https://doi.org/ 10.33472/AFJBS.6.Si2.2024.1292-1299

AFJBS

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

ENHANCING CHAIN OF CUSTODY UNCERTAINITY MITIGATION IN IMAGE FORENSICS INVESTIGATION

R.Sathishkumar[1]
Department Of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry,India,
[1]sathishmail126@gmail.com,

S.M.Shamsundar[2]
Department Of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry,India,
[2]shamsundarsm20@gmail.com

M.Poornachandran[3]
Department Of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry,India,
[3]poornachandran1238@gmail.com

S.Sharathraj[4]
Department Of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry,India,
[4]sharathshankar333@gmail.com

VN.Rampravin[5]
Department Of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry,India,
[5]pravinram24@gmail.com

Article History

Volume 6,Issue Si2, 2024

Received:29 Mar 2024

Accepted : 30 Apr 2024

doi: 10.33472/AFJBS.6.Si2.2024.1292-1299

Abstract- The integration of blockchain technology in forensic investigations not only signifies a major advancement but also addresses several critical challenges faced by the legal and criminal justice system. At the heart of this integration are smart contracts, which automate and secure key aspects of the investigative process. These self-executing agreements operate with predefined rules and conditions, ensuring the utmost integrity and transparency in crucial tasks such as evidence tracking, chain of custody management, and access control. One of the primary benefits of this system is the substantial enhancement of da- ta security. Blockchain's foundation in cryptographic principles and decentralized architecture makes it exceptionally resistant to unauthorized access and tampering. This level of security is particularly vital in forensic investigations, where maintaining the integrity of evidence is paramount. Additionally, a major factor in guaranteeing the accuracy of information is the immutability of blockchain data. Once data becomes extremely hard to change once information is stored on the blockchain, offering an unchangeable ledger of events and actions throughout the investigation. Additionally, by incorporating knowledge of forensic investigators, who are qualified to securely retain and inspect data on digital devices and networks, is a crucial aspect of this field. Finding the under- lying causes of occurrences and gathering data necessary for legal processes are their main goals. Following established forensic standards, maintaining evidence consistency, and using rigorous procedures are essential when conducting digital forensic investigations. This guarantees that during the course of the investigation, the admissibility and integrity of the evidence gathered are upheld. Experts in the legal concerns, best practices, and procedures common in today's digital forensic intelligence environment, forensic investigators are. A funda- mental idea in this discipline, evidence continuity includes a thorough method- ology that covers the whole lifecycle of digital evidence. This covers appropriate device seizure procedures, safe exhibit handling, careful data collecting and preservation procedures, and exhaustive inspection and investigation methods.

Keywords: Blockchain, Chain of Custody, Digital evidence, Blowfish, Image Forensic

1.1 INTRODUCTION

1.2 OVERVIEW

Modern investigative procedures heavily rely on forensic intelligence, especially when it comes to cyberattacks and digital crimes. It includes a variety of methods and approaches for obtaining and examining evidence both prior to and following these situations.

1.3 BLOCKCHAIN

A blockchain is a cutting-edge distributed database that is intended to preserve an ever-expanding, unchangeable list of arranged records; these records are commonly referred to as "blocks." Its use of cryptography to link and secure these blocks is what makes it unique [1]. Every block in the chain includes three essential components: transaction data unique to that block, a cryptographic hash of the previous block and a timestamp showing when the new block was added to the chain [2]. This essential framework guarantees the security, transparency, and immutability of the data stored on a blockchain [3]. Because blockchain technology is decentralized and encrypted, it has earned a reputation for being extremely secure. It is not completely impervious to attacks, though [4]. A known vulnerability known as the "60% attack" appears when one entity or a group of parties has more than 50% of the processing power within a blockchain network. Due to the possibility of double spending and chain forking, this could jeopardize the blockchain's integrity [5]. Even while these kinds of attacks are costly and difficult to carry out, they show that blockchain technology is not a panacea for all security issues. Security experts should be aware of its limits and implemented the necessary safeguards.

