ZKG INTERNATIONAL ISSN: 2366-1313

SECURE AND EFFICIENT BLOCKCHAIN-BASED DATA TRADING FOR MEDICAL EHR RECORDS

[1]Mrs. K.Srilatha,[2]T.Raja,[3]L.Yaswanth Goud,[4]N.Saketh Varma

[1]Assistant Professor, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

kumbamsrilatha@tkrec.ac.in@gmail.com

[2, 3, 4, BTech] Student, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad

rajathatikonda227@gmail.com,yashwanthgoudlalkota@gmail.com,sakethvarma1124@gmail.com

ABSTRACT:

We present a blockchain-based framework for equitable and confidential data exchange, tailored for precise data transactions. Our approach integrates attribute-based credentials, encryption, and zero-knowledge proof techniques to ensure fairness among trading parties. Sellers can verify data availability to buyers by revealing only necessary attributes, while buyers transfer funds upon successful key material verification. Additionally, to facilitate granular data transactions and safeguard identity privacy, we employ Merkle hash trees on data cipher texts with root node signatures, enabling sellers to partition data and remove sensitive information without compromising verification. Crucially, seller identities remain undisclosed, and transactions are unlikable. Formal security analysis validates our scheme's fairness and privacy preservation properties, while simulations underscore its practicality and efficiency.

Keywords*:*Blockchain, privacy preservation.

ISSN: 2366-1313

I INTRODUCTION

In today's digital age, data holds significant value, driving innovation, decision-making processes, and economic prosperity. The practice of data trading facilitates the exchange of data among parties, offering benefits to businesses and individuals alike. However, ensuring fairness in this exchange presents a notable challenge. Fairness entails buyers receiving the data they paid for and sellers being compensated upon successful delivery. Yet, inherent distrust often leads to a stalemate, as sellers are wary of providing data without payment, and buyers hesitate to pay upfront without guarantees.

Historically, solutions have relied on trusted intermediaries such as Dawex, Data coup, and Xignite to oversee transactions and establish trust. However, these intermediaries introduce their own concerns, including potential dishonesty and vulnerability to cyber threats. Additionally, centralized platforms pose risks of single points of failure, compromising the entire ecosystem's integrity.

To tackle these challenges, a blockchain-based solution emerges, leveraging its transparency, immutability, and decentralization. By recording transactions on a distributed ledger, blockchain eliminates the need for intermediaries and fosters trust among participants. Smart contracts, automated code deployed on the blockchain, ensure that both parties fulfill their obligations simultaneously.

Moreover, integrating privacy-preserving mechanisms into the blockchain infrastructure enhances data security and confidentiality. Techniques like zero-knowledge proofs and holomorphic encryption enable data sharing and verification without exposing sensitive information.

The proposed blockchain-based fair and fine-grained data trading system aims to transform the data economy by addressing trust issues, bolstering security, and safeguarding privacy. By decentralizing control and promoting transparency, it sets the stage for a more equitable and efficient data trading landscape.

II. LITERATURE SURVEY

Gregory Maxwell introduced the first blockchain-based fair data trading scheme, ZKCP, which addresses data availability through the verification of a public predicate function, typically a hash function. In ZKCP, data retrievability is ensured by disclosing

ISSN: 2366-1313

the encryption key. However, ZKCP faces setup challenges, particularly regarding the zero-knowledge proof system, specifically zkSNARK. To mitigate these issues, Li et al. proposed ZKPlus, which employs a commit-and-prove non-interactive zero-knowledge (CP-NIZK) scheme, providing a more practical approach to fair data exchange.

Furthermore, Zhao et al. proposed a machine learning-based fair data trading scheme, integrating sampling techniques and distance metric learning to validate data integrity. Additionally, a double authentication preventing signature mechanism is employed for decryption key recovery, enhancing the security of the data trading process.

Y. Zhao, B. Niu, and P. Li introduced an enhanced lightweight node for blockchain networks, focusing on Active Queue Management (AQM) to optimize network and application performance. By implementing various drop policies based on queue states and parameters, AQM aims to address inefficiencies related to large, unmanaged buffers, ultimately improving system efficiency and performance.

