# Framework for Data Trust Using Block-chain Technology and Adaptive Transaction Validation

**K. Jaya Krishna[1], SK. Anjaneyulu Babu[2], Medagam Ravindra Reddy[3], Ganugapeta Manohar[4], Jonnalagadda Chaitanya[5], Kakani Venkata Harish Babu[6], Pasala Ramesh[7]**

[1, 2] Asst.Professor, [3,4,5,6,7] PG. Scholars
Department of MCA, QIS College of Engineering & Technology (Autonomous) Ongole, AP, India.

**ABSTRACT**

The major obstacle limiting extensive data exchange is trust. Many data owners are unable to share their data due to the absence of transparent infrastructures for establishing data trust, while data consumers are concerned about the quality of the shared data. Data sharing is made easier by the data trust paradigm, which requires data users to be open about how they share and reuse their data. By using numerous parties to preserve agreement on an immutable record, blockchain technology suggests a distributed and transparent administration. With the use of blockchain technology, this article provides an end-to-end architecture for data trust that will improve reliable data exchange. The framework successfully handles access control, displays data provenance and activity tracking, and enhances data quality by evaluating input data sets. To assess the quality of the data, we provide an evaluation model that takes reputation, endorsement, and consistency into account.

We also provide an adaptive approach to calculating the estimated trust value-based number of transaction validators. By assuring the reliability and quality of the data at its source and its ethical and secure use in the end, the suggested data trust framework allays the worries of both data owners and consumers. A thorough experimental research reveals that the system being described can efficiently handle many transactions with little delay.

**Keywords:** Blockchain, data trust, data sharing, distributed, access control.

## 1. INTRODUCTION

Concerns about privacy and private concerns, data abuse, and moral and legal transgressions have made data sharing a hot topic. Many data owners are hesitant to provide their data, which might be essential for many research objectives, since there isn't a clear and reliable structure for data trust. Data consumers are worried about the legitimacy and dependability of the data given at the source, which is a major worry for data users as well as data owners. Therefore, trust is an issue that affects both data owners and consumers. Data trust is a relatively new idea that seeks to encourage data sharing by requiring data users to be open about the sharing and reuse of their data. Technical requirements for facilitating data sharing are part of data trust, along with legal, ethical, governance, and organisational structure considerations. Web observatories [1] and institutional repositories [2] may be useful for adopting data trust, according to earlier research. By changing current auditing procedures and automatically enforcing smart contract logic, block chain technology has the potential to effectively present the fundamental characteristics for developing a workable data trust framework. This would eliminate the need for intermediaries to establish trust. Numerous more studies have looked at the possibilities of block chains for data sharing, building trust, and access control. These studies, however, tend to be sporadic and have either selected a single stage or component in the data sharing process as their emphasis or have taken one side of the parties involved by addressing just the interests of data owners. Between data controllers and data consumers, a block chain may be utilised as a data trust interface. The block chain's distributed, secure, and dependable features may increase the data trust framework's credibility. Eight features, including (1) discovery, (2) provenance, (3) access restrictions, (4) access, (5) identity management, (6) auditing of usage, (7) responsibility, and (8) impact, are presented by O'Hara [1] as being important for data trust architecture. The block chain already has some of these qualities, including provenance, auditing of usage, and accountability. Because every block in a block chain is connected by its hash value, providing a secure, unchangeable record of transactions. On a permissioned block chain, smart contracts might be used to provide additional attributes like impact, access control, discovery, and impact. In permissioned block chains, identity management may be managed through the membership service.

## 2. LITERATURE REVIEW

Shala *et al.* established a reward system to encourage IoT network peers with low trust scores to raise it. The motivational system makes use of control loops with a goal trust score. A bundle of incentives, such as discounts for other services, will be provided to service providers with low trust ratings to entice them to deliver a better service in return for the promised advantages. In, authors introduced an incentive-based strategy to motivate medical data owners to share their high-quality (actual and practical) data and receive income, as well as miners who profit by taking part and confirming transactions.