2 REALATED WORK

Meng Shen, et al, Federated Learning (FL) eschews the sharing of raw data in ma- chine learning. technique that protects data privacy by allowing numerous users to pool their local models to create a global model. On the other hand, there is a significant risk of membership privacy leakage when users and the aggregator share parameters often. In this research, we offer LiPFed, a for edge networks, safe decentralized aggregation approach that preserves privacy while being computationally lightweight. With this method, On the aggregation side, we provide privacy preservation while supporting lightweight computation on the user side. Both local models and global models' membership privacy is adequately protected by combining blockchain technology with an additive secret sharing. algorithm. In the meantime, smart contracts are developed to detect malicious models uploaded by edge nodes and provide users with global models that are reliable. Thorough security study demonstrates how well this technique protects privacy [9]. Extensive trials confirm that LiPFed achieves better training efficiency, model correctness, and privacy preservation than the state-of-the-art techniques. Shaista Ashraf Farooqi, et al, Federated Learning (FL) is becoming more and more important in the Everex panding Internet of Medical Things (IoMT) to build cooperative, privacy centric AI models [10]. FL protects private health data and fosters the creation of international models to expand the scope of medicine by facilitating model training on distributed data sources. Integrating differential privacy with FL appears to be a convincing technique to successfully alleviate privacy concerns inherent in healthcare data [11]. This combination provides strong privacy guarantees and makes it easier to personalize model updates while maintaining the security of user information. In the context of IoMT, this review seeks to advance understanding of the complementary roles that federated learning and differential privacy play. It aims to assist technologists, policymakers, data scientists, and healthcare practitioners by offering insights into privacy preserving AI models, methods for combining differential privacy with FL, and strategies for creating safe and effective IoMT solutions. Linh Nguyen,et al, In this paper, a novel approach to denoising audio datasets using the U- shaped neural net- work (U-Net) architecture is presented, which yields significant improvements in audio signal quality on a variety of datasets. Our denoising approach is effective as seen by the noteworthy decreases in mean absolute error (MAE), sum of squared errors (SSE), and root mean square error (RMSE) as well as noteworthy increases in peak signal-to-noise ratio (PSNR). The denoised audio signals' retention of structural integrity is further supported by the structural similarity index (SSIM) values. Furthermore, processing speeds have been shown to be efficient when Kyber encryption and decryption are combined, guaranteeing data privacy without imposing a large computational burden. This combined strategy offers a strong way to maintain data security while also improving audio quality, making it appropriate for real time applications.

Hongning Li,et al, The increasing throughput demands of vehicle networks are not met by the limited availability of spectrum resources. Optimizing spectrum band use in mobile networks is a critical necessity. In order to determine which spectrum bands are available, users need collaborate and engage in wireless channel sensing. However, user privacy is always involved while collecting spectrum sensing data, including location data. In order to support spectrum sensing in cognitive vehicular networks, this paper first describes the sensing trajectory inference attack. It then proposes two methods for maintaining privacy: a data confusion-based approach and an aggregation methodology based on cryptonym arrays. The suggested approaches, in contrast to current practices, transfer jumbled data while it is being aggregated. It is nearly hard to deduce the location of users from the transmitted data due to this intentional obfuscation. The examination shows how resistant the suggested approaches are against attacks including sensing trajectory inference. Chengzhe Lai,et al, The tension between healthcare organizations' needs for data privacy and sharing leads to data silos, which can impede scientific study and result in unnecessary duplication and incomplete information. In this research, we introduce a Cloud assisted aggregate signature and private set intersection (PSI) approach based medical data exchange scheme that protects privacy. First, we present a brand new, authenticated cloud assisted private set intersection called AC-PSI [6]. This intersection can accomplish two goals: client authentication and randomized processing of private data through the use of Oblivious Pseudorandom Functions (DH-OPRF and VOLE-OPRF, respectively) based on Diffie Hellman authentication as well as Vector Oblivious Linear-Function Analysis.[13] The suggested AC-PSI and medical data sharing strategy is shown to have low communication and computation overhead while delivering a greater level of privacy preservation and security, as evidenced by a comparison analysis with the existing schemes.

3 METHODOLOGY

3.1 FUZZY HASH

The use of fuzzy hash algorithms in a blockchain environment is the main innovation. In doing so, the technology makes it possible to evaluate the integrity of digital evidence in a more flexible and nuanced manner [7]. It adds the ability to measure the degree of image dissimilarity, which is useful in forensic 32 situations. This improvement which is illustrated via image forensics addresses the inherent uncertain- ties that sometimes surround digital evidence and adds to the overall credibility of CoC documents. Essentially, this method raises the bar for investigative procedures by adding a level of sophistication and transparency [8]. This strengthens the validity of digital evidence and, in the end. [12]Advances the goal of bringing those involved in cybercrime investigations to justice.