Delgado-Segura et al. introduced a fair data trading scheme utilizing the cut-and-choose method, where random subsets of data, or samples, are selected for validation. This approach allows the buyer to verify data availability by inspecting the plaintext of the sampled data. For data retrievability, vulnerabilities in cryptographic algorithms, such as the elliptic curve digital signature algorithm (ECDSA), have been leveraged to implicitly reveal decryption keys.

III SYSTEM ANALYSIS

EXISTING SYSTEM

In the existing system, data availability is ensured through a public predicate function, like a hash function, with the data encrypted by a symmetric key. A zero-knowledge proof is generated to confirm that the encrypted data satisfies the public predicate. However, this Zero-Knowledge Contingent Payment (ZKCP) scheme faces setup issues as the data buyer is responsible for setting up the zero-knowledge proof system, specifically a Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARK) system. To overcome these challenges, Li et al. proposed a fair-exchange scheme called ZKPlus.

Limitations of Existing System

One significant disadvantage of the current approach is its reliance on setup procedures,

ISSN: 2366-1313

leading to potential complications and inefficiencies. Additionally, fair data trading has long been a subject of study, and while the emergence of blockchain-based crypto currencies offers promise for achieving trustless transactions, challenges remain in ensuring data availability and irretrievability. This reliance on traditional methods may hinder progress towards more efficient and secure data trading systems.

PROPOSED SYSTEM

Our project aims to establish a approach to fair and grained data trading on the blockchain, prioritizing fairness, privacy preservation, and fine-grained transactions. In our proposed system, data sellers can sell portions of data without compromising data availability verification. Privacy protection for data sellers is paramount, achieved through a methodology where the attributes of Electronic Medical Records (EMR) are signed by the respective hospital, with attribute values encrypted independently. The order of attributes and their values is maintained through an authenticated data structure. Utilizing zero-knowledge proofs ensures data seller privacy and facilitates equitable data trading.

Our system also accommodates scenarios where buyers seek only data analysis results, enabling them to achieve accurate computations without direct access to sellers' data.

Proposed system Advantages:

Our system implements an authentication-based mechanism to verify data availability, eliminating the need for a central authority and supporting multiple issuers. Data signed by any authorized issuer remains acceptable, ensuring verification without revealing issuer identities. Additionally, our scheme facilitates granular data selling by selectively exposing required data to buyers, while maintaining low on-chain computational overhead.

IV IMPLEMENTATION

Architecture:

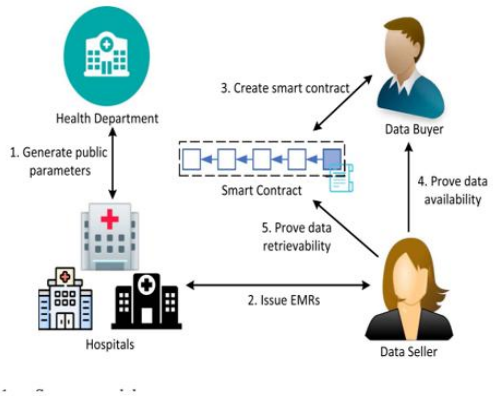

Fig-1. Architectures of the system model

ISSN: 2366-1313

- HD - The Health Department initiates by generating public system parameters for hospitals, facilitating the signing of Electronic Medical Records (EMRs) with uniform parameters. Following registration with the HD, hospitals' public keys are made publicly available.

- Hospital - Hospitals possess the ability to create and sign EMRs using their private keys, ensuring the authenticity of the data through signature verification. During data trading, hospitals maintain anonymity from data buyers.

- Data seller - Data sellers, typically patients owning EMRs, aim to monetize their data while safeguarding personal information from data buyers.

- Data buyer - Data buyers, which could include government bodies, pharmaceutical companies, or healthcare professionals, seek healthcare data and only release funds if the provided data meet their specified requirements.

- Smart Contract - Smart contracts, deployed on a blockchain, execute predefined conditions autonomously. These contracts ensure the integrity of transactions, automating fund transfers upon fulfillment of conditions.