Wang *et al.* developed a system for an incentive that protects anonymity in order to generate high-quality crowdsensing contributions. Participants are encouraged by the trust mechanism to give their high-quality sensing data in exchange for Bitcoin or Monero. Data miners also make money by ensuring the accuracy of the data.

Zavolokina *et al* gave a financial incentive for joining the network and offers top-notch information for automobile dossiers. The system anticipates that by penalising bad behaviour, mistakes would be reduced. For automatically calculating and implementing incentives, they use smart contracts. Blockchain technology and smart contracts were used by Shrestha and Vassileva to encourage data owners to contribute their research data without giving up ownership of it. In order to guarantee high-quality data exchange in the vehicular network, a subjective logic model has been employed to evaluate the reputation of nodes.

Dedeoglu *et al.* provided a trust model to evaluate the accuracy of data collected by IoT network sensor nodes. The credibility and repute of the data source, together with evidence from observations made by other neighbouring sensor nodes, make up the model. Blockchain is also used to monitor the accuracy of shared data by looking for incorrect or suspect data that may have been gathered by IoT or mobile crowdsensing.

Choudhury *et al.* maintained data privacy while ensuring data quality. As network members, regulatory bodies evaluate the accuracy of the data. By establishing activity-specific private channels, data privacy is protected. Delegated proof of reputation (DPoR), a lightweight consensus technique, was introduced by An et al. to address the challenging computing issue relevant to crowdsensing nodes' data quality management. Through the use of smart contract verification procedures, Huang et al. made sure that the data gathered from sensor nodes in the crowdsensing network was of high quality. To promote the sharing of high-quality data, Su et al. created a two-tier incentive scheme based on reinforcement learning (RL). In the edge computing layer, Casado-

Vara et al. also introduced a cooperative approach based on game theory to support data quality and false data detection.

## 3. Proposed System

The suggested solution includes a blockchain-based end-to-end architecture for data trust that guarantees the reliability and quality of the data at its source for data consumers and the moral and secure use of data for data owners. First, we provide a trust model that evaluates the credibility of input data sets based on three factors: the endorsement and reputation of the data owner, the endorsement of the data asset, and the amount of confidence of the data owner in the given data set. Each new transaction will change all of these parameters, which are shown on the ledger.

The solution further uses state-based endorsement based on dataset trust value for adaptive transaction validation utilising Hyper Ledger Fabric. The system then does a thorough performance study to show how well it scales across several companies and handles massive sets of transactions.

According to the system, all the attributes necessary for data trust are present in our system. It also gains from the automation capabilities of smart contracts and the transparency, immutability, and security provided by blockchain technology.

