ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 4 Issue 2 April 2024 / Page No: 11-18
Paper Id: JETA-V4I2P102 / Doi: 10.56472/25832646/JETA-V4I2P102

Original Article

Human-Computer Interaction between Blockchain Technology and User Privacy Protection

AnNing[1], WangZhuoxian[2]
[1,2]*Institute for Advanced and Smart Digital Opportunities (IASDO), School of Computing, Universiti Utara Malaysia, Sintok, Kedah, Malaysia*

Received Date: 05 February 2024 Revised Date: 03 March 2024 Accepted Date: 03 April 2024

Abstract: *The rise of blockchain technology has brought significant advancements to various industries. However, it has also raised concerns about user privacy protection. This paper investigates the human-computer interaction between blockchain technology and user privacy protection. The purpose of this study is to analyze the impact of blockchain technology on user privacy and propose effective measures to enhance privacy protection. The research method employed in this study includes a comprehensive literature review and a detailed analysis of existing blockchain systems. The results indicate that while blockchain technology offers transparency and immutability, it also poses challenges to user privacy due to the inherent characteristics of the blockchain. Based on the findings, this study concludes that integrating privacy-enhancing techniques, such as zero-knowledge proofs and encryption, into blockchain systems can effectively address user privacy concerns.*

Keywords: *Human-Computer Interaction, Blockchain Technology, User Privacy Protection.*

I. INTRODUCTION

Blockchain technology has revolutionized various industries by providing transparency and immutability. However, this advancement has also raised concerns about user privacy protection. The purpose of this study is to investigate the human-computer interaction between blockchain technology and user privacy protection, analyze the impact of blockchain technology on user privacy, and propose effective measures to enhance privacy protection.

A. Blockchain Technology

Blockchain technology is a decentralized and distributed ledger that records transactions across multiple computers. It is characterized by its principles of transparency, immutability, and security. Over the years, blockchain technology has evolved and developed, with various innovations and improvements implemented.

B. User Privacy Protection

User privacy refers to the control that individuals have over the collection, use, and disclosure of their personal information. In today's digital era, user privacy protection has become increasingly important due to the vast amount of personal data being collected and shared. However, it faces challenges such as data breaches, identity theft, and surveillance.

Methods of user privacy protection include data anonymization, encryption, access control, and user consent. These methods aim to safeguard user privacy by preventing unauthorized access to personal information and ensuring individuals have control over their data.

C. Human-Computer Interaction between Blockchain Technology and User Privacy Protection

The integration of blockchain technology and user privacy protection presents a dynamic interaction. On one hand, blockchain technology offers transparency and immutability, which can enhance user privacy by providing a verifiable and tamper-resistant record. On the other hand, the inherent characteristics of the blockchain, such as the public nature of transactions and the permanence of records, pose challenges to user privacy.

Solutions to enhance user privacy protection with blockchain technology include the adoption of privacy-enhancing techniques such as zero-knowledge proofs and encryption. These techniques can provide anonymity and confidentiality while maintaining the integrity of the blockchain. Case studies of blockchain in enhancing user privacy showcase various applications such as decentralized identity management systems, private transaction mechanisms, and secure data-sharing platforms. These case studies demonstrate the potential of blockchain technology to address user privacy concerns.

D. Conclusion

In conclusion, the human-computer interaction between blockchain technology and user privacy protection is a topic of critical importance. The impact of blockchain technology on user privacy should not be overlooked, and effective measures

should be implemented to enhance privacy protection. By integrating privacy-enhancing techniques into blockchain systems, user privacy concerns can be effectively addressed. Further research and development in this area are necessary to ensure the full potential of blockchain technology in protecting user privacy.

II. BLOCKCHAIN TECHNOLOGY

A. Definition and Principles of Blockchain Technology

Blockchain technology is a decentralized and distributed ledger system that records and verifies transactions across multiple computers or nodes. It is based on cryptographic principles to ensure the security and integrity of the data stored on the blockchain. The core concept of blockchain technology is the creation of a chain of blocks, where each block contains a list of transactions. These blocks are linked together using cryptographic hashes to form a tamper-proof and transparent ledger.