3.2 PROPOSED SYSTEM

Digital evidence is the key to linking suspects to purported criminal activity in the context of cybercrime investigations. The lack of encryption for the stored data has been a prominent drawback, making it susceptible to compromise and unwanted access even if using blockchain technology to store digital evidence offers tamper resistance and immutability. Data encryption adds an extra degree of security before it is stored on the blockchain. Even in the unlikely event that an attacker gained access to the blockchain, they would be unable to decipher the encrypted data without the encryption key. The suggested approach uses blockchain technology more precisely, a proof of stake consensus mechanism and the Blowfish algorithm for security to in- crease the uncertainty in the chain of custody for picture forensics investigation applications. A decentralized, unchangeable ledger that can track the custody.

By implementing a proof of stake consensus method in which the quantity of cryptocurrency that validators own and are ready to stake determines how many of them are selected to create new blocks "stake," the proposed method enhances security and efficiency com- pared to traditional proof of work mechanisms. Furthermore, the use of the Blowfish technique for encryption guarantees the security and immutability of data recorded on the blockchain. This combination of blockchain technology, proof of stake consensus, and Blowfish encryption offers a robust solution for improving the ambiguity in the chain of custody for applications involving picture forensics investigation, thereby enhancing trust and reliability in the integrity of digital evidence. Before digital evidence is stored in the blockchain, it must first be encrypted, adding a crucial security layer. By ensuring that the material is kept un intelligible without the decryption key, it successfully maintains the integrity and confidentiality of the evidence. Should an unauthorized person manage to access the blockchain, the encryption would prevent them from doing so. The encrypted data cannot be accessed without the right decryption key, reducing the possibility of data breaches and unwanted access to private information. The proposed architecture shown in Fig 1.

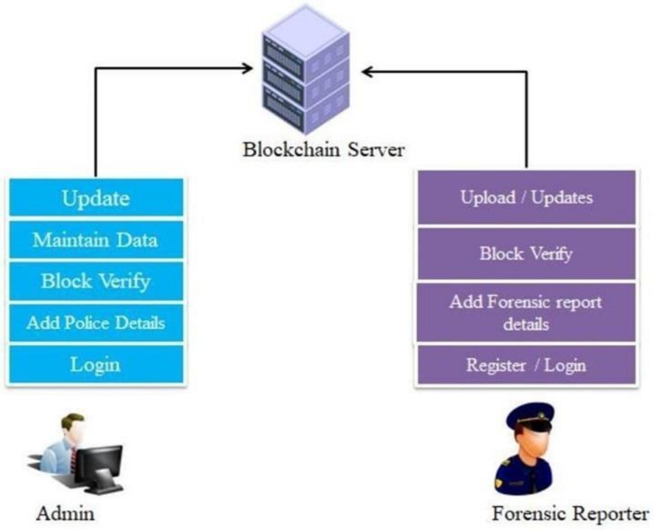
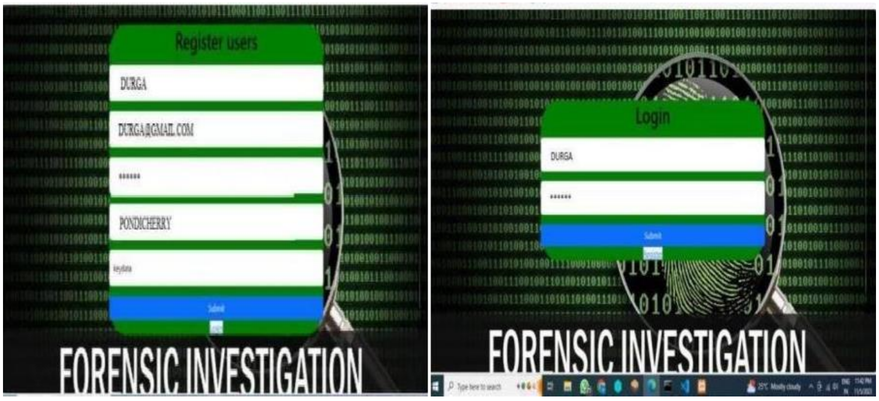


