AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

PRIVACY-FOCUSED REDACTABLE BLOCKCHAIN WITH RESTRICTED ACCESS IN DECENTRALIZED ECOSYSTEMS:

Syeda Kulsum[1], Dr. Lalitha Saroja CH[2], Ruqiya Fatima[3]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, Syedakulsum6054@gmail.com
[2]Assoc Professor, Department of CSE, Shadan Women's College of Engineering and Technology lalithasarojathota@gmail.com

ABSTRACT:
Redactable blockchain, which provides decentralization, traceability, and transparency while permitting permitted changes to on-chain data, has become a promising technology in recent years. Despite their benefits, existing redactable blockchain systems are limited in their practical use by issues including significant communication overhead and data privacy breaches. This study presents PriChain, a fine-grained redactable blockchain technology for decentralized contexts that preserves privacy in order to address these problems. PriChain gives data owners the authority to manage who may access and alter their on-chain data, guaranteeing that redaction can only be carried out by authorized users while maintaining data confidentiality. Through the use of attribute-based encryption with several authorities, PriChain guarantees resistance to unwanted cooperation or collusion and permits exact access control. When compared to traditional techniques, the framework dramatically lowers communication and storage overhead. PriChain is a reliable and useful option for blockchain applications that prioritize privacy as security analysis demonstrates that it is impervious to chosen-plaintext attacks.
KEYWORDS: Blockchain, Fine-grained redaction, Privilege downward compatibility, Privacy preservation

1. INTRODUCTION

Due to its special feature of data redaction, the redactable blockchain has garnered a lot of interest from both academic and business perspectives since it was first introduced. Since the beginning, the original blockchain technique's immutability has been a double-edged sword. While it can make blockchain extremely trustworthy, it also prevents its further application for new requirements that have emerged during the development of modern society, such as the right to be forgotten under the General Data Protection Regulation (GDPR). Furthermore, immutability implies that all subsequent blockchain users run the danger of spreading bad material once it reaches the original blockchain and are unable to redact it. In order to lessen the original blockchain's immutability and prevent the dissemination of illicit information, the idea of a redactable blockchain was put out. Redactable blockchain has been the subject of several proposals in recent years. In order to achieve a coarse-grained block-level rewriting in centralized settings, Ateniese first presented an improved collision-resistant chameleon hash and public key architecture. Following Ateniese, Derler developed a redactable blockchain paradigm using a linear secret sharing scheme (LSSS) and policy-based chameleon hash (PCH) to achieve fine-grained rewriting. The aforementioned two systems have a rapidly increasing communication cost due to their centralized architecture, lacking encryption and searching tools. Additionally, they created an accountable rewriting system with rudimentary property accountability that was influenced by PCH in centralized settings. However, it lacked privacy protection features and had poor searching performance. The aforementioned redactable blockchains created in centralized environments have a number of security issues, including illicit block-level tampering and malicious rewriting and selling, which can result in grave security violations. Therefore, to address these issues and improve security, they created a DPCH (decentralized policy-based chameleon hash) structure and constructed their decentralized redactable blockchain based on DPCH. However, the connection overhead and search running time have increased to an unprecedented level when decentralized settings were introduced. In general, despite the numerous proposals for redactable blockchain, there are still three obstacles to its implementation. Privacy violations are the first restriction. Current redactable blockchain methods transmit visible data without encryption, which leads to serious privacy violations and abuses. Furthermore, we observe that under basic encryption, data cannot be put directly into redactable blockchains since the person who can redact the data should also be able to decode it. To put it another way, the encryption method needs to be downward compatible with fine-grained data rights. Unbearable communication overhead is the second restriction. The number of requests and the amount of the policy have increased.

