exchange across diverse platforms and organizations, fostering collaboration and operational efficiency.

To facilitate user interaction with the blockchain network, a user-friendly interface is provided, offering dashboards or specialized applications for ease of access and navigation. Additionally, compliance mechanisms are integrated into the framework to ensure adherence to regulatory requirements, incorporating embedded rules and auditing mechanisms for regulatory compliance.

5. PROPOSEDMETHODOLOGY

In the proposed system, an end-to-end framework for data trust is introduced, utilizing blockchain to ensure the reliability and quality of data for users while ensuring ethical and secure data usage for owners. Initially, a trust model is introduced to evaluate the trustworthiness of input data sets based on three parameters: the reputation and endorsement of the data owner and asset, and the confidence level of the data owner in the provided data. These parameters are recorded on the ledger and updated with each transaction. Additionally, the system employs adaptive transaction validation using Hyperledger Fabric's state-based endorsement, which is determined by the trust value of datasets. Lastly, a comprehensive performance analysis is conducted to showcase the system's effectiveness in managing large transaction volumes and scaling across multiple organizations. The system emphasizes that it possesses all the necessary properties for data trust, benefiting from the transparency, immutability, and security provided by blockchain technology, as well as the automation capabilities of smart contracts.

The flow chart and various entities in it are explained following the figure

International Research Journal
IJNRD
Research Through Innovation

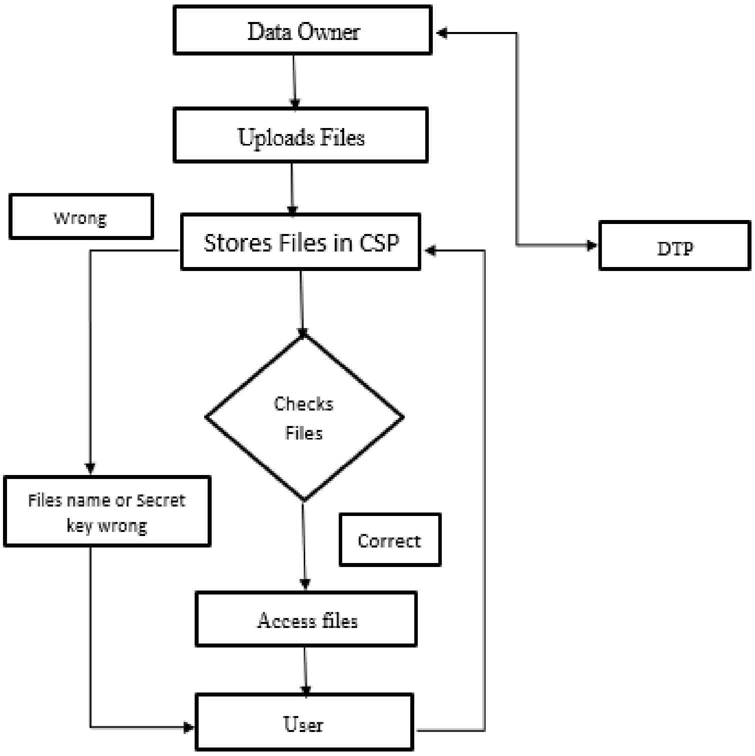


Figure 2: Flow Chart

6.SOLUTION

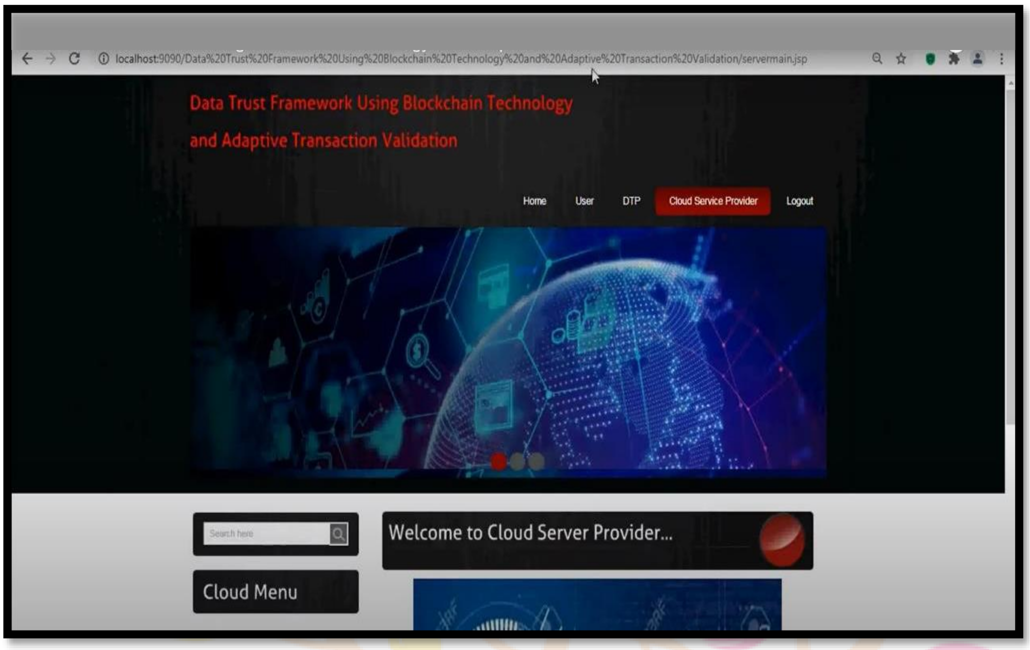
The solution for a data trust framework using blockchain technology and adaptive transaction validation involves selecting a suitable blockchain platform, developing smart contracts, implementing data validation mechanisms, and adapting transaction validation based on factors like data trustworthiness. Privacy enhancements, interoperability solutions, and a user-friendly interface are integrated, along with compliance mechanisms to adhere to regulations. Testing, deployment, and maintenance ensure the framework's efficiency, scalability, and ongoing functionality.