The principles underlying blockchain technology include decentralization, immutability, transparency, and consensus. Decentralization means that there is no central authority controlling the blockchain, making it resistant to single points of failure and censorship. Immutability refers to the inability to alter or delete data once it has been added to the blockchain. Transparency means that all transactions on the blockchain can be accessed and verified by anyone, fostering trust and accountability. Consensus mechanisms, such as proof-of-work or proof-of-stake, ensure that all participants in the network agree on the validity of transactions and the state of the blockchain.

By leveraging these principles, blockchain technology enables secure and trustless transactions, eliminates the need for intermediaries, and enhances data integrity and transparency. It has gained significant attention and adoption in various industries, including finance, supply chain management, healthcare, and more. The potential of blockchain technology lies in its ability to revolutionize existing systems and processes by providing a secure and efficient way to validate and store digital information.

In the context of user privacy protection, the use of blockchain technology raises concerns due to its inherent characteristics. The transparency of the blockchain, while beneficial for security and accountability, also means that all transactions and associated data are visible to anyone on the network. This transparency poses challenges to user privacy, as sensitive information may be exposed. Additionally, the pseudonymity of blockchain transactions, where users are identified by their public keys instead of their real identities, raises questions about the privacy implications and the potential for de-anonymization.

Thus, understanding the impact of blockchain technology on user privacy and implementing effective measures to enhance privacy protection is crucial for the successful adoption and integration of blockchain systems. In the following sections, this paper will explore the current situation and challenges of user privacy protection, analyze the human-computer interaction between blockchain technology and user privacy, and propose solutions to address these concerns.

B. Evolution and Development of Blockchain Technology

Blockchain technology has undergone significant evolution and development since its inception. Initially introduced as the underlying technology for Bitcoin, blockchain has now expanded its applications beyond cryptocurrency and has gained attention in various industries.

The initial concept of blockchain technology was proposed by Satoshi Nakamoto in 2008, with the release of the Bitcoin whitepaper. Nakamoto envisioned a decentralized and trustless system where transactions could be securely recorded. This marked the beginning of the evolution of blockchain technology.

Over the years, blockchain technology has evolved to include various features and improvements. One notable development is the introduction of smart contracts. Smart contracts are self-executing contracts with the terms of the agreement directly written into the code. They automatically facilitate, verify, or enforce the negotiation or performance of a contract, eliminating the need for intermediaries.

Another significant development in blockchain technology is the emergence of different types of blockchains. Initially, blockchain operated on a public and permissionless network, where anyone could participate and contribute to the network. However, as the technology matured, private and permissioned blockchains were introduced. Private blockchains are restricted to a specific group of participants, while permissioned blockchains require participants to obtain permission to join the network.

Furthermore, scalability and efficiency have been major focus areas in the development of blockchain technology. Initially, Bitcoin's blockchain had limitations in terms of transaction speed and scalability. However, subsequent

developments, such as the introduction of second-layer solutions like Lightning Network, have addressed these issues and improved the overall performance of blockchain technology.

Moreover, interoperability and compatibility between different blockchain networks have become important considerations. As the number of blockchain platforms and applications increases, the need for seamless communication and data exchange between different networks has emerged. Projects such as Cosmos and Polkadot aim to address these challenges by providing interoperability solutions.

In conclusion, blockchain technology has witnessed significant evolution and development since its inception. The introduction of smart contracts, different types of blockchains, scalability improvements, and a focus on interoperability have contributed to the advancement of blockchain technology. These developments have paved the way for the application of blockchain in various industries and have opened up new possibilities for innovation and disruption.

C. Application of Blockchain Technology

Blockchain technology has found applications in various industries, revolutionizing the way transactions and data are recorded and verified. One of the major applications of blockchain technology is in the financial sector. It has enabled the creation of decentralized cryptocurrencies, such as Bitcoin, that allow for secure and transparent peer-to-peer transactions without the need for intermediaries like banks.

Apart from finance, blockchain technology has also been applied in supply chain management. By utilizing blockchain, the entire supply chain process can be recorded and tracked transparently. This enhances the efficiency and security of supply chain operations, minimizing the risks of counterfeiting and improving customer trust.

Moreover, blockchain technology has been adopted in the healthcare sector. The secure and decentralized nature of blockchain makes it ideal for storing and sharing sensitive patient data. With blockchain, patients have control over their medical records and can securely share them with healthcare providers, ensuring privacy and reducing the likelihood of data breaches.

