Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach

Chaosheng Feng, Keping Yu, *Member, IEEE,* Ali Kashif Bashir, *Senior Member, IEEE,* Yasser D. AI-Otaibi, Yang Lu, Shengbo Chen, and Di Zhang, *Senior Member, IEEE*

***Abstract*—The drone's open and untrusted environment may create problems for authentication and data sharing. To address this issue, we propose a blockchain-enabled efficient and secure data-sharing model for 5G flying drones. In this model, blockchain and attribute-based encryption (ABE) are applied to ensure the security of instruction issues and data sharing. The authentication mechanism in the model employs a smart contract for authentication and access control, public-key cryptography for providing accounts and ensuring accounts security, and a distributed ledger for security audit. In addition, to speed up outsourced computations and reduce electricity consumption, an ABE model with parallel outsourced computation (ABEM-POC) is constructed, and a generic parallel computation method for ABE is proposed. The analysis of the experimental results shows that parallel computation significantly improves the speed of outsourced encryption and decryption compared with serial computation.**

***Index Terms*—Blockchain, 5G flying drones, Attribute-based encryption, Ciphertext sharing, Authentication.**

I. Introduction

Drones are an ideal solution for environmental monitoring due to their survivability, mobility, time savings, and cost-effective benefits. Empowered by fifth-generation (5G) technology, which aims to connect anything anywhere and anytime, the capabilities of drones have been significantly enhanced. The high bandwidth provided by 5G technology enables drones to access the Internet at high speed. Its high reliability and low delay make it possible to perform real-time measurement, control, and data analysis for drones. 5G-enabled drones have been increasingly employed in geodispersed applications such as environmental monitoring, rescue operation monitoring, traffic surveillance, natural disaster monitoring, crop analysis, and consumer product delivery. With the assistance of 5G technology, drones play irreplaceable roles in information collection and delivery, especially in geographically dispersed and inaccessible scenarios. However, drones typically work in open and untrusted environments where drone networks can be easily hacked by malicious users and identity authentication becomes very difficult. All these problems make it a challenge for the information security and privacy protection of drone-based transmission.

While drones send information in plaintext format directly to the control nodes and the cloud through air interfaces, information leakage might occur. Once sensitive information such as drone instructions and coordination instructions among drones is leaked, serious consequences may occur. To prevent information leakage, some early attempts tried to encrypt the data and instructions before uploading them [1]. However, how to effectively share these ciphertexts is still a challenge. Some traditional schemes, whether symmetric or asymmetric, can be used to share the ciphertext. However, they are of low efficiency because the data owner must simultaneously share the public or symmetric key. This will result in the encryption time increasing linearly with the number of shared users, which is sometimes impractical.

A more feasible approach for preventing information leakage is to use attribute-based encryption (ABE). Generally, ABE [2]–[4] is considered a promising ciphertext sharing method since it can provide fine-grain access control, expressive access policy, one-to-many encryption, and so on. However, encryption and decryption in ABE involve expensive computations, which are difficult for resource-constrained terminals (e.g., drones). In addition, the computational time grows with the number of access policy attributes, which makes ABE encryption and decryption consume more power and take a longer time. To fill this gap, some amended ABE schemes with outsourced encryption or decryption were proposed. These schemes outsource the majority of computations to the cloud or the fog. Thus, the computing overhead at terminals and the consumed power are significantly reduced. Nevertheless, outsourced encryption or decryption in these schemes still adopts a serial computing mode with slower computing speed, which fails to provide excellent experiences for resource-constrained terminal users.

To solve the problems mentioned above, a blockchain-enabled data-sharing model for drones is introduced in this paper. The blockchain is useful for building trust mechanisms

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61373163, and in part by the Japan Society for the Promotion of Science (JSPS) Grants-in-Aid for Scientific Research (KAKENHI) under Grant JP18K18044. Chaosheng Feng and Keping Yu are co-first authors. (Corresponding author: Di Zhang)

C. Feng is with the Department of Computer Science, Sichuan Normal University, China (email: csfenggy@126.com).

K. Yu is with Global Information and Telecommunication Institute, Waseda University, Tokyo, 169-0072 Japan (email: keping.yu@aoni.waseda.jp).