2. STIMULATING

The PriChain project involves designing and implementing a fine-grained redactable blockchain infrastructure that is appropriate for decentralized situations while maintaining privacy. In order to provide secure redaction without sacrificing secrecy, the system is designed to give data owners total control over who may view and alter on-chain data. By using multi-authority attribute-based encryption (MA-ABE), which allows for exact access restriction based on user attributes, it mitigates the privacy issues seen in traditional redactable blockchains. PriChain maintains the effectiveness of data retrieval and search activities while reducing the unnecessary

communication and storage overhead seen in previous systems. The framework is applicable to situations where sensitive data, including financial records, legal papers, or personal data storage, must be maintained on blockchain. Its architecture provides resilience against malevolent rewriting and guarantees resistance against illegal collaboration or collusion. Only authorized users can selectively decrypt and redaction data thanks to the project's systems supporting fine-grained data permissions. Additionally, PriChain is scalable, which enables the system to effectively manage a high volume of users, policies, and transactions. By enabling the right to be forgotten in a safe and auditable way, it guarantees adherence to data privacy laws like GDPR. Applications that need both selective mutability for allowed repairs and immutable audit trails can use this framework. While cryptographic safeguards preserve security, its decentralized structure reduces single points of failure and improves transparency. The technology can also be utilized as a paradigm for future redactable blockchains that prioritize privacy. The project's overall goal is to offer a workable, safe, and effective way to handle sensitive on-chain data in decentralized systems.

3.OBJECTIVE

The PriChain project's main goal is to create a fine-grained, redactable blockchain architecture that protects privacy and allows safe management and regulated alteration of on-chain data. By giving data owners the power to decide who can access and redact their data, it seeks to guarantee that only authorized users make changes. By using multi-authority attribute-based encryption (MA-ABE) for strong access control, the project aims to solve the privacy violations frequently found in current redactable blockchain systems. Reducing communication and storage overhead while preserving high data retrieval and search performance is another goal. PriChain works to safeguard private information from malevolent influence by preventing illegal cooperation or collusion. Scalability is another goal of the framework, which enables the system to efficiently manage a large number of users, characteristics, and transactions. It seeks to preserve a visible and auditable blockchain history while enabling safe redaction. In order to enable features like the right to be forgotten, the project also plans to adhere to data protection laws like GDPR. Another important goal is to improve system dependability and usability in decentralized settings. Additionally, the research focuses on offering a workable solution for applications that need both selective mutability and immutability. It hopes to set the standard for next redactable blockchain systems that prioritize privacy. Additionally, the system aims to be applicable to other businesses that need data management that is both safe and verifiable. Overall, the objective is to create a robust, efficient, and secure blockchain framework that balances transparency with data privacy. The project also emphasizes ease of adoption and integration into existing decentralized ecosystems.

3.1 What The Project Is About

Redactable blockchains have brought to light significant difficulties in striking a balance between data privacy and immutability, rendering current systems inadequate for real-world uses. Because data is sent and kept without strong encryption, sensitive information is exposed to unauthorized users in current redactable blockchain frameworks, which frequently suffer from serious privacy breaches. Conventional methods also have intolerable communication overhead, which makes the system ineffective and challenging to scale as user demands and policy complexity rise. Additionally, it takes a lot of time to search and retrieve specific data from big ciphertext collections, which lowers operating efficiency. While decentralized settings increase communication and computation costs, centralized alternatives to redactable blockchains fall short in addressing security issues including malicious rewriting and unauthorized tampering. The secure deployment of sensitive data on-chain is limited by the lack of encryption that is compatible with selective redaction. Trust in blockchain applications is further undermined by the inadequacy of current frameworks in preventing collusion and illegal sharing. The use of redactable blockchains for privacy-critical situations is still limited if these issues are not resolved. Additionally, there is a lack of adherence to legal requirements such as GDPR, especially with regard to the right to be forgotten. Developing a system that maintains efficiency, security, and usability in decentralized systems while protecting data confidentiality and selective mutability is the major problem.

4. EXISTING SYSTEM:

When data has to be updated or deleted while preserving the fundamental blockchain characteristics of decentralization, traceability, and immutability, these methods are helpful. Nevertheless, the majority of current redactable blockchain techniques have serious drawbacks. They often have data privacy breaches, which allow unauthorized users to see sensitive on-chain data even during or after redaction. Furthermore, these systems frequently rely on complex cryptographic methods with substantial computing and communication overhead, such modular exponentiation, bilinear pairings, and map-to-point hash functions. They are less appropriate for real-time or resource-constrained applications because of these resource-intensive procedures. Furthermore, searching and locating specific data on-chain in such systems tends to be inefficient, adding further operational delays and complexity.