Additionally, blockchain technology has shown the potential to revolutionize the energy sector. By utilizing blockchain, energy transactions can be recorded and verified transparently and securely. This enables peer-to-peer energy trading and reduces reliance on centralized energy providers, leading to a more efficient and sustainable energy system.

Furthermore, blockchain technology has been explored in the field of voting systems. Blockchain can provide a secure and tamper-proof platform for conducting elections, ensuring transparency and trust in the voting process. This has the potential to eliminate fraudulent activities and enhance the democratic process.

Overall, the applications of blockchain technology span across various industries, offering improved efficiency, transparency, and security. However, it is important to address the potential challenges and implications on user privacy posed by the implementation of blockchain technology.

III. USER PRIVACY PROTECTION

A. Definition and Significance of User Privacy

User privacy refers to the protection of personal information and the control individuals have over the collection and use of their data. It is a fundamental right that ensures individuals are in control of their information and can maintain their autonomy in the digital age. Ensuring user privacy is of utmost importance as it prevents the misuse or unauthorized access to personal data. With the rapid advancement of technology and the increasing reliance on digital platforms, the need for user privacy protection has become even more critical.

User privacy plays a significant role in maintaining the trust and confidence of individuals in the online environment. When users feel that their privacy is adequately protected, they are more likely to engage and participate in various online activities without hesitation. On the other hand, if user privacy is compromised, it can lead to a loss of trust, reduced user engagement, and potential damage to individuals' personal and financial well-being.

Achieving effective user privacy protection is a complex task due to various factors. Firstly, individuals generate massive amounts of data through their online activities, including browsing history, financial transactions, social media interactions, and more. This data can be highly sensitive and vulnerable to misuse if not adequately protected. Secondly, the collection, storage, and processing of personal data are often carried out by multiple parties, making it challenging to ensure consistent privacy protection throughout the entire data lifecycle. Finally, emerging technologies, such as blockchain, present new challenges and opportunities in user privacy protection.

Given the significance of user privacy in the digital era, it is crucial to establish robust frameworks and mechanisms to protect individuals' personal information. This requires a comprehensive understanding of user privacy, the challenges it faces, and the development of effective methods for privacy protection. The integration of blockchain technology into privacy protection measures holds great promise, as it offers transparency, immutability, and decentralized control over data. By exploring the human-computer interaction between blockchain technology and user privacy, we can identify innovative solutions to protect user privacy in the digital age.

B. Current Situation and Challenges of User Privacy Protection

With the increasing ubiquity of technology and the rapid growth of internet-based services, user privacy has become a major concern. The collection and use of personal data by companies and organizations has raised significant challenges in terms of ensuring the privacy and security of individuals.

In recent years, the rise of blockchain technology has introduced new opportunities and challenges in the realm of user privacy protection. While blockchain offers many benefits, such as decentralization and transparency, it also poses risks to user privacy.

One of the key challenges in user privacy protection is the issue of anonymous transactions. While blockchain technology ensures that all transactions are recorded on a public ledger, the identities of the individuals involved in the transactions remain pseudonymous. This means that while the transactions can be traced back to wallet addresses, the specific individuals behind these addresses may remain unknown.

Another challenge is the potential exposure of sensitive personal information. Traditional blockchain systems, such as Bitcoin, store all transaction data on a public ledger, which means that personal information, such as transaction amounts and addresses, is readily available for anyone to access. This poses a significant risk to user privacy, as it enables potential malicious actors to analyze and track user activities.

Furthermore, the immutability of blockchain poses challenges to user privacy protection. Once data is recorded on the blockchain, it cannot be altered or deleted. This means that any personal information that is accidentally or maliciously included in a transaction will remain on the blockchain indefinitely.

Additionally, the lack of standardized privacy policies and regulations surrounding blockchain technology further complicates user privacy protection. As blockchain is still a relatively new technology, there is a lack of established guidelines and legal frameworks for ensuring privacy and data protection.

Overall, the current situation of user privacy protection in the context of blockchain technology is challenging. The inherent characteristics of blockchain, such as pseudonymity, transparency, and immutability, create risks to user privacy. Addressing these challenges requires innovative solutions and the implementation of privacy-enhancing techniques to protect user data and ensure privacy in blockchain systems.

C. Methods of User Privacy Protection

Several methods can be utilized to protect user privacy in the context of blockchain technology. These methods aim to safeguard sensitive user information and ensure that it remains private and secure.