## 4. SYSTEM ARCHITECTURE

### FLOW CHART

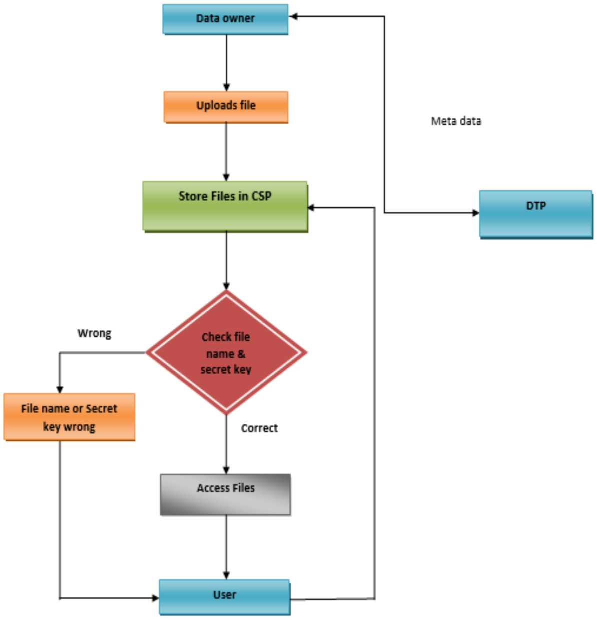


Fig 4.1: Flow chart

## Data Flow Diagram
## Level -0

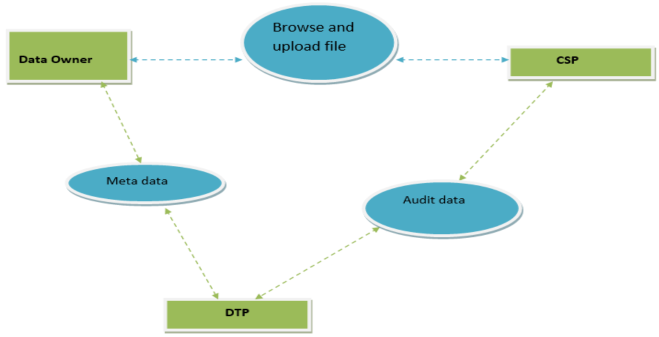


Fig:4.2: Level 0 data flow

## Level -1

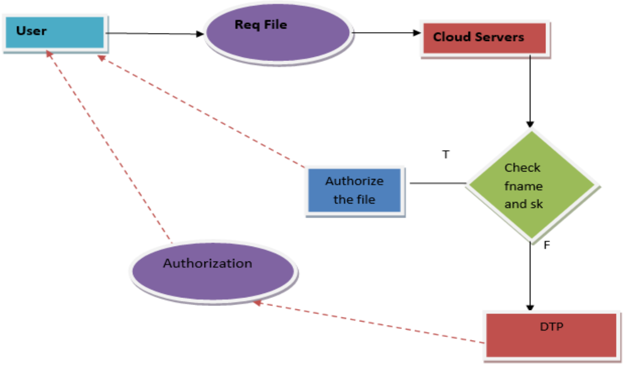


Fig:4.3: Level 1 data flow

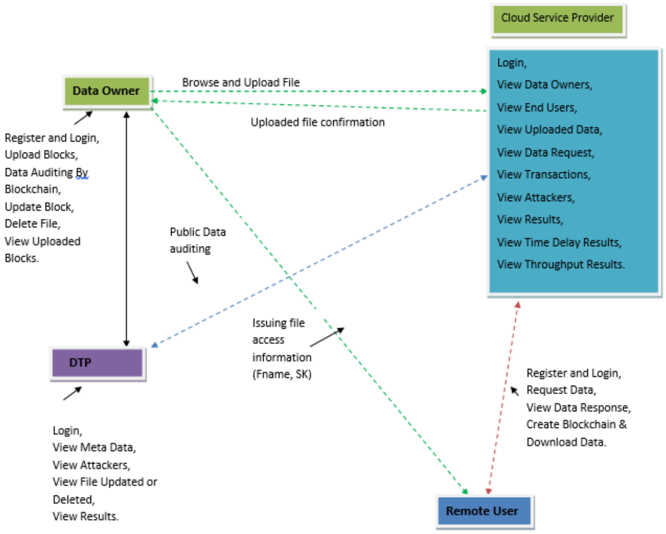


Fig:4.4: System architecture

## 5. RESULTS

Fig5.1: Home

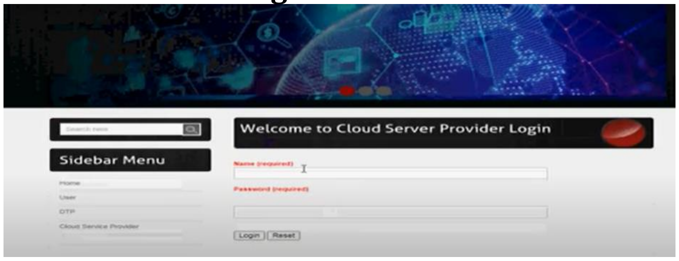