The system operates in two phases: pre-trading and trading. During the pre-trading phase, the HD facilitates the generation of public parameters for hospitals, enabling them to issue and sign EMRs. In the trading phase, hospitals are relieved of direct involvement, alleviating their operational burden. Data buyers initiate by creating smart contracts, defining data requirements (referred to as policies) and depositing data rewards. Data sellers, possessing EMRs meeting the defined policy, engage with the buyer and the smart contract to facilitate trading.

MODULES

Health Department Module:

This module enables the health department to register and log in securely, upload patient records encrypted for privacy, and manage requests from sellers. The department can respond to requests by providing a security key for data access if the seller's request matches the records.

Seller Module:

Sellers can register, request health data from the department, and receive a security key to decrypt the data. They can also view requests from buyers and send them to the blockchain for verification. If the buyer's

ISSN: 2366-1313

request matches the available data and authorization is confirmed, the seller can grant permission for data access.

Buyer Module:

Buyers register and send requests to the blockchain specifying criteria like data size and keywords. The blockchain generates keys for requested records and matches the requests with sellers. If a seller with relevant data approves the request, the buyer can pay for the data securely through the blockchain.

Blockchain Module:

This module manages requests from buyers, verifies the authenticity of sellers, and facilitates secure data exchange. It generates blockchain records for each request, ensuring transparency and security throughout the data trading process.

IMPLEMENTATION

1. Blockchain Infrastructure Setup:

- Establish a decentralized blockchain network utilizing frameworks like Ethereum or Hyperledger Fabric.
- Deploy smart contracts to oversee transaction management, data storage, and operational protocols.
- Configure nodes to uphold decentralization, security measures, and consensus protocols.

2. User Management and Verification:

Develop user registration functionalities catering to Health Department, Sellers, and Buyers. Implement robust authentication protocols to validate user identities during login procedures.

3. Health Department Operations:

- Enable secure uploading of patient records by implementing encryption techniques for data protection.
- Design a secure system for Health Departments to process and respond to data requests from Sellers.
- Facilitate the generation and distribution of security keys by Health Departments for authorized data decryption by Sellers.

4. Seller Operations:

- Develop Seller-centric functionalities for registration, data request submission, and authorization receipt from Health Departments.
- Implement verification mechanisms for Sellers to authenticate authorization

ISSN: 2366-1313

requests from Buyers prior to data access provisioning.Enable Sellers to access requested data securely and provide decryption keys for authorized transactions.

5. Buyer Operations:

- Create Buyer-centric features for registration, data search, and request submission within the blockchain network.
- Implement robust systems for Buyers to specify data requirements, initiate secure transactions, and receive decryption keys upon authorization.

6. Blockchain Integration:

- Develop smart contracts governing interactions among Health Departments, Sellers, and Buyers.
- Implement logic for validating data requests, authorizations, and secure transactions within the blockchain ecosystem.
- Design encryption key management systems to ensure data privacy and integrity preservation.
- Facilitate efficient transaction validation and block generation processes within the blockchain infrastructure.

7. Testing and Deployment Procedures:

- Conduct comprehensive testing to validate functionality, security measures, and system performance.
- Deploy the blockchain-based platform in a production environment, emphasizing scalability and reliability.
- Continuously monitor the system post-deployment, incorporating necessary updates or enhancements based on performance feedback and analysis.

V RESULT AND DISCUSSION

Fig 2 Represents Homepage

ISSN: 2366-1313

The output screen represents the homepage it includes the health department, seller, buyer, blockchain.

Fig 3 Represents Health Department Login Page

The output screen represents the health department(hospitals) can login ,by giving the details.