The following methods have been identified as effective means of enhancing user privacy protection:

a) Encryption:

One of the fundamental methods for protecting user privacy is through the use of encryption techniques. This involves encoding data in a way that makes it unreadable to unauthorized individuals. By encrypting user data, blockchain systems can ensure that sensitive information remains confidential and cannot be easily accessed or tampered with.

b) Anonymity:

Ensuring user anonymity is crucial for preserving privacy. Blockchain systems can incorporate techniques that allow users to engage with the technology without disclosing their real identities. By employing anonymity measures, users can participate in transactions and interactions on the blockchain while maintaining their privacy.

c) Zero-Knowledge Proofs:

Zero-knowledge proofs are cryptographic protocols that allow a user to prove the validity of a statement without revealing any additional information. This method can be used in blockchain systems to verify transactions or interactions without disclosing specific details to maintain user privacy.

d) Permissioned Blockchains:

Implementing permissioned blockchains can offer greater privacy protection. With permission blockchains, access to the network and participation in transactions are restricted to authorized parties only. This ensures that user information is shared only among trusted entities, reducing the risk of unauthorized access.

e) Data minimization:

Blockchain systems can implement data minimization techniques to limit the amount of user information stored on the blockchain. By minimizing the data stored, the potential for privacy breaches or leaks is reduced, as there is less sensitive information available for unauthorized parties to access.

f) Consent-Based Data Sharing:

Providing users with control over their data and obtaining their explicit consent before sharing it can greatly enhance privacy protection. Blockchain systems can incorporate mechanisms that require user consent for data sharing, ensuring that individuals have control over how their information is utilized.

In summary, these methods can significantly contribute to the protection of user privacy in the context of blockchain technology. By employing encryption, anonymity, zero-knowledge proofs, permissioned blockchains, data minimization, and consent-based data sharing, blockchain systems can enhance the privacy of user information and address the challenges posed by the technology's inherent characteristics.

IV. HUMAN-COMPUTER INTERACTION BETWEEN BLOCKCHAIN TECHNOLOGY AND USER PRIVACY PROTECTION

A. Impact of Blockchain Technology on User Privacy Protection

The rapid development of blockchain technology has brought significant advancements to various industries. However, it has also raised concerns about user privacy protection. In this section, we will examine the impact of blockchain technology on user privacy protection.

One of the main challenges is the transparency and immutability of the blockchain. While these characteristics ensure trust and security within the system, they also pose risks to user privacy. The public nature of blockchain transactions means that anyone can access and view the transaction history, including sensitive personal information. This lack of privacy can be a major concern for users, especially in situations where confidentiality is required.

Moreover, the use of pseudonyms in blockchain transactions does not completely guarantee anonymity. In many cases, it is still possible to link pseudonyms to real-world identities through various techniques such as IP address tracking or transaction patterns analysis. This can potentially expose users' personal information and compromise their privacy.

Furthermore, the increasing adoption of blockchain technology in various sectors, such as healthcare and finance, introduces new challenges for user privacy protection. For example, in healthcare, the use of blockchain for storing and sharing medical records can potentially expose sensitive health information to unauthorized parties. Similarly, in the financial sector, blockchain-based systems for financial transactions may expose users' financial data and transaction history.

To address these challenges, effective measures need to be implemented to enhance user privacy protection in blockchain systems. This can include the integration of privacy-enhancing techniques such as zero-knowledge proofs and encryption. These techniques can provide users with the ability to prove the validity of a transaction without revealing any sensitive information.

In conclusion, while blockchain technology offers transparency and immutability, it also poses challenges to user privacy. The impact of blockchain technology on user privacy protection cannot be ignored, and measures need to be taken to ensure the privacy and confidentiality of users' information. Integrating privacy-enhancing techniques into blockchain systems can effectively address these concerns and enhance user privacy protection.

B. Solutions to Enhance User Privacy Protection with Blockchain Technology

To address the challenges posed by blockchain technology to user privacy, several solutions can be implemented to enhance privacy protection. These solutions utilize various privacy-enhancing techniques and mechanisms, such as zero-knowledge proofs and encryption, to safeguard user data within blockchain systems.

One effective solution is the integration of zero-knowledge proofs (ZKPs) into blockchain systems. ZKPs allow for the verification of a statement without revealing any underlying information. By employing ZKPs, users can prove their knowledge of certain data or transactions without disclosing the actual data itself, thereby preserving their privacy. For example, ZKPs can be used to verify the validity of a transaction without revealing the details of the transaction, ensuring the privacy of the involved parties.