7. FUTURE ENHANCEMENT AND CONCLUSION

In the future, we can make the data trust system better by making it handle even more data and transactions, so it works faster and more reliably. We can also focus on improving privacy to keep sensitive information safe while still sharing data openly.

In conclusion, the data trust framework using blockchain and adaptive transaction validation is a great way to make sure data sharing is safe and trustworthy. By using blockchain's transparency and adaptability, we can create a system that builds trust between people who share data. With more improvements, this system can solve many of the problems with sharing data securely and openly.

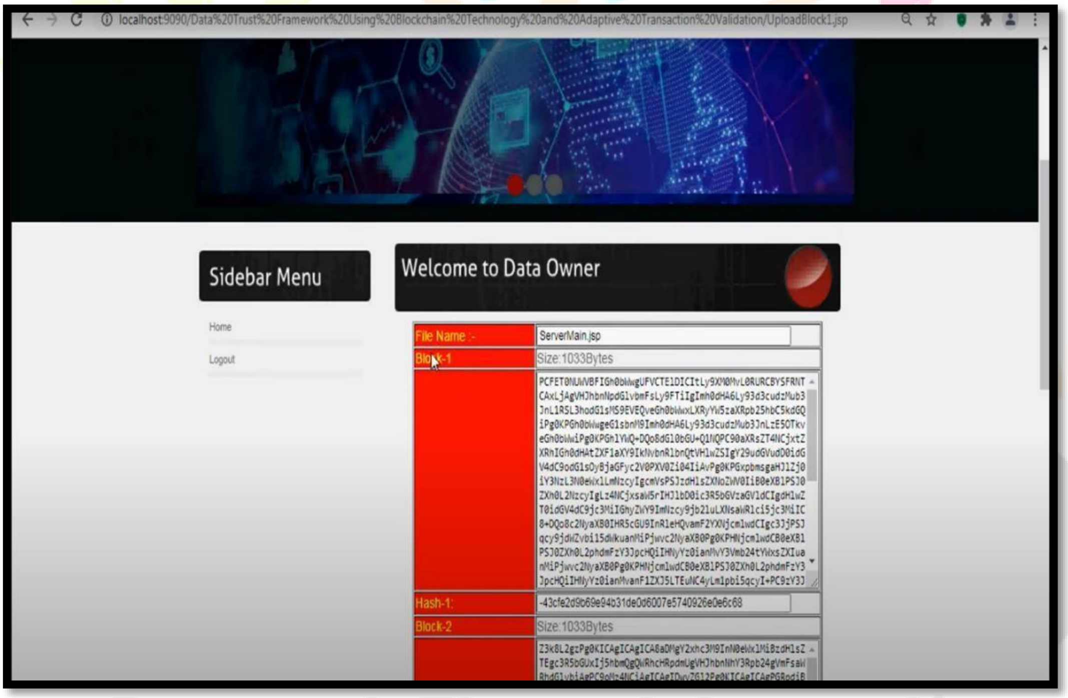
8. RESULT



localhost:9090/Data%20Trust%20Framework%20Using%20Blockchain%20Technology%20and%20Adaptive%20Transaction%20Validation/servermain.jsp

Data Trust Framework Using Blockchain Technology and Adaptive Transaction Validation

Welcome to Cloud Server Provider...



localhost:9090/Data%20Trust%20Framework%20Using%20Blockchain%20Technology%20and%20Adaptive%20Transaction%20Validation/UploadBlock1.jsp