A. K. Bashir is with Department of Computing and Mathematics, E-154, John Dolton, Chester Street, M15 6H, Manchester Metropolitan University, Manchester, United Kingdom and with School of Electrical Engineering and Computer Science (SEECS), National University of Science and Technology, Islamabad (NUST), Pakistan. (email: dr.alikashif.b@ieee.org).

Yasser D. AI-Otaibi is with the Department of Information Systems in Rabigh, King Abdulaziz University, Jeddah 21589, Saudi Arabia (email: yalotaibi@kau.edu.sa).

Y. Lu is with School of Computing, University of Kent, UK (email: Y.LU@kent.ac.uk).

S. Chen is with School of Computer and Information Engineering, Henan University, China (email: ccb02kingdom@gmail.com).

D. Zhang is with School of Information Engineering, Zhengzhou University, Zhengzhou, 450001 China (email: dr.di.zhang@ieee.org).

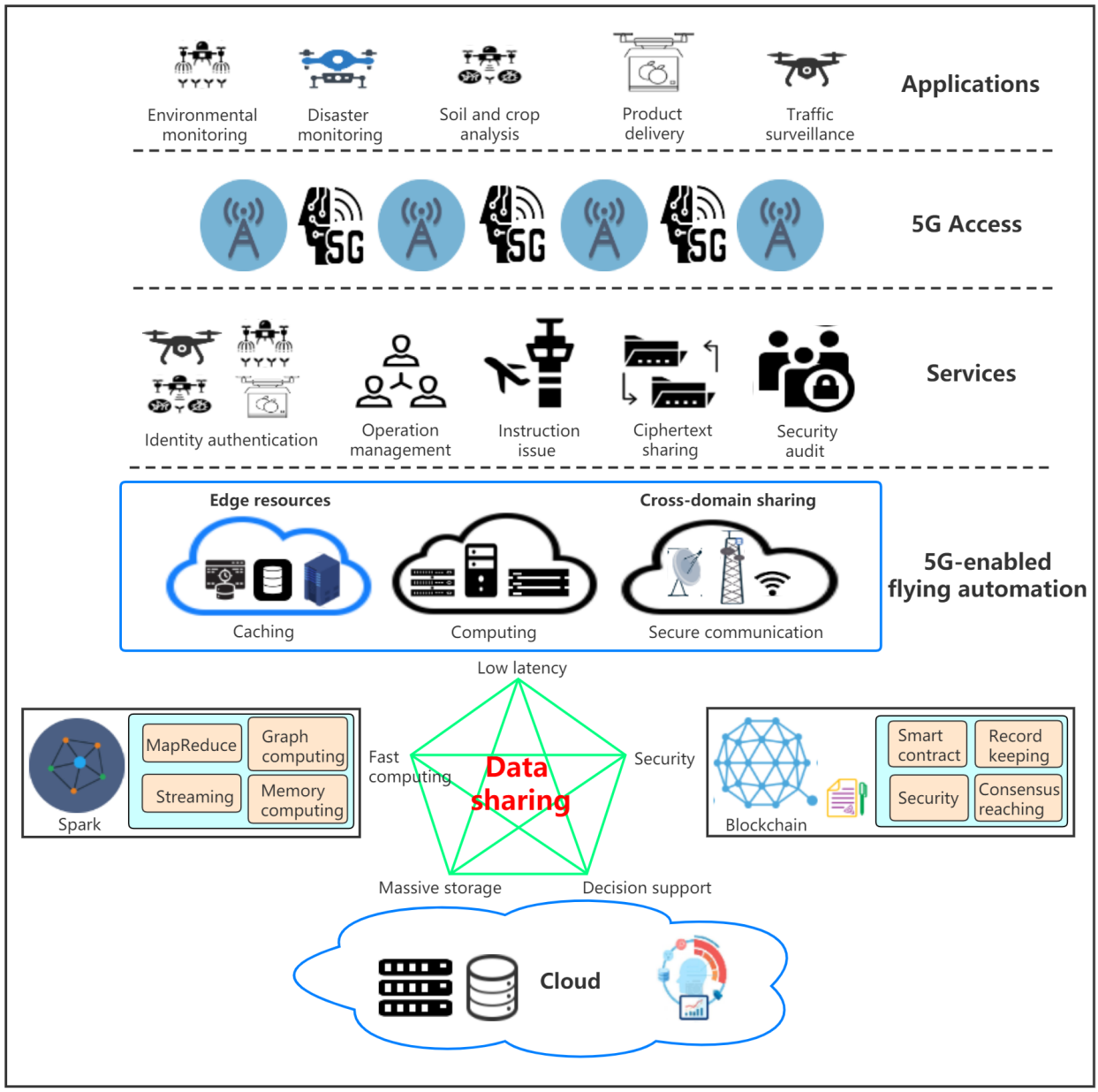


Fig. 1. A blockchain-enabled efficient and secure data-sharing framework for drones