Another solution is the use of encryption techniques to protect user data within blockchain systems. Encryption algorithms can be utilized to securely encrypt user data, ensuring that it remains confidential and inaccessible to unauthorized parties. This prevents the leakage of sensitive information and enhances user privacy. Additionally, using encryption techniques in conjunction with secure key management systems can further strengthen data protection within blockchain systems.

Furthermore, the implementation of privacy-focused consensus mechanisms can enhance user privacy protection in blockchain systems. Traditional blockchain systems often rely on consensus mechanisms that expose user identities and transaction details. However, privacy-focused consensus mechanisms, such as zero-knowledge-based consensus protocols, can enable secure transaction validation while preserving user privacy. These mechanisms ensure that only the necessary information is visible to network participants, protecting user privacy without compromising the integrity of the blockchain.

To provide users with more control over their privacy, the development of user-centric privacy interfaces and tools is essential. User-centric interfaces can empower individuals to manage their privacy preferences effectively. For instance, users can choose to disclose information selectively, granting access only to authorized entities. Additionally, privacy-preserving tools, such as decentralized identity management systems and privacy-enhancing wallets, can enhance user privacy and give individuals greater control over their data.

Case studies have demonstrated the effectiveness of integrating these solutions into blockchain systems to enhance user privacy protection. These implementations have showcased improved privacy-preserving capabilities while maintaining the integrity and transparency of the blockchain.

In conclusion, to mitigate the privacy challenges posed by blockchain technology, it is crucial to implement effective solutions. By integrating zero-knowledge proofs, encryption techniques, privacy-focused consensus mechanisms, and user-centric privacy interfaces and tools, blockchain systems can enhance user privacy protection. These solutions ensure that users have control over their data, verify transactions without compromising privacy, and safeguard sensitive information within the blockchain.

C. Case Studies of Blockchain in Enhancing User Privacy

In this section, we present several case studies that showcase the use of blockchain technology in enhancing user privacy protection.

a) Case Study 1: Healthcare Data Management

One application of blockchain technology in enhancing user privacy is in healthcare data management. In traditional healthcare systems, patient data is often scattered across different healthcare providers and is susceptible to breaches and unauthorized access. By implementing blockchain technology, healthcare providers can securely store and manage patient data while ensuring the privacy of the users.

b) Case Study 2: Identity Management

Blockchain technology can also be used to enhance user privacy in identity management systems. Traditional identity management systems often rely on centralized authorities, making them vulnerable to data breaches and identity theft. By leveraging blockchain technology, users can have more control over their personal information and have the ability to selectively disclose their identity when necessary, thereby protecting their privacy.

c) Case Study 3: Financial Transactions

Blockchain technology has been widely adopted in the financial sector, particularly in cryptocurrencies. Cryptocurrencies like Bitcoin provide users with pseudonymity, allowing them to make transactions without revealing their true identity. This feature enhances user privacy in financial transactions and reduces the risk of identity theft and fraud.

d) Case Study 4: Supply Chain Management

Another case study of blockchain technology enhancing user privacy is in supply chain management. By utilizing blockchain, supply chain participants can track and authenticate the movement of goods without disclosing sensitive business information. This ensures privacy protection for all parties involved while maintaining transparency and accountability.

e) Case Study 5: Social Media Platforms

Some blockchain-based social media platforms have emerged to address privacy concerns in traditional social media platforms. These decentralized platforms allow users to have full control over their data, decide who has access to their information, and prevent the collection of personal data by third parties.

In conclusion, these case studies demonstrate the effectiveness of blockchain technology in enhancing user privacy protection. Blockchain can be applied in various domains such as healthcare data management, identity management, financial transactions, supply chain management, and social media platforms. By leveraging the transparency and security offered by blockchain, users can have greater control over their data and mitigate privacy risks.

V. CONCLUSION

This study investigates the human-computer interaction between blockchain technology and user privacy protection. Through a comprehensive literature review and analysis of existing blockchain systems, the impact of blockchain technology on user privacy protection has been examined. The results indicate that while blockchain technology offers transparency and immutability, it also poses challenges to user privacy due to the inherent characteristics of the blockchain.