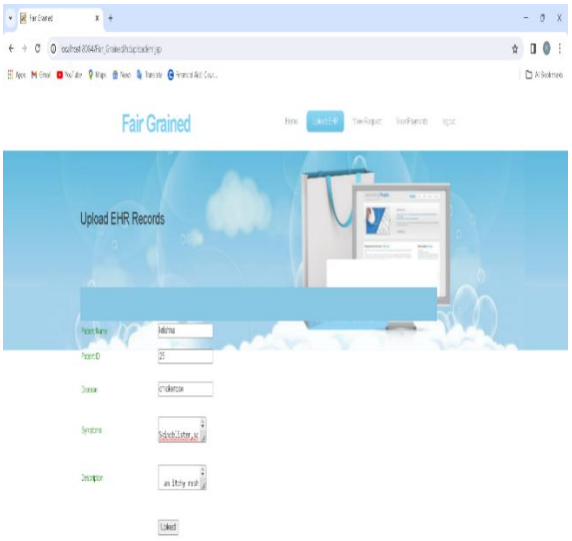

Fig 4 Represents Upload EHR Records

The output screen shows the uploading the patients electronic health records by giving details like patient name,patient id,disease,symptoms,description.

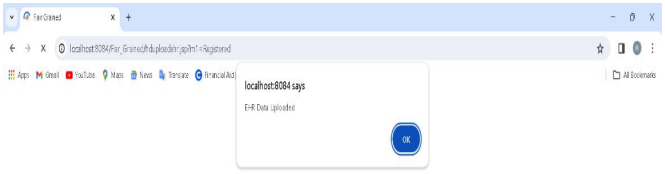

Fig 5 Represents EHR Data Uploaded

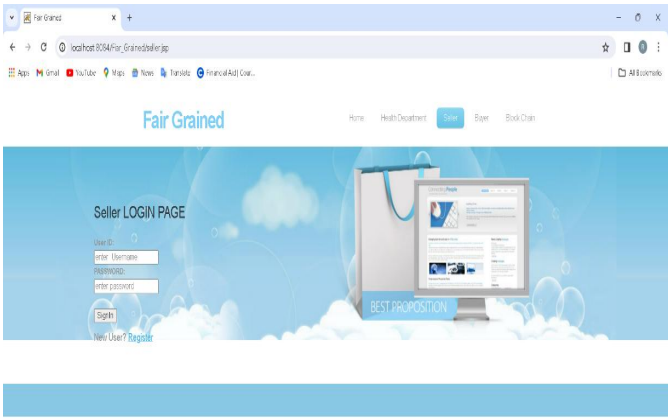

Fig 6 Represents Seller Login Page

The output screen represents seller login page by giving details like username and

ISSN: 2366-1313

passwords.

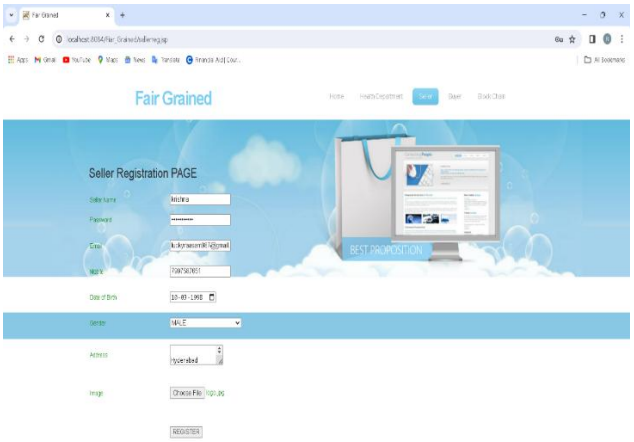

Fig 7 Represents Seller Registration Page

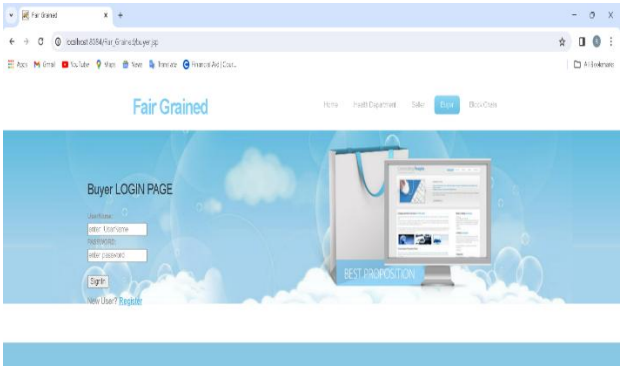

Fig 8 Represents Buyer Login Page

The output screen shows the representation of buyer login page by giving valid details like username ,password.