Fig 5.2: Cloud server provider login

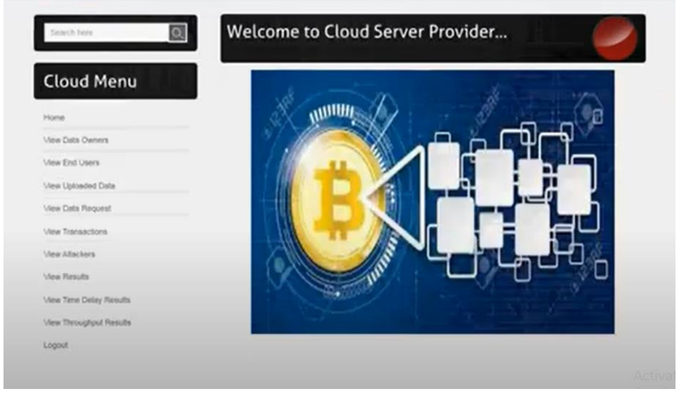


Fig5.3: welcome cloud server provider

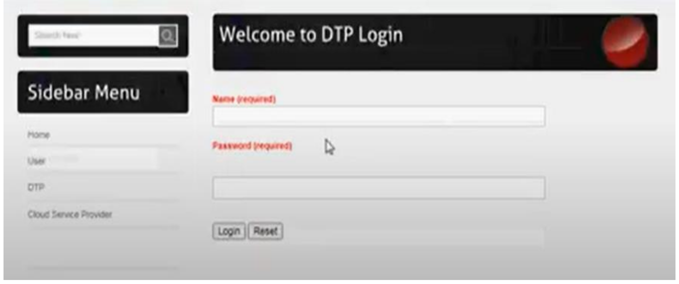


Fig5.4: DTP login

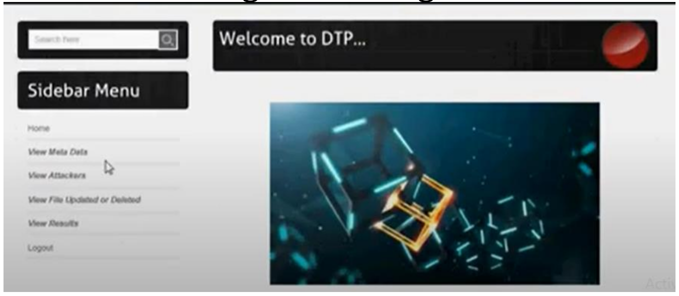


**Fig5.5: DTP**

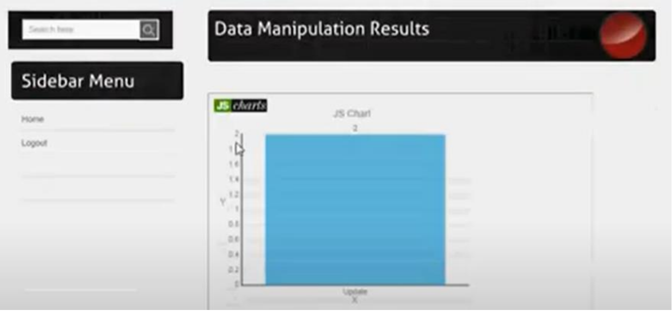
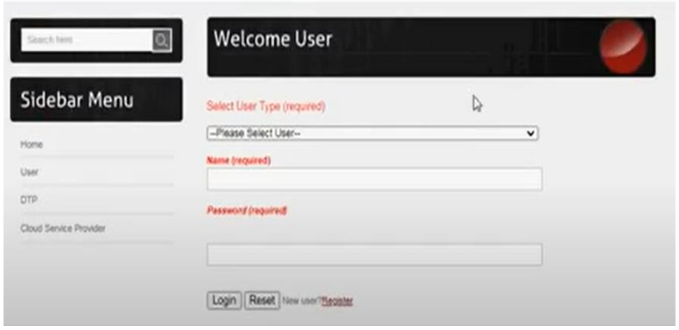

Data Manipulation Results

**Fig5.6: Manipulation results**


Welcome User

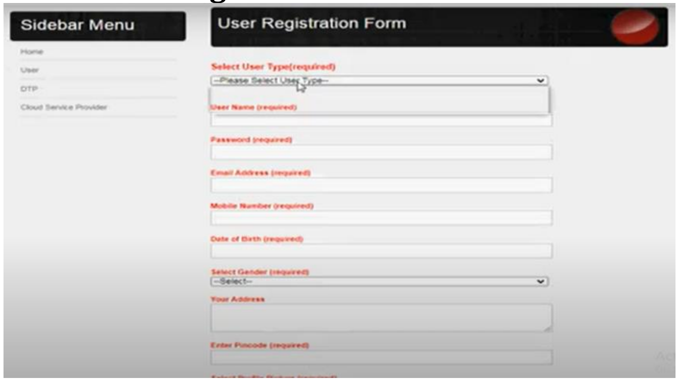
Select User Type (required)