4.1 Existing System Disadvantages:

- Their lack of fine-grained access control limits the flexibility of who may see or alter data.
- They also have high communication and storage overhead.

4.2 THE PROPOSED SYSTEM

In a decentralized redactable blockchain context, this cryptographic technique is essential for providing fine-grained access control. In contrast to conventional single-authority models, MA-ABE permits the management and distribution of user characteristics and associated cryptographic keys by several independent authorities. In the context of the overwritten abstract, this implies that, according on the characteristics supplied to each user, data owners can determine who is authorized to access or redact certain on-chain data. Because no one authority can independently decrypt or abuse the data, this strategy greatly increases data privacy and provides collusion resistance. Additionally, MA-ABE ensures downward compatibility, meaning that if a user has the authority to redact data, they also naturally have the permission to read it. Because of this, the PriChain system avoids the performance issues associated with previous redactable blockchain methods and is both highly adaptable to decentralized settings and safe and privacy-preserving.

4.2.1 Proposed System Advantage

- Ensures that only authorized users can view or redact data by providing privacy-preserving access control.
- Guarantees downward compatibility, which gives redactors read access by default.
- Increases data confidentiality without compromising openness or traceability.

5. METHODOLOGIES

1. Design of User Interfaces

The user must enter their username and password in order to connect to the server. The user can log in to the server directly if they have previously left; otherwise, they must register their information, including their username, password, email address, city, and country. To manage upload and download rates, the database will generate an account for every user. The user ID will be used as the name. To access a particular website, you often need to log in. The query will be searched and displayed.

2.Multi-Authority Attribute-Based Encryption (MA-ABE)

The primary access-control method in this project is Multi-Authority Attribute-Based Encryption (MA-ABE), which enforces decentralized and fine-grained permission management. Multiple authorities oversee various sets of properties, including user roles, access type (read or read/redact), and approval status, rather than depending on a single trusted authority. Users must meet the necessary attribute policies specified by the data owner and validated by the authority module during file access requests. Only users with legitimate attribute combinations are able to decrypt or alter the protected data thanks to MA-ABE. By removing single-point authority failures and enhancing scalability, this method improves security. Additionally, it facilitates controlled redaction, which enables authorized users to modify data without disclosing encryption keys to unapproved parties. The solution delivers safe, policy-driven access control that is compatible with decentralized contexts by incorporating MA-ABE. This strategy guarantees privacy, adaptability, and confidence among various parties engaged in the data-sharing procedure.

3.Block chain

The project uses blockchain technology to manage sensitive file activities with immutability, transparency, and trust. A blockchain-inspired immutable workflow is used for all crucial processes, including file uploads, access approvals, redaction permissions, and request status updates. Unauthorized manipulation is prevented since once a file or request is accepted, it cannot be changed without the appropriate authority. In decentralized systems, blockchain guarantees the tamper-proof preservation of transaction history and access data. As a layer of governance, the authority module verifies operations prior to their commit. This distributed ledger method improves system dependability by eliminating reliance on a centralized server. By keeping a verifiable record of file access and change activities, it also facilitates auditability. By integrating blockchain concepts, the project ensures data integrity, accountability, and secure collaboration among data owners and users.

4. SHA-256

The project uses SHA-256 to provide data integrity, authentication, and safe file and access key verification. A SHA-256 hash is created when a file is submitted in order to uniquely reflect the original material without disclosing its contents. Any unlawful changes to the stored file can be found with the aid of this hash. Secure secret keys, which are necessary for file access verification, are likewise generated using SHA-256. The system uses the stored hash to verify the file's validity during download or redaction requests. This ensures that even if several copies of the data are made, the original data will not alter. The hashing method improves defense against replay and manipulation. The concept establishes a strong security foundation by integrating SHA-256 with encryption and blockchain technology. This ensures trust, integrity, and consistency across all data operations in the system.