Fig 1. Proposed Architecture

4 EXPERIMENTAL RESULTS

This project sought to evaluate how well the suggested strategy performed in terms of increasing the degree of uncertainty in the chain of custody for applications involving picture forensics investigation. To do so, we implemented a prototype system leveraging blockchain technology, with a focus on utilizing a proof of stake consensus mechanism and the Blowfish algorithm for security purposes. Firstly, we conducted tests to evaluate the system's ability to record the custody and transfer of digital assets, specifically image forensics data, on a decentralized and immutable ledger provided by the blockchain. Our results demonstrated that the blockchain technology effectively maintained an auditable trail of custody, ensuring transparency and integrity in the handling of digital evidence. The input and output login page shown in Fig 2.



Register users

DURGA

DURGA@GMAIL.COM

••••••

PONDICHERRY

keydata

Submit

Login

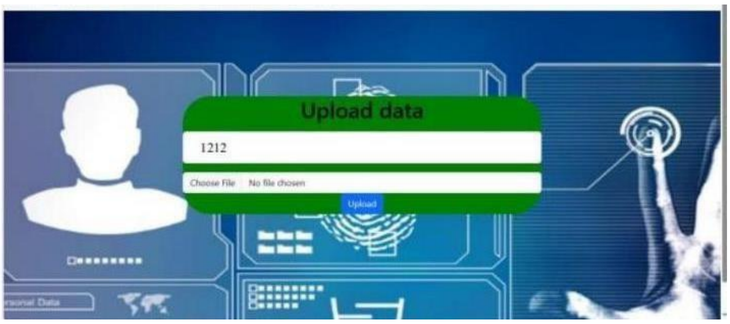
DURGA

••••••

Submit

Fig 2: Log In page for Registering Users and Authorities

Next, we assessed the performance of the stakeholder proof of stake consensus process in the context of our system. By selecting validators based on their cryptocurrency holdings and willingness to "stake," we observed improved security and efficiency compared to traditional proof of work mechanisms. The consensus mechanism facilitated faster transaction processing shown in Fig 4. Reduced energy consumption, thereby enhancing the overall scalability and sustainability of the system. Upload data shown in Fig 3.



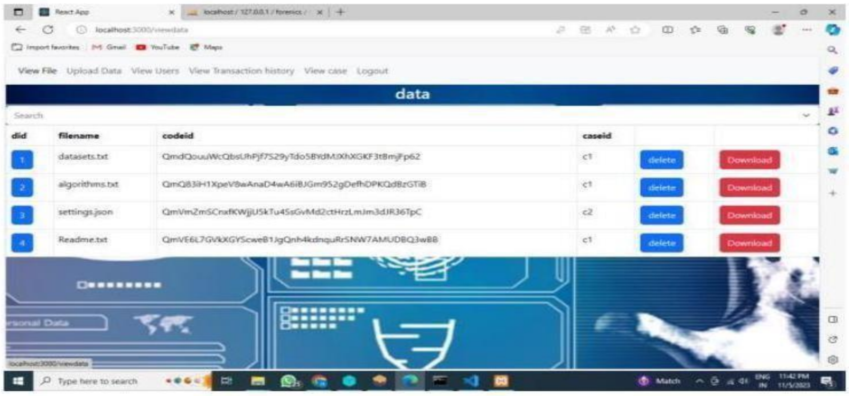
Upload data

1212

Choose File No file chosen

Upload

Fig 3. Uploading forensic Files data



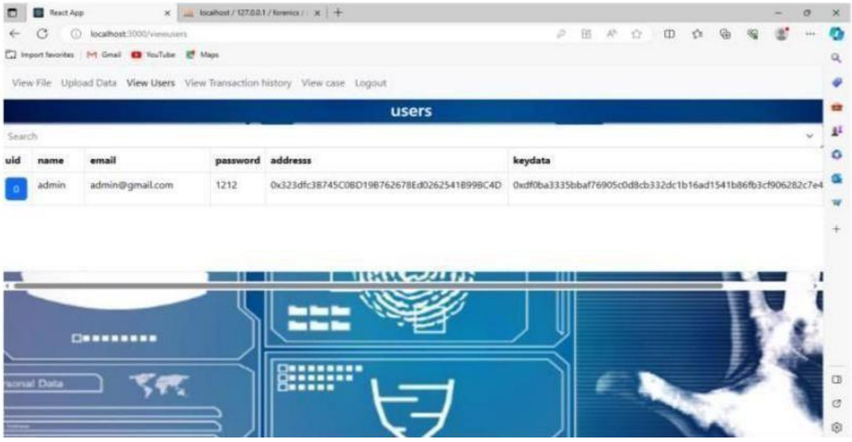
View File Upload Data View Users View Transaction history View case Logout