--Please Select User--

Name (required)

Password (required)

**Fig5.7: Welcome user**


User Registration Form

Select User Type(required)

--Please Select User Type--

User Name (required)

Password (required)

Email Address (required)

Mobile Number (required)

Date of Birth (required)

Select Gender (required)

--Select--

Your Address

Enter Pincode (required)

**Fig5.8: Registration form**

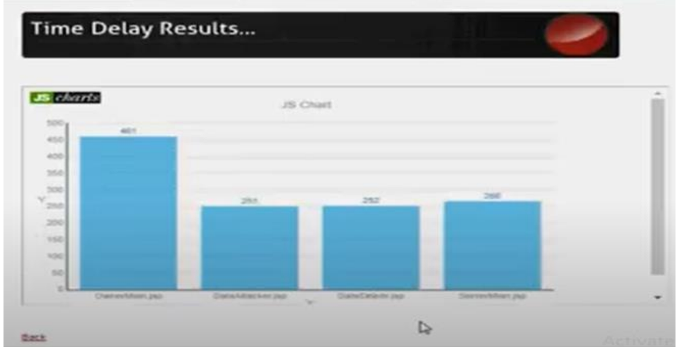

Time Delay Results...

**Fig5.9: Time delay results**

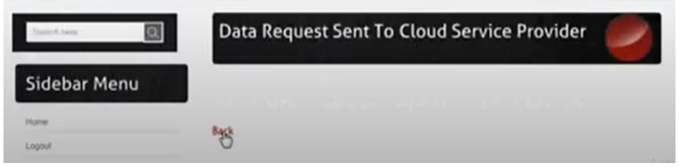

Data Request Sent To Cloud Service Provider

**Fig5.10: Data sent**

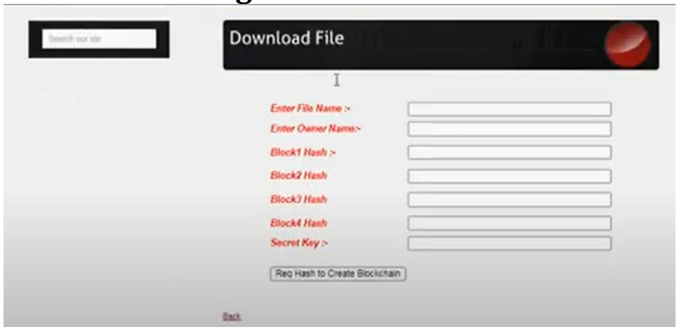


Fig5.11 Download file

## CONCLUSION

Due to a lack of mutual trust, current methods are unable to provide a workable and transparent method for data exchange. In this study, we provide a permissioned block chain-based end-to-end data trust system. Our proposed approach evaluates the input data quality using an unique trust model that takes into account the reputation, recommendations, and assurance in the data offered by the data owner. As a result, data consumers make sure that the quality of the accessible data sets has been updated and reviewed in an adaptive manner. In the architecture we provide, smart contracts are used to govern access in a safe, transparent, and automated manner for the advantage of data owners. Data owners are the only players in the system who have full control over their data assets and who are able to manage access rights independently of other parties. By using the provenance and audibility aspects of blockchain technology, data owners may also keep an eye on and track access restrictions and alterations to their data assets. Additionally, useful records may be gleaned from the ledger to provide a transparent picture of the system, spot suspicious requests, and identify protocol violations that might reveal potential risks. The system's ability to handle a high number of transactions for writing, updating, and querying trust parameter values is shown by the evaluation results.

In the future, we want to increase the framework's legitimacy by including rewards that will motivate users to participate honestly by including ratings and recommendations. Another crucial step in improving the system is detecting evaluations that are incorrect due to input from disruptive users.

## REFERENCES

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