6. TECHNIQUE ALGORITHM USED

6.1 Proposed Algorithm

- **Multi-Authority Attribute-Based Encryption (MA-ABE) Algorithm**

This project uses the MA-ABE algorithm to enable decentralized, fine-grained access control over

encrypted data. MA-ABE enables access decisions to be based on user factors including role, approval status, and access type (read or read/redact), in contrast to conventional encryption. The reliance on a single reliable authority is eliminated by the independent issuance of attribute keys by several authorities. An access policy is created using characteristics rather than user IDs when a data owner uploads a file. Only if the user's attribute set complies with the authorities' imposed policy may they decrypt the file. In decentralized settings, scalability and adaptability are essential, and our algorithm offers both. Only authorized users are able to carry out read or read/redact actions in this project thanks to MA-ABE. The method eliminates unwanted data leaks and improves secrecy. All things considered, MA-ABE is essential to implementing safe, policy-driven access control that is in line with the project's privacy goals.

- **Block chain Algorithm**

Every transaction in this project's distributed ledger, including doctor registration, patient file uploads, and laboratory report production, is recorded in a safe, verifiable chain of blocks. Digital signatures, hash values, timestamps, and encrypted file contents are all included in each block and are connected via cryptographic connections based on past and present hashes. The block chain method guarantees that all records are verified by a consensus process prior to being added to the chain, hence removing the single point of failure present in conventional centralized healthcare systems. In project, this guarantees data authenticity, traceability, and resilience, making it impossible for attackers to alter or forge medical records without detection.

- **SHA-256 Algorithm**

The project uses the SHA-256 algorithm, a cryptographic hash function, to ensure data authenticity and integrity during all transactions. A distinct 256-bit hash value that serves as a digital fingerprint is established each time a doctor, patient, or file is created. It is simple to identify any tampering since even a slight modification to the file or identification data entirely changes the hash. SHA-256 is used in this project to provide hash values for patient and physician IDs as well as for each block of an encrypted patient file kept in the block chain. This guarantees medical data's traceability and immutability, shielding it against alteration or fabrication. By connecting the hash of each block to the next, the algorithm further facilitates the decentralized character of the system.

6.2 EXISTING SYSTEM

- **Redactable blockchain**

To put it simply, homomorphic encryption is a redactable blockchain technology that allows blockchain data to be altered or removed under specific approved circumstances. When data has to be updated or deleted while preserving the fundamental blockchain characteristics of decentralization, traceability, and immutability, these methods are helpful. Nevertheless, the majority of current redactable blockchain techniques have serious drawbacks. They often have data privacy breaches, which allow unauthorized users to see sensitive on-chain data even during or after redaction. Furthermore, these systems frequently rely on complex cryptographic methods with substantial computing and communication overhead, such modular exponentiation, bilinear pairings, and map-to-point hash functions. They are less appropriate for real-time or resource-constrained applications because of these resource-intensive procedures. Furthermore, searching and locating specific data on-chain in such systems tends to be inefficient, adding further operational delays and complexity.