Welcome to Data Owner

File Name :- ServerMain.jsp

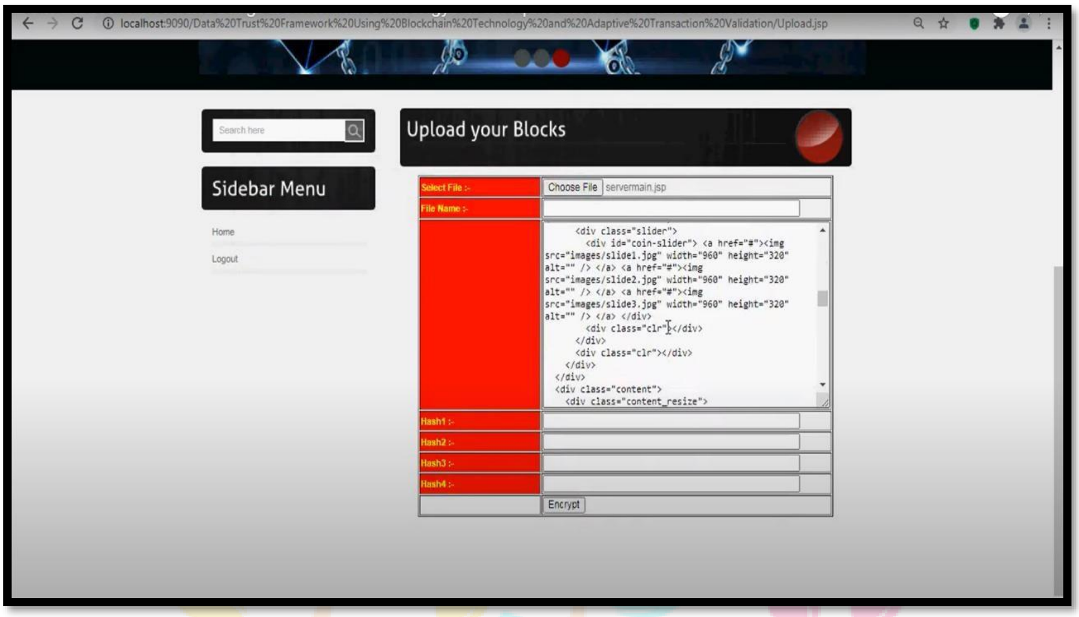
Block-1 Size:1033Bytes

PCFET0NUWVBFIGh0bWwgUFVCTElDICItLy9XM0MvL0RURCBYSFRNT
CAxLjAgVHJhbnNpdGlvbmFsLy9FTiIgImh0dHA6Ly93d3cudzMub3
JnL1RSL3hodGlsMS9EVEQveGh0bWwxLXRyYW5zaXRpb25hbC5kdGQ
iPg0KPGh0bWwgeG1sbnM9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkv
eGh0bWwiPg0KPGhlYWQ+DQo8dGl0bGU+Q1NQPC90aXRsZT4NCjxtZ
XRhIGh0dHAtZXF1aXY9IkNvbnRlbnQtVHlwZSIgY29udGVudD0idG
V4dC9odG1sOyBjaGFyc2V0PXV0Zi04IiAvPg0KPGxpbmsgaHJlZj0
iY3NzL3N0eWxlLmNzcyIgcmVsPSJzdHlsZXNoZWV0IiB0eXBlPSJ0
ZXh0L2NzcyIgLz4NCjxsaW5rIHJlbD0ic3R5bGVzaGVldCIgdHlwZ
T0idGV4dC9jc3MiIGhyZWY9ImNzcy9jb21uLXNsaWRlci5jc3MiIC
8+DQo8c2NyaXB0IHR5cGU9InRleHQvamF2YXNjcmlwdCIgc3JjPSJ
qcy9jdWZvbi15dWkuanMiPjwvc2NyaXB0Pg0KPHNjcmlwdCB0eXBl
PSJ0ZXh0L2phdmFzY3JpcHQiIHNyYz0ianMvY3Vmb24tYWxsZXIua
nMiPjwvc2NyaXB0Pg0KPHNjcmlwdCB0eXBlPSJ0ZXh0L2phdmFzY3
JpcHQiIHNyYz0ianMvanF1ZXJ5LTEuNC4yLm1pbi5qcyI+PC9zY3J

Hash-1: -43cfe2d9b69e94b31de0d6007e5740926e0e6c68

Block-2 Size:1033Bytes

Z3k8L2gzPg0KICAgICAgICA8aDMgY2xhc3M9InN0eWxlMiBzdHlsZ
TEgc3R5bGUxIj5hbmQgQWRhcHRpdmUgVHJhbnNhY3Rpb24gVmFsaW
RhdGlvbiAgPC9oMz4NCiAgICAgIDwvZGl2Pg0KICAgICAgPGRodiB


localhost:9090/Data%20Trust%20Framework%20Using%20Blockchain%20Technology%20and%20Adaptive%20Transaction%20Validation/Upload.jsp
Search here
Sidebar Menu
Home
Logout
Upload your Blocks
Choose File
Encrypt