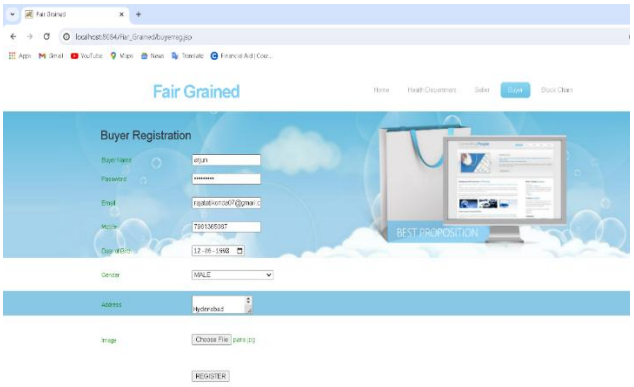

Fig 9 Represents Buyer Registration

The output screen represents the buyer registration by giving details like buyer name, password, email, mobile no, date of birth, gender, address, image.

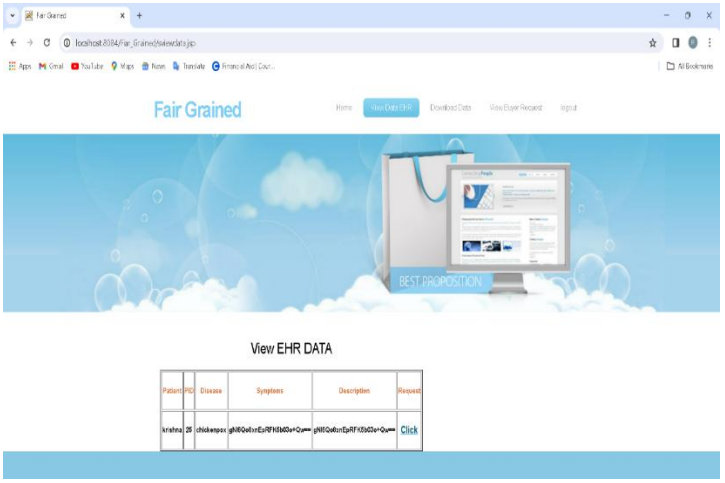

Fig 10 Represents view EHR DATA in seller page

The output screen represents EHR DATA it includes patient name,patient id ,disease, symptoms, description, request can be sent clicking on click in seller page.

ISSN: 2366-1313

Fig 11 Represents view EHR DATA in buyer page

The output screen represents EHR Data in buyer page like patients name, patients id, diseases, symptoms, descriptions

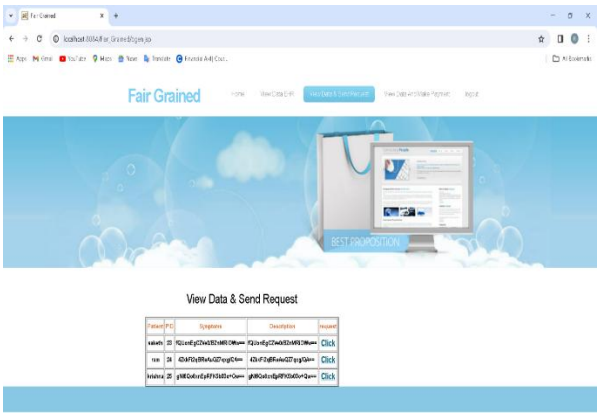

Fig 12 Represents view data and send request

The output screen represents the data and send request to the seller by showing the details patient name, pid, symptoms, description, request send to the seller.

Fig 13 Represents the conditions page

The output screen represents the conditions page in the buyer page to know the diseases in the seller page by entering disease name.