7. SYSTEM ARCHITECTURE

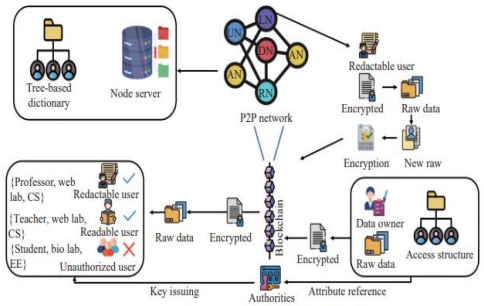
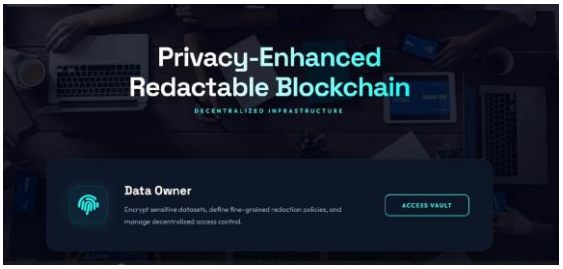
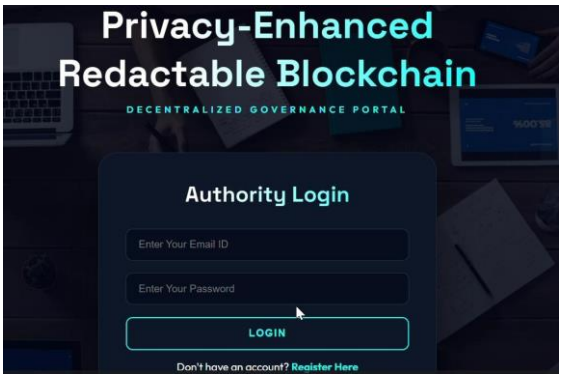
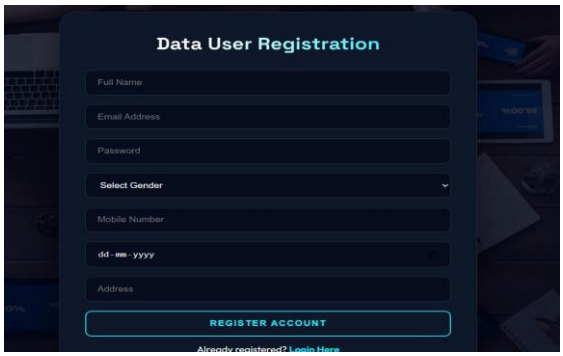


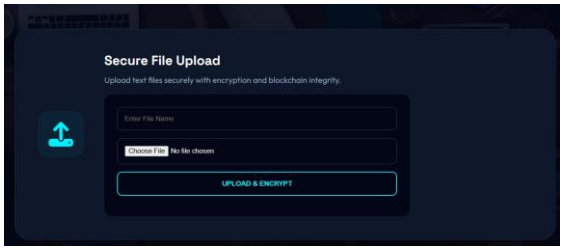
FIG:7 System Architecture

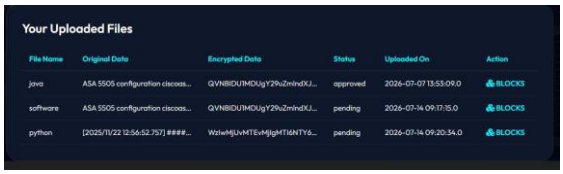
8. RESULTS











9. CONCLUSION

In summary, this project effectively demonstrates a safe and private data exchange system based on blockchain technology and Multi-Authority Attribute-Based Encryption (MA-ABE). Controlled and responsible data access is ensured by the system's efficient division of duties among the Data Owner, Data User, and Authority modules. The project's usage of MA-ABE improves scalability and flexibility by enabling fine-grained access control based on user traits rather than IDs. By ensuring that data consumers only receive the amount of information that is allowed, the read/redact policy mechanism helps to reduce needless data exposure. For all access requests and approvals, blockchain integration offers immutability, transparency, and a trustworthy audit trail. By making it simple to identify any tampering with stored files, SHA-256 hashing improves data integrity. The Authority module is essential for managing trust between various entities, enforcing policies, and validating attributes. Unauthorized access is absolutely prohibited thanks to secure request-approval protocols. Each component may operate and be maintained independently thanks to the modular architecture. By spreading confidence across several authorities, the system reduces single-point failures. Verifiable access logs kept on the blockchain provide user responsibility. The project shows how decentralized technology and cryptographic enforcement might cooperate to address practical data privacy issues. Overall, sensitive data security, integrity, and restricted accessibility are achieved by the suggested method. It offers a workable basis for safe data exchange in remote and cloud systems. The architecture is resilient, scalable, and flexible enough to accommodate changing security needs.