for application environments without any trusted third party or with a trusted third party, but privacy protection is required [5] [6]. Drones work in such an environment where there is no trusted third party, and privacy protection is essential and required. We then introduce a smart contract for blockchain-enabled authentication and access control, public-key cryptography is used to ensure accounts security, and we employ the distributed ledger for security auditing. To speed up the outsourced computations, we adopt a parallel computing mode in the ABE model and propose a model called ABEM-POC, in which a generic parallel computing method for ABE is adopted. In other words, an ABE scheme constructed based on the proposed ABEM-POC will support parallel outsourced encryption and decryption. If an existing ABE scheme with serial outsourced computation can also be modified according to the ABEM-POC, the modified scheme will be featured with parallel outsourced computations.

II. Related Work

Identity-based encryption (IBE) generally has poor error tolerance in practical applications. To address this problem, Sahai and Waters [2] proposed a new vision of encryption called ABE under fuzzy IBE. Goyal et al. [3] presented the first key-policy attribute-based encryption (KP-ABE) scheme, in which an encrypted message is associated with a set of attributes and a user private key is associated with an

access policy or structure. Bethencourt et al. [4] proposed the first ciphertext-policy attribute-based encryption (CP-ABE) scheme. As opposed to the KP-ABE scheme, the CP-ABE scheme labels a user's private key with a set of attributes and associates a ciphertext with an access policy. All these schemes represent access policies with trees as access structures. Due to the lack of satisfaction with Bethencourt et al.'s scheme, which is secure in the generic group model, Water [7] implemented a CP-ABE system in the standard model. The most unique aspect in Water's scheme is the linear secret sharing scheme (LSSS) instead of the conventional tree-like access structures to represent the access policies. Afterward, Rouselakis and Waters proposed two large-universe attribute-based encryption constructions in [8]. In a large-universe ABE construction, any string can be used as an attribute, and attribute enumeration is not necessary at the system setup step. To provide cloud users with shared access to privileges, Ahuja et al. proposed a scalable attribute-based access control scheme for cloud storage [9]. Based on a key encapsulation mechanism (KEM), Lin et al. [10] and Qin et al. [11] constructed an ABE model with verifiable outsourced decryption. The model in [10] also ensures the security of outsourced decryption with all or nothing transforms (AONTs). In addition, Mao et al. [12] proposed a generic construction of chosen-plaintext attack (CPA)-secure and replayable chosen ciphertext attack (RCCA)-secure ABE systems with verifiable outsourced decryption from CPA-secure ABE systems with outsourced decryption. Although these ABE constructions outsource the decryption to the cloud or the fog, all outsourcing decryptions adopt serial computing.

As an emerging and promising technique in digital currency systems, blockchain can share data even without a credible central server with its advantages of transaction anonymity, credibility, tamper resistance, and high distribution. Gao et al. [13] proposed a blockchain-based privacy-preserving payment mechanism for vehicle-to-grid (V2G) networks, which ensures the anonymity of user payment data. Shen et al. [14] proposed a blockchain-based system for medical image retrieval with privacy protection. Xia et al. [15] implemented a secure fine-grain access control system for outsourced data, which supports data read and write operations. Moreover, blockchain technologies are also utilized to enhance traceability and visibility.