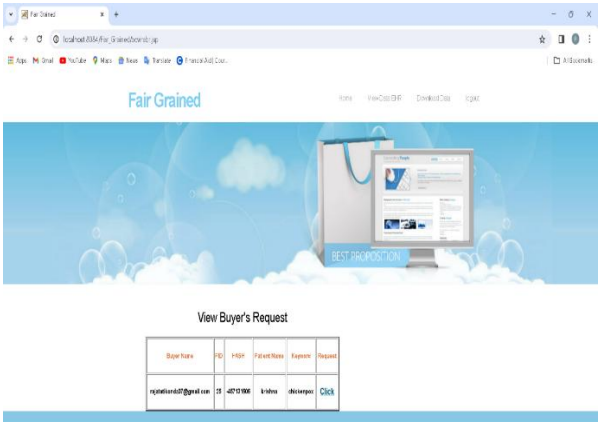

Fig 14 Represents the view buyer's request.

ISSN: 2366-1313

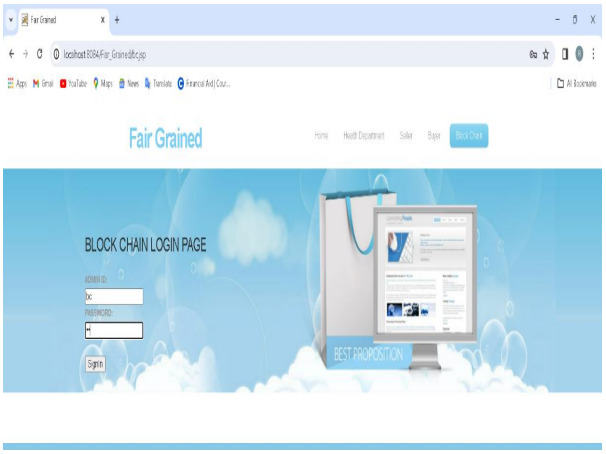

Fig 15 Represents the blockchain login page

The output screen represents the blockchain login page by giving details like admin id or username, password.

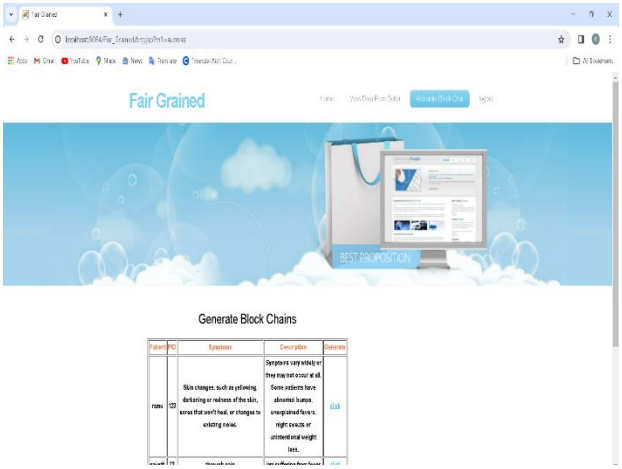

Fig 16 Represents the generate block chain

The output shows represents the generations for the above details to secure.

Fig 17 Represents the key verificiation

The output screen shows the key verification sended from the seller to get the security key of the patient id.

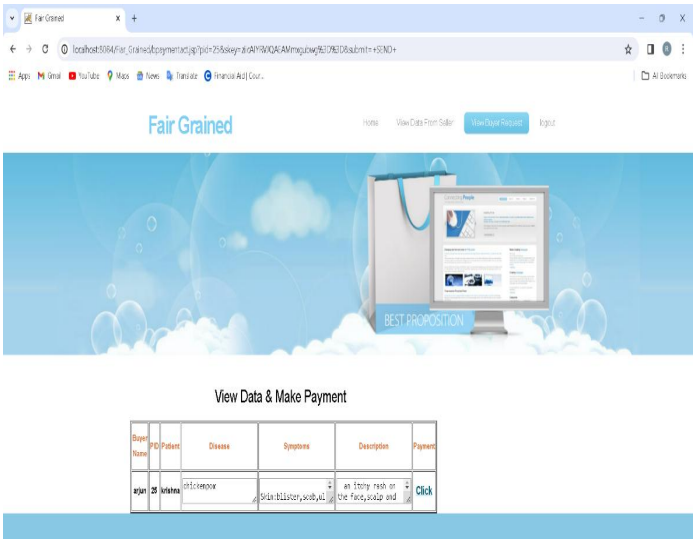

Fig 18 Represents the view data and make payment

ISSN: 2366-1313

The output screen represents the payments by showing the details like patient id, buyer , amount.