9.2 FUTURE ENHANCEMENT

While maintaining the current design, future improvements to this project can further improve security, scalability, and usability. Authorities can change or revoke user attributes in real time without re-encrypting whole datasets by extending the MA-ABE module to include dynamic attribute revocation. By allowing partial content access rather than whole-file control, fine-grained field-level redaction can improve the present read/redact policy. By using smart contracts to automate file access request approval processes and do away with human authority interaction, blockchain integration may be further enhanced. By upgrading the Authority module to a completely decentralized multi-authority governance architecture, trust may be increased and single-point control can be decreased. Integrating off-chain storage solutions, such IPFS, for encrypted data while keeping hashes on the blockchain can boost performance. Authorities can trace access patterns and policy infractions by adding sophisticated real-time monitoring dashboards to enhance auditability. Incorporating AI-based anomaly detection can assist in spotting questionable access patterns or credential abuse. Additionally, cross-domain data sharing across entities with federated authority can be supported by expanding the system. To increase accessibility for owners and users, mobile and API-based access can be implemented. Threshold cryptography is one example of an enhanced key management technique that can increase resistance to key compromise. To comply

with data protection laws like GDPR, compliance elements might be incorporated. All things considered, these improvements will maintain the fundamental objectives of safe, policy-driven data exchange utilizing MA-ABE and blockchain technology while increasing the system's adaptability, intelligence, and scalability.

REFERENCES

[1] Y. Liu, L. Xu, X. L. Yuan, et al., "The right to be forgotten in federated learning: An efficient realization with rapid retraining," in IEEE Conference on Computer Communications, London, UK, pp. 1749–1758, 2022.
[2] M. Ferreira, T. Brito, J. F. Santos, et al., "RuleKeeper: GDPR-aware personal data compliance for web frameworks," in IEEE Symposium on Security and Privacy, San Francisco, CA, USA, pp. 2817–2834, 2023.
[3] G. Ateniese, B. Magri, D. Venturi, et al., "Redactable blockchain-or-rewriting history in bitcoin and friends," in IEEE European Symposium on Security and Privacy, Paris, France, pp. 111–126, 2017.
[4] D. Derler, K. Samelin, D. Slamanig, et al., "Fine-grained and controlled rewriting in blockchains: Chameleon-hashing gone attribute-based," in 26th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, 2019.
[5] S. M. Xu, X. Y. Huang, J. M. Yuan, et al., "Accountable and fine-grained controllable rewriting in blockchains," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 101–116, 2023.
[6] J. H. Ma, S. M. Xu, J. T. Ning, et al., "Redactable blockchain in decentralized setting," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1227–1242, 2022.
[7] P. Datta, I. Komargodski, and B. Waters, "Fully adaptive decentralized multi-authority ABE," in Advances in Cryptology-42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, pp. 447–478, 2023.
[8] J. H. Wei, X. F. Chen, J. F. Wang, et al., "Securing fine grained data sharing and erasure in outsourced storage systems," IEEE Transactions on Parallel and Distributed Systems, vol. 34, no. 2, pp. 552–566, 2023.
[9] J. H. Li, H. Ma, J. B. Wang, et al., "Wolverine: A scalable and transaction-consistent redactable permissionless blockchain," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1653–1666, 2023.
[10] J. Shen, X. F. Chen, Z. L. Liu, et al., "Verifiable and redactable blockchains with fully editing operations," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 3787–3802, 2023.
[11] G. H. Tian, J. H. Wei, M. Kutyłowski, et al., "VRBC: A verifiable redactable blockchain with efficient query and integrity auditing," IEEE Transactions on Computers, vol. 72, no.7, pp. 1928–1942, 2023.
[12] T. Li, H. Q. Wang, D. B. He, et al., "Designated-verifier aggregate signature scheme with sensitive data privacy protection for permissioned blockchain-assisted IIoT," IEEE Transactions on Information Forensics and Security, vol. 18, pp.4640–4651, 2023.
[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in 2007 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, pp. 321–334, 2007.
[14] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology-30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, pp. 568–588, 2011.
[15] K. Zhang, J. F. Ma, J. J. Liu, et al., "Adaptively secure multi-authority attribute-based encryption with verifiable out sourced decryption," Science China Information Sciences, vol. 59, no. 9, article no. 99105, 2016.
[16] K. Zhang, H. Li, J. F. Ma, et al., "Efficient large-universe multi-authority ciphertext-policy attribute-based encryption with white-box traceability," Science China Information Sciences, vol. 61, no. 3, article no. 032102, 2018.
[17] P. Datta, I. Komargodski, and B. Waters, "Decentralized multi-authority ABE for DNFs from LWE," in Advances in Cryptology-40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, pp. 177–209, 2021.
[18] P. Datta, I. Komargodski, and B. Waters, "Decentralized multi-authority ABE for NC1 from BDH," Journal of Cryptology, vol. 36, no. 2, article no. 6, 2023.
[19] C. Zhang, M. Y. Zhao, L. H. Zhu, et al., "FRUIT: A blockchain-based efficient and privacy-preserving quality aware incentive scheme," IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3343–3357, 2022.
[20] S. Y. Guo, K. Q. Zhang, B. Gong, et al., "Sandbox computing: A data privacy trusted sharing paradigm via blockchain and federated learning," IEEE Transactions on Computers, vol. 72, no. 3, pp. 800–810, 2023.
[21] Y. Guo, C. Zhang, C. Wang, et al., "Towards public verifiable and forward-privacy encrypted search by using blockchain," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 2111–2126, 2023.
[22] C. F. Hu, C. Zhang, D. Lei, et al., "Achieving privacy-preserving and verifiable support vector machine training in the cloud," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 3476–3491, 2023.
[23] C. Zhang, M. Y. Zhao, L. H. Zhu, et al., "Enabling efficient and strong privacy-preserving truth discovery in mobile crowdsensing," IEEE