III. Blockchain-Enabled Efficient and Secure Data-Sharing Framework for Drones

In this section, a blockchain-enabled efficient and secure data-sharing framework for drones is proposed, as shown in Fig. 1. In this framework, the 5G-enabled flying automation layer provides drones with five core services: identity authentication, operation management, security auditing, instruction issues, and ciphertext sharing. Specifically, the first three are mainly implemented based on blockchain, and the remaining two are mainly implemented based on ABE. To reduce the transmission latency, all the time-consuming and power-consuming computational tasks are outsourced to edge computing devices. To accelerate the encryption and decryption of ABE, a Spark platform is deployed on the edge network so that the encryption and decryption tasks outsourced by drones are carried out in parallel computation on the Spark platform. The public cloud provides data storage and analysis and supports decision making by managers. Note that the collected large-sized data are stored in the public cloud rather than the blockchain. Only the small-sized data for authentication and sharing, such as identity information, shared metadata, and operation information, are stored in the blockchain. The 5G-enabled flying automation layer consists of blockchain, edge networks and devices, the Spark platform, and the cloud. The following are the implementation principles of the five services mentioned above.

Identity authentication: The drone registers an account in the blockchain, and it can be authorized by a smart contract. When authenticating a drone, the smart contract determines whether the authentication request issued by the account meets the criteria. If so, the blockchain returns certain credentials; otherwise, it discards this request.

Operation management: For each instruction to be executed, the drone must authenticate both the instruction issuer and the integrity of the instruction.

Instruction issue: Operation instructions are sensitive information and must be sent in ciphertext format. In most cases, the console or drones send instructions with the characteristics of the "one-to-many", i.e., an instruction is executed by many drones. Considering this characteristic, the ABE is adopted to improve the efficiency of encryption. ABE realizes ciphertext sharing by efficient key distribution. To ensure the security of the instruction issue, each instruction is encrypted before it is sent. Meanwhile, the key for encryption is distributed efficiently using ABE.

Ciphertext sharing: If the data collected by drones are also sensitive, encryption is required before uploading to the cloud. Such data are usually analyzed by multiple users with the same attributes before decision making. Since the encryption process also features "one-to-many" sharing and fine-grained access control is demanded, ABE is also adopted.

Security audit: To facilitate the security audit and accountability, instruction issues, instruction execution, data sharing, and other important operations are written into the distributed ledger in the transaction form.

IV. Blockchain-Enabled Identity Authentication Mechanism for Drones

A blockchain-enabled identity authentication mechanism is built in this section, as shown in Fig. 2. The proposed mechanism consists of the following components.

Smart contract for identity management: The contract is an n-m multisignature smart contract created by the authorization center. It is created by m administrators and requires the authorization of n administrators to invoke contract management. The contract is used to hold the access control list (including the trusted list and the revocation list), which can only be signed by n administrators to invoke the add function. Multiple signatures can prevent the leakage risks caused by the loss of a single administrator's private key or excessive permissions.