Select File :- servermain.jsp

File Name :-

```
        <div class="slider">
          <div id="coin-slider"> <a href="#"><img
src="images/slide1.jpg" width="960" height="320"
alt="" /> </a> <a href="#"><img
src="images/slide2.jpg" width="960" height="320"
alt="" /> </a> <a href="#"><img
src="images/slide3.jpg" width="960" height="320"
alt="" /> </a> </div>
          <div class="clr"></div>
        </div>
        <div class="clr"></div>
      </div>
    </div>
    <div class="content">
      <div class="content_resize">
```

Hash1 :-

Hash2 :-

Hash3 :-

Hash4 :-

9. REFERENCES

[1] K. O’Hara, ``Data trusts: Ethics, architecture and governance for trustworthy data stewardship,'' Univ. Southampton, Southampton, U.K., Tech. Rep., 2019.

[2] Alsaad, K. O'Hara, and L. Carr, ``Institutional repositories as a data trust infrastructure,'' in Proc. Companion Publication 10th ACMConf.Web Sci., Jun. 2019, pp. 1_4.

[3] S. Rouhani and R. Deters, ``Security, performance, and applications of smart contracts: A systematic survey,'' IEEE Access, vol. 7, pp. 50759_50779, 2019.

[4] J.-H. Cho, K. Chan, and S. Adali, ``A survey on trust modeling,'' ACM Comput. Surv., vol. 48, no. 2, pp. 1_40, Nov. 2015.

[5] Z. Yan and S. Holtmanns, ``Trust modeling and management: From social trust to digital trust,'' in Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solutions. Hershey, PA, USA: IGI Global, 2008, pp. 290_323.

[6] S. Stalla-Bourdillon, G. Thuermer, J. Walker, L. Carmichael, and E. Simperl,
``Data protection by design: Building the foundations of trustworthy data sharing,'' Data Policy, vol. 2, pp. 1_10, Jan. 2020.

[7] G. S. Nelson, ``Practical implications of sharing data: A primer on data privacy, anonymization, and de-identification," in Proc. SAS Global Forum,2015, pp. 1_23.

[8] R Jegadeesan,A. Beno,S. P. Manikandan,D. S. Naga Malleswara Rao,Bharath Kumar Narukullapati,5T. RajeshKumar,Batyrkhan Omarov,Areda Batu, "Stable Route Selection for Adaptive Packet Transmission in 5G-BasedMobile Communications", "Wireless Communications and Mobile Computing 2022 "Research Article | OpenAccess Volume 2022 | Article ID 8009105 | https://doi.org/10.1155/2022/8009105.

[9] M. Akshitha, R Jegadeesan, G. Akshaya, P. Akhilac, M.Pavan Kalyan, G.Sindhusha, 2021 & June, "Covid-19Future Forecasting Using Supervised Machine Learning Models", Zeichen Journal, Volume 7, Issue 6, Page No.257-269, ISSN No: 0932-4747. DOI:15.10089.ZJ.2021.V7I6.285311.2425 (UGC Care Group II Journal)

[10] PerukaPriyavarshini, R Jegadeesan, Thatla Vaishnavi, KampellySahithi, Boga Shivani, P.Balakishan, 2021 &June, "Cyber Money Laundering Detection Using Machine Learning", Zeichen Journal, Volume 7, Issue 6, 2021,Page No.231-238,ISSN No: 0932-4747. DOI:15.10089.ZJ.2021.V7I6.285311.2422 (UGC Care Group II Journal)

[11] R Jegadeesan, Dava Srinivas, N Umapathi, G Karthick, N Venkateswaran "Personal Healthcare Chatbot ForMedical Suggestions Using Artificial Intelligence And Machine Learning", European Chemical Bulletin, Eur.Chem. Bull. 2023, 12 (S3), 6004 – 6012, DOI: 10.31838/ecb/2023.12.s3.670. (Scopus)

[12] S. Xuan, L. Zheng, I. Chung, W. Wang, D. Man, X. Du, W. Yang, and M. Guizani, ``An incentive mechanism for data sharing based on blockchain with smart contracts," Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106587.

[13] K. Shrestha and J. Vassileva, ``User data sharing frameworks: A blockchain- based incentive solution," in Proc. IEEE 10th Annu.Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON), Oct. 2019, pp. 0360_0366.

IJNRD Research Through Innovation