Transactions on Information Forensics and Security, vol. 17, pp. 3569–3581, 2022.
[24] D. Yang, Z. R. Cheng, W. T. Zhang, et al., "Burst-aware time-triggered flow scheduling with enhanced multi-CQF in time-sensitive networks," IEEE/ACM Transactions on Networking, vol. 31, no. 6, pp. 2809–2824, 2023.
[25] D. Yang, W. T. Zhang, Q. Ye, et al., "DetFed: Dynamic resource scheduling for deterministic federated learning over time-sensitive networks," IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 5162–5178, 2024.
[26] W. T. Zhang, D. Yang, W. Wu, et al., "Optimizing federated learning in distributed industrial IoT: A multi-agent approach," IEEE Journal on Selected Areas in Communications, vol. 39, no. 12, pp. 3688–3703, 2021.
[27] C. Zhang, M. Y. Zhao, T. Wu, et al., "Towards secure bilateral friend query with conjunctive policy matching in social networks," in IEEE International Conference on Parallel &Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking, Melbourne, Australia, pp.98–105, 2022.
[28] C. Zhang, C. F. Hu, T. Wu, et al., "Achieving efficient and privacy-preserving neural network training and prediction in cloud environments," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 5, pp. 4245–4257, 2023.
[29] C. Zhang, X. Q. Luo, J. W. Liang, et al., "POTA: Privacy preserving online multi-task assignment with path planning," IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 5999–6011, 2024.
[30] C. Zhang, M. Y. Zhao, J. W. Liang, et al., "NANO: Cryptographic enforcement of readability and editability governance in blockchain databases," IEEE Transactions on Dependable and Secure Computing, in press, 2023.
[31] H. S. G. Pussewalage and V. Oleshchuk, "A delegatable attribute based encryption scheme for a collaborative E-health cloud," IEEE Transactions on Services Computing, vol. 16,no. 2, pp. 787–801, 2023.
[32] S. Hohenberger, G. Lu, B. Waters, et al., "Registered attribute-based encryption," in Advances in Cryptology - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, pp.511–542, 2023.
[33] C. P. Ge, W. Susilo, J. Baek, et al., "Revocable attribute based encryption with data integrity in clouds," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5,pp. 2864–2872, 2022.
[34] D. Z. Han, N. N. Pan, and K. C. Li, "A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 316–327, 2022.
[35] M. A. Islam and S. K. Madria, "Attribute-based encryption scheme for secure multi-group data sharing in cloud," IEEE Transactions on Services Computing, vol. 15, no. 4, pp.2158–2172, 2022.
[36] S. Agrawal, A. Yadav, and S. Yamada, "Multi-input attribute-based encryption and predicate encryption," in Advances in Cryptology-42nd Annual International Cryptology Conference, Barbara, CA, USA, pp. 590–621, 2022.
[37] I. Kim, W. Susilo, J. Baek, et al., "Harnessing policy authenticity for hidden ciphertext policy attribute-based encryption," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1856–1870, 2022.