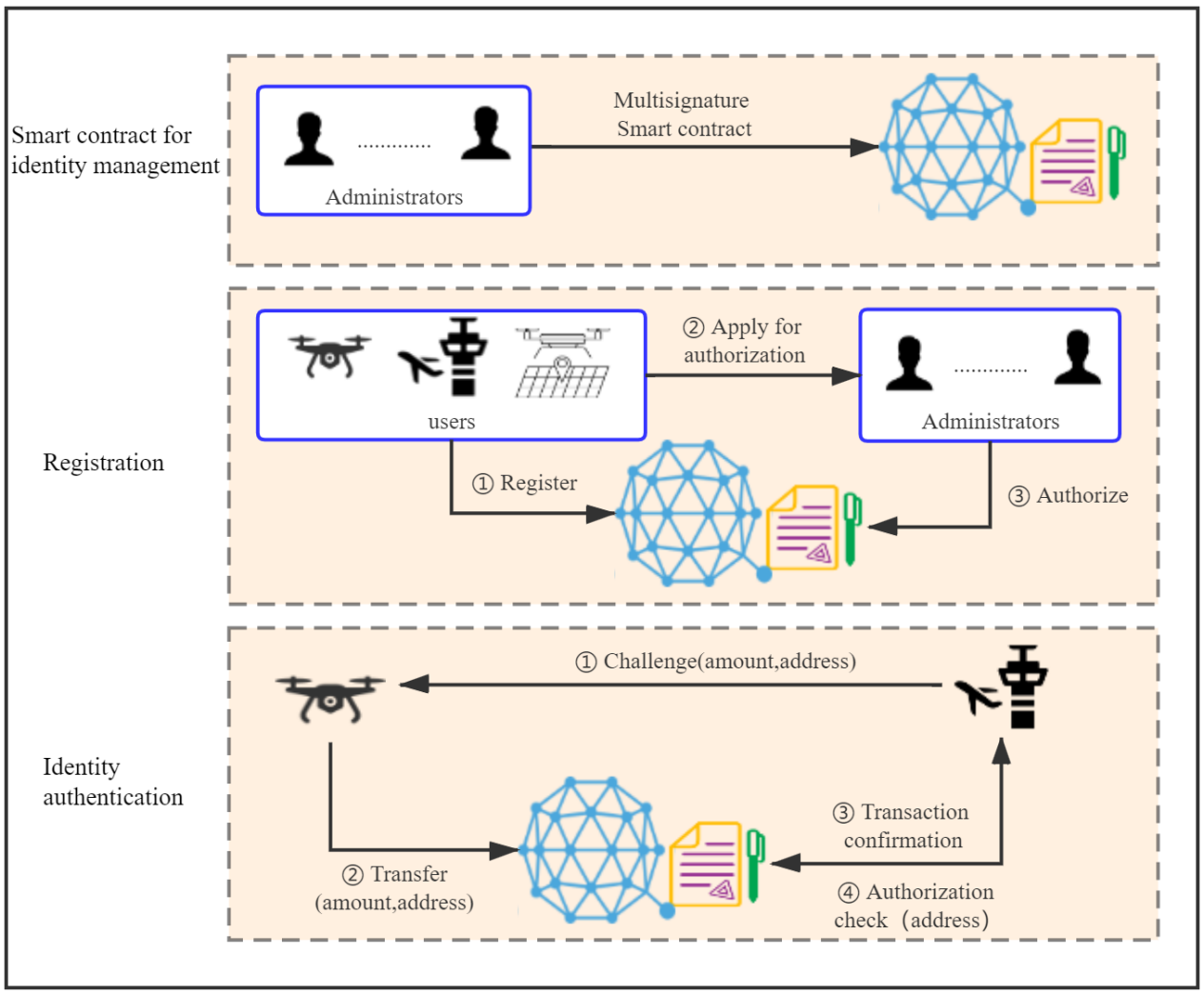


Fig. 2. Blockchain-enabled identity authentication mechanism for drones

Registration: Users (e.g., drones, control centers, and intelligent receiving stations) can apply for accounts in the blockchain and locally store the encrypted private key. Users submit their account address to the administrator through a secure channel. After verifying the registration requested by the user, the administrator adds the address to a trusted list in the smart contract. In contrast, for the users who apply for account cancellation or loss, their addresses are added to the revocation list of the smart contract.

Identity authentication: When a user authenticates other users, he/she requests a small number of designated coins to transfers to their accounts. After receiving the coins, they look up the address from the access control list. If Records (trusted list) > Records (revocation list) (this condition allows the user to repeatedly register and log out), the identity is legal.

V. Blockchain-Enabled Secure Data Sharing for Drones

In this section, a blockchain-enabled secure data-sharing model and an ABE model with parallel outsourced computations are constructed. Furthermore, a generic parallel computing method for ABE is proposed.

A. Blockchain-Enabled Secure Data-Sharing Model

As shown in Fig. 3, the blockchain-enabled secure data-sharing model for drones consists of the following 5 components.

Drones: When a drone registers a blockchain account, it obtains a unique identifier. For the 5G drone, there are two methods for encrypting collected data before it is uploaded to the cloud. One is that the drone encrypts the data using a symmetric key assigned in advance and sends the ciphertext to the node manager. Then, the node manager uses ABE to encrypt the key. The other is that the drone generates a key

