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 ADAPTIVE TRANSACTION VALIDATION

[1]M.RAVINDAR, [2]K. ASHRITHA,[3] K.UDAY KUMAR,[4]B.MADHUMITHA,[5]J.BRIJESH,
[2,3,4,5]Department – of Computer Science and Engineering
[1]Asso. Professor, Jyothishmathi Institute of Technology and Science
Karimnagar, Telangana

ABSTRACT:

The primary impediment to widespread data exchange is trust. Many data owners are unable to share their data and data consumers are concerned about the quality of the shared data due to the absence of transparent infrastructures for implementing data trust. The paradigm of data trust makes data sharing easier by requiring data users to be open and honest about the sharing and reuse of their data. This study uses blockchain technology to propose an end-to-end paradigm for data trust, enabling more reliable data exchange. By evaluating input data sets, efficiently handling access control, and providing data provenance and activity monitoring, the framework fosters data quality. We present an evaluation model for data quality that incorporates endorsement, reputation, and condense criteria.By guaranteeing the reliability and quality of the data at the point of origin and the ethical and secure use of the data at the conclusion, the proposed data trust framework satisfies the concerns of both data owners and users. A thorough experimental analysis successfully illustrates the system that is being presented.

INTRODUCTION

Concerns about data abuse, privacy and confidentiality difficulties, and ethical and legal transgressions have made data sharing a major problem. A transparent and reliable foundation for data trust is lacking, which prevents many data owners from sharing their data—which could be essential for a variety of research uses. The dependability and trustworthiness of the data at its source is a major concern for data users as well as data owners when it comes to data sharing. Therefore, trust is a mutually exclusive issue for data owners and users. A relatively new idea called "data trust" seeks to make data sharing easier by making data users disclose the

details of how they share and reuse their data. In addition to technical needs for facilitating data sharing, data trust involves legal, ethical, governance, and organizational structure considerations. Web observatories and institutional repositories have been mentioned in previous research as viable tools for adopting data trust. Through the transformation of current auditing techniques and automatic enforcement of smart contract logic, block chain technology has the significant ability to successfully offer the key qualities for constructing a workable framework for data trust, without the need for intermediaries to establish trust. Numerous more studies have looked into the possibilities of blockchain technology for data exchange, access management, and trust establishment. Nevertheless, those studies are mainly dispersed and have concentrated on a single phase or particular facet of data sharing, or they have taken a side in the data sharing process by solely addressing the concerns of data owners.The block chain's distributed, secure, and dependable characteristics can support the data trust framework's credibility. O'Hara presents eight properties—discovery, provenance, access controls, identity management, auditing of use, accountability, and impact—that ought to be taken into account while designing a data trust architecture. Certain qualities, such accountability, auditing of use, and provenance, are already present in the block chain. Due to the fact that the block chain maintains an unchangeable, secure record of all transactions and links all blocks together using hash values. Other characteristics that could be accomplished on permissioned block chains through smart contracts include impact, discovery, access control, and access.

LITERATURE SURVEY

The primary approach to project development is to construct a mail-enabled platform for a small business. This platform should include an address book, search engine, and engaging games in addition to making sending and receiving messages simple and convenient. When it is accepted by the company and our project manager, the first action, or preliminary inquiry, starts.

An evaluation of the financial case for a computer-based project is known as economic feasibility or cost-benefit analysis. The hardware project had a cheap cost because hardware was installed from the start and served many tasks. Any number of employees linked to the organization's local area network (LAN) can utilize this tool at any time because it is network-based. The organization's current resources will be used to construct the virtual private network. Therefore, the proposal is financially viable.The computer's output is needed mostly to establish an effective channel of communication within the organization, especially between the project manager and his team—that is, between the administrator and the clients. The system that the VPN produces enables the project manager to oversee his clients by adding new ones, assigning them new projects, keeping track of the projects' validity, and granting each client user-level access to folders based on the projects assigned to them. The client may be given a new project to work on after one has been completed.

PROPOSED METHOD

The suggested solution offers a blockchain-based end-to-end architecture for data trust, guaranteeing data owners' ethical and safe use of their data as well as the reliability and quality of the data at origin for data consumers. Firstly, we present a trust model that uses three criteria to evaluate the trustworthiness of input data sets: data owner confidence level in the given data set, data owner endorsement and reputation, and data asset endorsement. Every new transaction will update the ledger, which has records of all these parameters.Additionally, the system uses state-based endorsement from Hyper Ledger Fabric for adaptive transaction validation depending on trust values of datasets. Lastly, the system does an extensive performance analysis to show how well our system scales across numerous companies and handles massive sets of transactions. According to the system, our system has all the qualities needed for data trust. It also gains from the immutability, security, transparency, and automation powers of smart contracts provided by blockchain technology.According to the system, our system has all the qualities needed for data trust.It also gains from the immutability, security, transparency, and automation powers of smart contracts provided by blockchain technology.