[38] D. Riepel and H. Wee, "FABEO: Fast attribute-based encryption with optimal security," in Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, Los Angeles, CA, USA, pp. 2491–2504, 2022.
[39] C. Zhang, M. Y. Zhao, Y. H. Xu, et al., "Achieving fuzzy matching data sharing for secure cloud-edge communication," China Communications, vol. 19, no. 7, pp. 257–276, 2022.
[40] Y. W. Li, M. Y. Zhao, Z. H. Li, et al., "Achieving a blockchain-based privacy-preserving quality-aware knowledge marketplace in crowdsensing," in 20th IEEE International Conference on Embedded and Ubiquitous Computing, Wuhan, China, pp. 90–97, 2022.
[41] R. H. Xu, C. Li, and J. Joshi, "Blockchain-based transparency framework for privacy preserving third-party services," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 2302–2313, 2023.
[42] X. Y. Wu, X. H. Du, Q. T. Yang, et al., "Redactable consortium blockchain based on verifiable distributed chameleon hash functions," Journal of Parallel and Distributed Computing, vol. 183, article no. 104777, 2024.
[43] X. Y. Li, J. Xu, L. Y. Yin, et al., "Escaping from consensus: Instantly redactable blockchain protocols in permissionless setting," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 5, pp. 3699–3715, 2023.
[44] D. Deuber, B. Magri, and S. A. K. Thyagarajan, "Redactable blockchain in the permissionless setting," in IEEE Symposium on Security and Privacy, San Francisco, CA, USA, pp.124–138, 2019.
[45] S. M. Xu, J. T. Ning, J. H. Ma, et al., "K-time modifiable and epoch-based redactable blockchain," IEEE Transactions on Information Forensics and Security, vol. 16, pp.4507–4520, 2021.
[46] M. Jia, J. Chen, K. He, et al., "Redactable blockchain from decentralized chameleon hash functions," IEEE Transactions on Information Forensics and Security, vol. 17, pp.2771–2783, 2022.
[47] X. Y. Luo, Z. Xu, K. P. Xue, et al., "ScalaCert: Scalability oriented PKI with redactable consortium blockchain enabled "on-cert" certificate revocation," in 42nd IEEE International Conference on Distributed

Computing Systems, Bologna, Italy, pp. 1236–1246, 2022.
[48] H. C. Guo, H. T. Liang, M. Y. Zhao, et al., "Privacy-preserving fine-grained redaction with policy fuzzy matching in blockchain-based mobile crowdsensing," Electronics, vol. 12, no. 16, article no. 3416, 2023.
[49] Z. Xu, X. Y. Luo, K. P. Xue, et al., "SEREDACT: Secure and efficient redactable blockchain with verifiable modification," in 43rd IEEE International Conference on Distributed Computing Systems, Hong Kong, China, pp. 818–828, 2023.
[50] T. Ye, M. Luo, Y. Yang, et al., "A survey on redactable blockchain: Challenges and opportunities," IEEE Transactions on Network Science and Engineering, vol. 10, no. 3, pp. 1669–1683, 2023.
[51] M. J. Zhai, Y. L. Ren, G. R. Feng, et al., "Fine-grained and fair identity authentication scheme for mobile networks based on blockchain," China Communications, vol. 19, no. 6, pp. 35–49, 2022.