VI CONCLUSION

In summary, our innovative blockchain-based solution for fair and fine-grained data trading represents a significant breakthrough, especially in sensitive sectors like healthcare. Through our system, data buyers can specify their needs while data sellers can selectively share only relevant data, safeguarding sensitive information. The security proof validates the effectiveness of our approach, inspiring confidence in its real-world applicability. Furthermore, the adaptability of our method extends beyond healthcare, promising privacy preservation and precise trading across various domains. Moving forward, our research will focus on enhancing our system to accommodate scenarios where buyers seek computation results rather than raw data, ensuring seamless and secure data trading across diverse contexts.

FUTURE ENHANCEMENT

Potential future improvements could revolve around enhancing the scalability and efficiency of the blockchain-based fair and fine-grained data trading system. This may entail investigating methods to manage larger transaction volumes while keeping latency and costs minimal. Additionally, there's room for enhancing privacy protection measures to ensure stronger assurances of data anonymity and confidentiality. Exploring advanced cryptographic techniques or utilizing emerging technologies like homomorphic encryption could bolster security and functionality. Simplifying the data trading process through user-friendly interfaces and tools could drive wider adoption across various industries. Integration of machine learning or AI algorithms to optimize data matching and improve the trading experience could be beneficial. Furthermore, addressing regulatory and legal considerations to align with data protection laws and standards is crucial for long-term viability and acceptance.

VII REFERENCES

[1] Dawex. (2015). Dawex Platform. Retrieved from https://www.dawex.com/en/

[2] Xue, L., Liu, D., Ni, J., Lin, X., &Shen, X. (2022). Regulatory Compliance and Enforcement in Decentralized Anonymous Payment Systems.

[3] Liu, Y., et al. (2023). inIoT with Blockchain.

[4] Liu, D., Huang, C., Ni, J., Lin, X., &Shen, X. (2022). IEEE Transactions on Computers, 71(12), 3322–3335.

[5] Dziembowski, S., Eckey, L., & Faust, S. (2018). Fair Exchange Mechanism for Digital Goods.

[6] Campanelli, M., Gennaro, R., Goldfeder, S., &Nizzardo, L. (2017). Zero-Knowledge Contingent Payments Revisited: Security Analysis and Applications.

[7] Li, Y., et al. (2021). ZKCPlus: Fair-Exchange Protocol Supporting Practical Data Exchange.

[8] Galteland, Y. J., & Wu, S. (2021). Privacy-Preserving Fair Data Trading Protocol on Blockchain. Cryptology ePrint Archive. Retrieved from https://eprint.iacr.org/2021/1321

[9] Bobolz, J., Eidens, F., Krenn, S., Ramacher, S., &Samelin, K. (2021). Issuer-Hiding Attribute-Based Credentials. In Proceedings of the International Conference on Cryptology and Network Security (pp. 158–178).

[10] M. Petkus explains the principles behind zk-SNARK in "Why and how zk-SNARK works," available on arXiv (2019), under the identifier arXiv:1906.07221.

[11] Delgado-Segura, S., Pérez-Solà, C., Navarro-Arribas, G., & Herrera-Joancomartí, J. present a fair protocol for data trading based on Bitcoin transactions in "A fair protocol for data trading based on Bitcoin transactions," published in Future Generation Computer Systems (2020), volume 107, pages 832–840.

[12] Prasadu Peddi (2015) "A review of the academic achievement of students utilisinglarge-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35.

AUTHORS

Mrs. K.Srilatha,Assistant Professor Dept. of CSE, Teegala Krishna Reddy Engineering College Meerpet, Hyderabad.

Email: kumbamsrilatha@tkrec.ac.in@gmail.co

Mr. T.Raja, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: rajathatikonda227@gmail.com

ISSN: 2366-1313

Mr. L.Yaswanth Goud, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: yashwanthgoudlalkota@gmail.com

Mr. N.Saketh Varma, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: sakethvarma1124@gmail.com