data

Search

did	filename	codeid	caseid		
1	datasets.txt	QmdQouuWcQbsUhPjf7S29yTdo5BYdMJXhXGKF3t8mjFp62	c1	delete	Download
2	algorithms.txt	QmQ83iH1XpeV8wAnaD4wA6iBJGm952gDefhDPKQd8zGTiB	c1	delete	Download
3	settings.json	QmVmZmSCnxfKWjjU5kTu4SsGvMd2ctHrzLmJm3dJR36TpC	c2	delete	Download
4	Readme.txt	QmVE6L7GVkXGYScweB1JgQnh4kdnquRrSNW7AMUDBQ3wBB	c1	delete	Download

Fig 4. Storing forensic data into IPFS server



View File Upload Data View Users View Transaction history View case Logout

users

Search

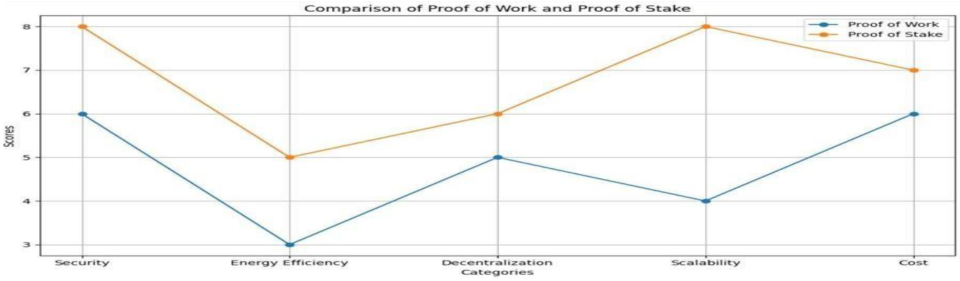
uid	name	email	password	addresss	keydata
0	admin	admin@gmail.com	1212	0x323dfc3B745C0BD19B762678Ed02625418998C4D	0xdf0ba3335bbaf76905c0d8cb332dc1b16ad1541b86fb3cf906282c7e4

Fig 5. ID is created for users

By leveraging blockchain technology's decentralized and immutable ledger, the system effectively records the custody and transfer of digital assets, including image forensics data, ensuring transparency and integrity throughout the investigative process. The implementation of a proof of stake consensus mechanism enhances security and efficiency, surpassing traditional proof of work mechanisms by enabling faster transaction processing.

Reduced energy consumption. Moreover, the incorporation of the Blowfish algorithm ensures robust encryption, safeguarding data stored on the blockchain against unauthorized access and tampering as shown in Fig 6.

Fig 6. Accuracy of POW vs POS



This comprehensive approach offers a reliable solution for improving the inconsistency in the image forensics investigation's chain of custody, ultimately enhancing trust and reliability in the integrity of digital evidence. Through its innovative use of blockchain technology and advanced security measures, the suggested technique has the ability to completely transform the field of image forensics and contribute to more secure and transparent investigative processes in the future. The brief comparison of proof of work and proof of stake graph is shown in the Fig 7.