Based on the findings, this study proposes effective measures to enhance user privacy protection in blockchain systems. The integration of privacy-enhancing techniques, such as zero-knowledge proofs and encryption, can effectively address user privacy concerns. These techniques allow for secure and private transactions on the blockchain while maintaining the transparency and immutability that blockchain technology provides.

Furthermore, case studies have shown the successful implementation of blockchain technology in enhancing user privacy. These cases demonstrate the effectiveness of privacy-enhancing techniques in protecting user data and ensuring confidentiality in blockchain transactions.

In conclusion, the study highlights the importance of considering user privacy protection when implementing blockchain technology. By incorporating privacy-enhancing techniques into blockchain systems, users can have increased confidence in the security and privacy of their transactions. As the use of blockchain technology continues to grow, it is imperative to prioritize user privacy and develop strategies to effectively protect personal information.

Conflict of Interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Data Availability Statement:

The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Author Contributions:

The author confirmed the contributions of the five authors and agreed to publish them.

Funding:

This work was supported by the Department of Education of Anhui Province (2019 Anhui University Humanities and Social Science key project, SK2019A0544).

Research on the Influencing Factors and Model Construction of Mobile Short Video User Experience: Based on Partial Students of Higher Education Institutions in Anhui Province.

Acknowledgments:

Strong support from the School of Computer Science, University of Northern Malaysia, Mainland China The author is grateful for the insightful comments suggested by the editor and the anonymous reviewers.

Compliance with Ethical Standards

Ethics Statement:

This research does not involve any plagiarism of others' work and respects all researchers

VI. REFERENCES

[1] F Voelter,N Urbach,J Padget.Trusting the trust machine: Evaluating trust signals of blockchain applications[D].International Journal of Information Management,2023

[2] KW Su,PC Chiu,TH Lin.Establishing a blockchain online travel agency with a human–computer interaction perspective[D].Journal of Hospitality & Tourism Technology,2022

[3] M Frhlich,F Waltenberger,L Trotter,et al.Blockchain and Cryptocurrency in Human-Computer Interaction: A Systematic Literature Review and Research Agenda[D].,2022

[4] J Gunaratne.Influencing Financial Decision-Making through Human-Computer Interaction Design Interventions[D].,2017

[5] Smith, Alisha J J. Definition and Development of a Measurement Instrument for Compellingness in Human-Computer Interaction[D].,2017

[6] K Wang.Human-Computer Interaction Design of Intelligent Vehicle-Mounted Products Based on the Internet of Things[D].Mobile Information Systems,2021
[7] BD Whitsell.Human-Robot Interaction Utilizing Asymmetric Cooperation and the Brain[D].,2017
[8] Deval Parikh, Sarangkumar Radadia, Raghavendra Kamarthi Eranna, 2024. “Privacy-Preserving Machine Learning Techniques, Challenges and Research Directions”, *International Research Journal of Engineering and Technology (IRJET)*, Volume 11, Issue 3, pp. 499-509. [Link].
[9] SA Amraii.Human-Data Interaction in Large and High-Dimensional Data[D].,2017
[10] A Rapp.Design fictions for learning: A method for supporting students in reflecting on technology in Human-Computer Interaction courses[D].Computers & Education,2019
[11] F Ren, Y Bao.A Review on Human-Computer Interaction and Intelligent Robots[D].International Journal of Information Technology & Decision Making,2019
[12] F Ren, Y Bao.A Review on Human-Computer Interaction and Intelligent Robots[D].,2020
[13] LI Peili,XU Haixia,MA Tianjun,et al.The Application of Blockchain Technology in Network Mutual Aid and User Privacy Protection[D].Netinfo Security,2018
[14] Dodiya, K., Radadia, S. K., & Parikh, D. (2024). "DIFFERENTIAL PRIVACY TECHNIQUES IN MACHINE LEARNING FOR ENHANCED PRIVACY PRESERVATION", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.11, Issue 2, page no.b148-b153, February-2024, Available: http://www.jetir.org/papers/JETIR2402116.pdf
[15] Y Lu, Q Tang, G Wang.ZebraLancer: Private and Anonymous Crowdsourcing System atop Open Blockchain[D].,2018
[16] Wander, Jeremiah D. D. Neural correlates of learning and intent during human brain-computer interface use.[D].,2015
[17] J Zhang. Interaction design research based on large data rule mining and blockchain communication technology[D]. Soft Computing, 2020.