ARCHIETECTURE DESIGN:

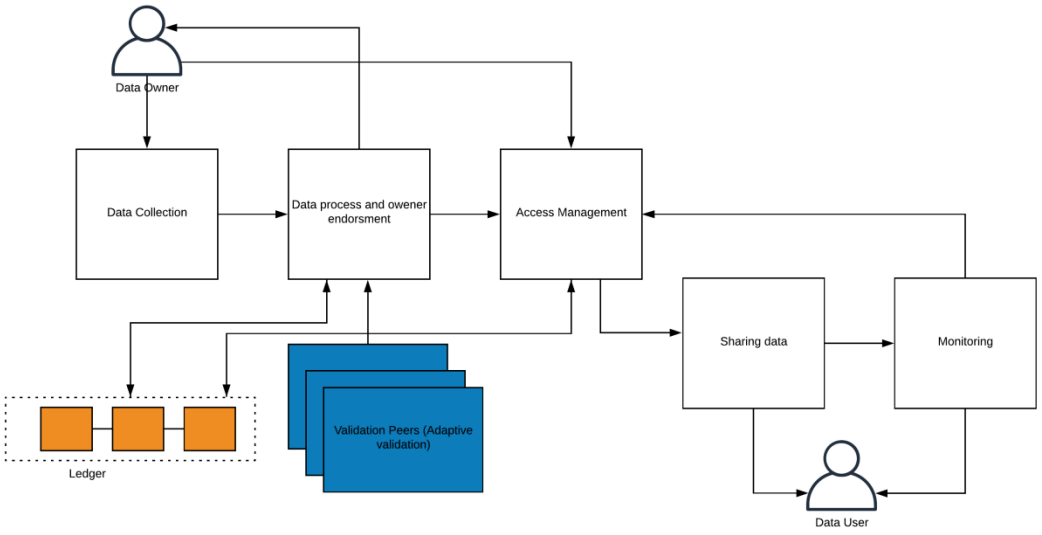

Figure1:SYSTEMARCHITECTURE

We model trust for the input data sets. For any initial data set, our system calculates its trust value through a blockchain-based application. This value is used to ensure only trusted data sets are confirmed, and the system only records trusted data assets on the ledger. Section V explains which parameters are involved and how the trust value is calculated.The data sets with lower trust values are considered suspicious, and they are required to be validated by more verifiers. This adaptive selection of the number of verifiers provides an acceptable

trade-off between the system's data assets quality and its performance and resource consumption. In order to prevent a data breach by data investigators, they would have access to a small chunk of data. The accuracy and quality of the data are examined through that small chunk.

RESULT:

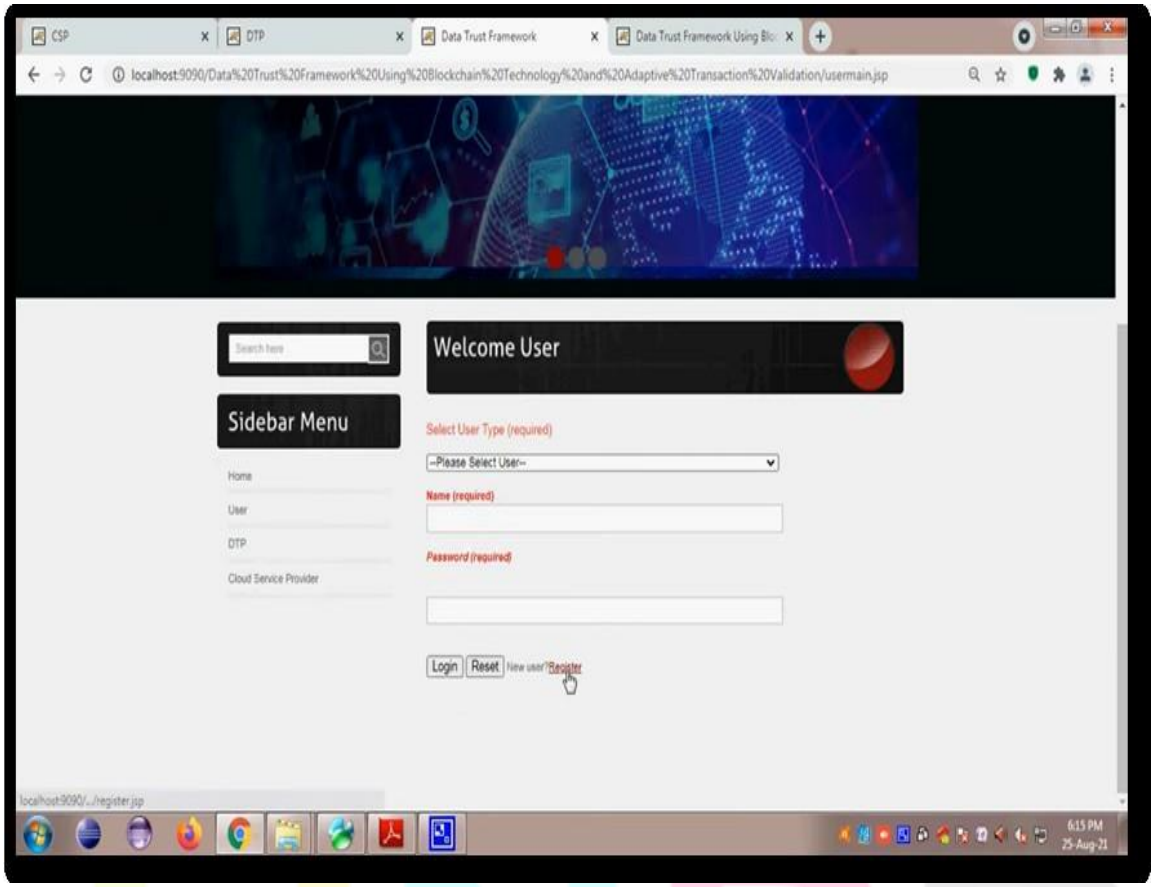

Figure 2 : Registration of the user through data trust framework login page by selecting type of the user and providing a name and password.

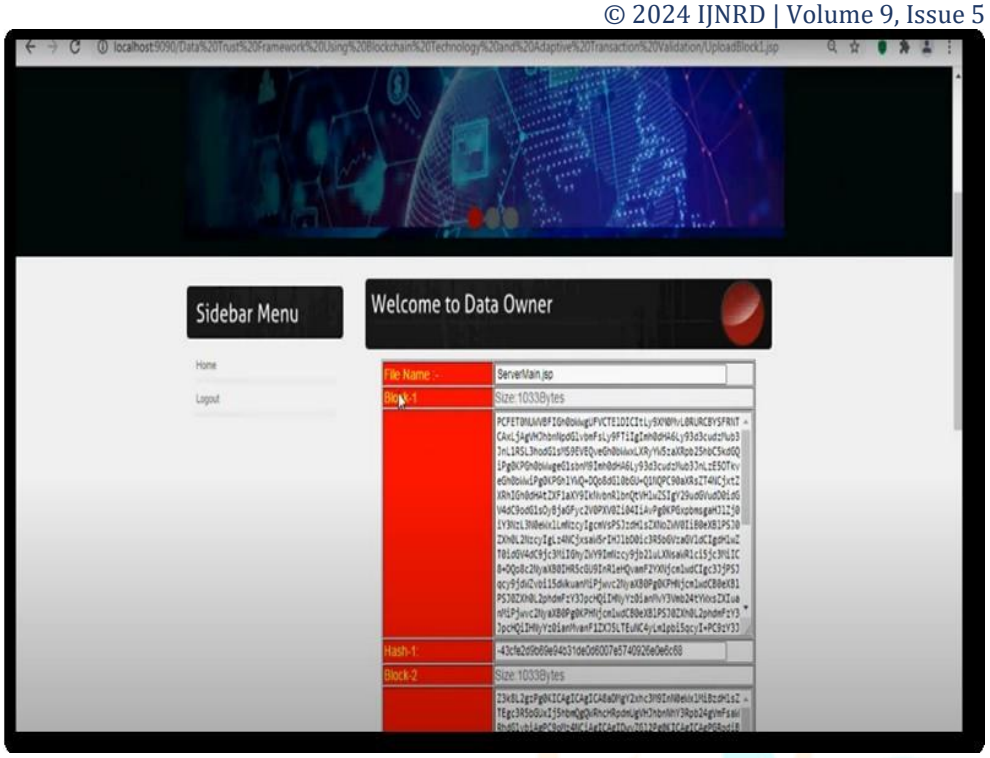

Figure3: Accessingdataowner withfilename,blockwithsizeinbytesandhashnumbers.

Figure 4: Finals results of ownerMain.jsp getting 12258, DataAttacker.jsp getting 41904, DataDelete.jsp getting 96960 in jsp chart.

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 applicationsof 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," ACMComput. Surv., vol. 48, no. 2, pp. 1_40, Nov. 2015.
5. Z.YanandS.Holtmanns,``Trustmodelingandmanagement:Fromsocialtrust to digital trust," in Computer Security, Privacy, and Politics: CurrentIssues, Challenges, and Solutions. Hershey, PA, USA: IGI Global, 2008, pp.290_323.
6. S.Stalla-Bourdillon,G.Thuermer,J.Walker,L.Carmichael, andE.Simperl,``Data protection by design: Building the foundations of trustworthydata 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-identi_cation," in Proc. SAS Global Forum,2015, pp. 1_23.
8. S. Xuan, L. Zheng, I. Chung, W. Wang, D. Man, X. Du, W. Yang,and M. Guizani, ``An incentive mechanism for data sharing based onblockchain with smart contracts," Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106587.
9. 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.
10. M. Shen,J. Duan, L. Zhu, J.Zhang, X. Du, and M. Guizani, Blockchain based incentives for secure and collaborative data sharing in multipleclouds," IEEE J.Sel. AreasCommun., vol. 38, no. 6, pp. 1229_1241, Jun. 2020.