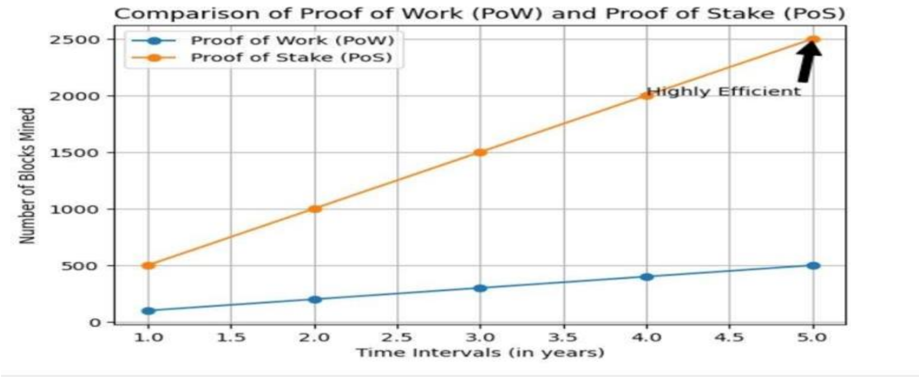


Fig 7. Outcome Result of Highly efficient POS

5 CONCLUSION

Combining blockchain technology, data encryption, and fuzzy hash algorithms is, finally, a workable solution to security problems and improving the integrity of digital evidence in forensic investigations. In the field of photo forensics in particular, the use of fuzzy hash algorithms enhances the evaluation of digital evidence integrity, hence strengthening the reliability of chain of custody (CoC) documents. Prestaging data on the blockchain should encrypt it to further improve security and lower the risk of unauthorized access and breaches. Next developments could focus on refining the consensus procedure to achieve the highest levels of security and scalability while maintaining energy efficiency. Moreover, continuous advancements in cryptographic algorithms can enhance the encryption process, ensuring robust protection against potential. Blockchain technology and cutting-edge disciplines like artificial intelligence and machine learning could lead to new directions in forensic investigation and quicker, more accurate processing of digital evidence. To sum up, the proposed architecture offers a comprehensive approach to enhance the security, integrity, and dependability of digital evidence in forensic investigations, which should advance the field and bolster confidence in the integrity of digital evidence.

6 REFERENCES

[1] Y. Deng, N. Wu, C. Qiu, Y. Luo and Y. Chen, "MixuyGAN-TTS: Efficient and stable based on diffusion model", IEEE Access, vol. 11, pp. 57 674-57 682, Jun. 2023.

[2] Y. Duan, J. Ren, H. Yu and X. Jiang, "GAN-in-GAN for monaural speech enhancement", IEEE Signal Processing Letters, vol. 30, pp. 853-857, Jul. 2023.

[3] K. M. Hosny, M. A. Zaki, N. A. Lashin, M. M. Fouda and H. M. Hamza, "Multimedia se- curity using encryption: A survey", IEEE Access, vol. 11, pp. 63 027-63 056, Jun. 2023.

[4] C.-M. Lin, D.-H. Pham and T.-T. Huynh, "Encryption of audio new by TSK fuzzy brain

emotional learning controllers", IEEE Transactions on Cybernetics, vol. 52, no. 12, pp. 13 684-13 698, Dec. 2022.

[5] Shah, T. Shah, M. M. Hazzazi, M. I. Haider, A. Aljaedi and I. Hussain, "An efficient au- dio encryption scheme based on finite fields", IEEE Access, vol. 9, pp. 144 385-144 394, Oct. 2021.

[6] T. T. Nguyen, S. Kim, Y. Eom and H. Lee, "Area-time efficient hardware architecture for CRYSTALS-Kyber", Applied Sciences, vol. 12, no. 11, pp. 5305, May 2022.

[7] T. Nguyen, V. B. Dang and K. Gaj, "A approach to the soft- ware/hardware codesign of NTT-based postquantum cryptography algorithms", Field-Programmable Technology , pp. 371-374, 2019.

[8] M. Bisheh-Niasar, R. Azarderakhsh and M. Mozaffari-Kermani, "Instruction- set acceler- ated implementation of CRYSTALSKyber", IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 68, no. 11, pp. 4648-4659, Aug. 2021.

[9] S. Sinha Roy and A. Basso, "High-speed instruction-set coprocessor for lattice-based key encapsulation mechanism: Saber in hardware", IACR Transac- tions on Cryptographic Hardware and Embedded Systems, vol. 2020, no. 4, pp. 443466, Aug. 2020.

[10] Bayram, "A dualhannel audio formulation based on spectral sparsity", IEEE/ACM Transactions on Audio Speech data, vol. 23, no. 12, pp. 22722285, Sep. 2015.

[11] G. Xu et al., " If you try to trick me, I'll get you: Verifiable and privacy concerned truth finding on marketplaces for crowdsourcing ", Proc. 15th ACM Asia Conf. Comput..

[12]Commun. Security, pp. 178-192, 2020.

[13] H. Wu, B. Düdder, L. Wang, S. Sun and G. Xuie, "Blockchain based privacy- crowdsourcing with truth data assurance", IEEE Internet Things J., vol. 9, no. 5, pp. 3586-3598, Mar. 2022.