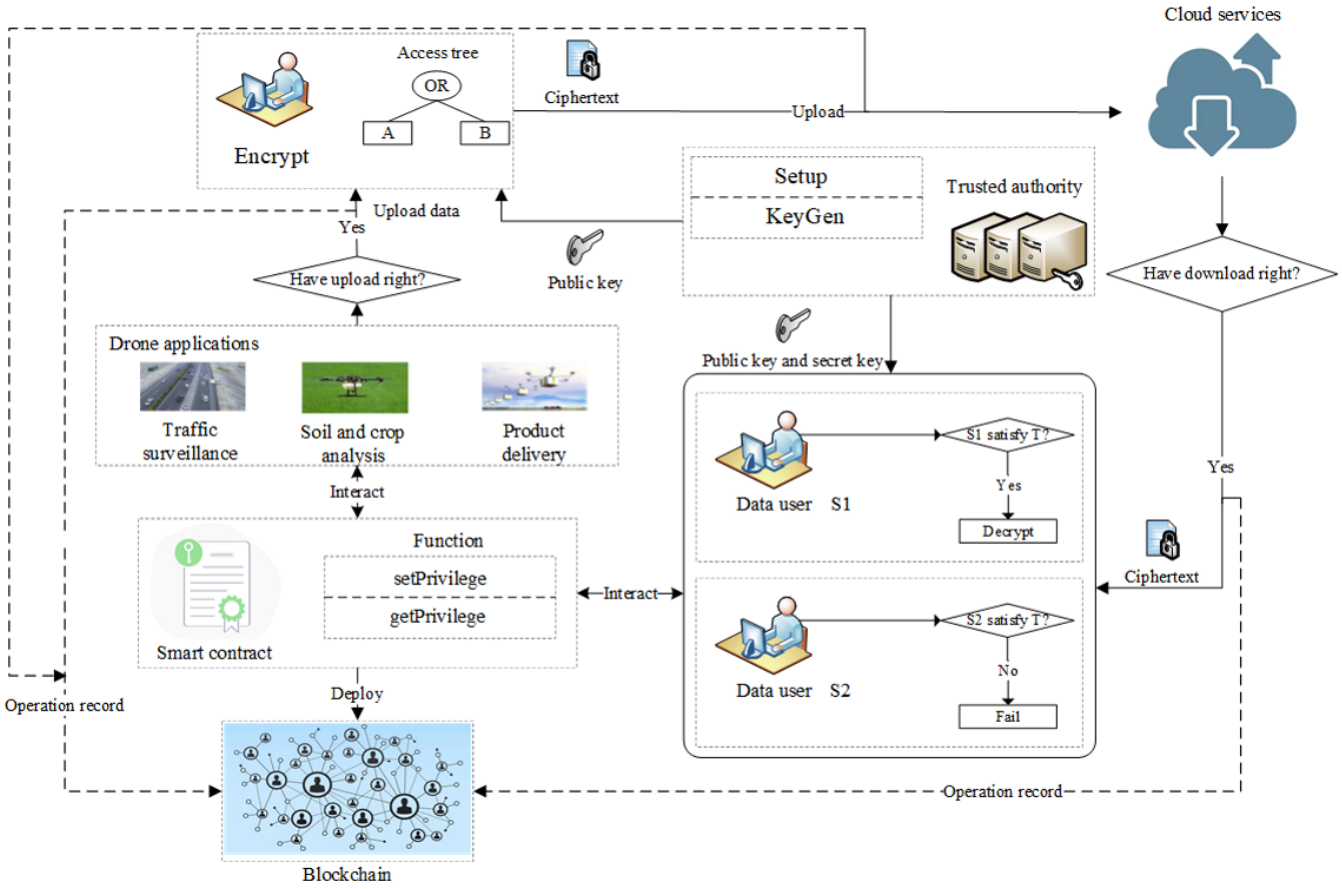


Fig. 3. Blockchain-enabled secure data sharing for drones

randomly, encrypts the data with this key and then uses ABE to encrypt the key. The 5G drone mainly adopts the latter.

Trusted authority (TA): The TA as the central point can perform operations such as initialization and secret key generation, generate the system public key, and the system master secret key.

Cloud: The cloud stores and analyzes the data collected by drones.

Blockchain: The blockchain is responsible for identity authentication and recording operations.

Data consumer (DC): The DC refers to a user who can decrypt and read instructions and collected data.

The secure sharing process based on the blockchain for 5G drones is as follows. The drone encrypts the collected data in symmetric encryption (e.g., AES) and encrypts the corresponding symmetric encryption key. Then, the drone sends a data upload request to the blockchain. After receiving the request, the blockchain validates the request with a preagreed smart contract. If the request is valid, the blockchain returns a credential to the drone. Once the drone receives the credential, it uploads the ciphertext along with the credential to the cloud. When the ciphertext is confirmed to be valid, the cloud stores it and sends the storage confirmation message to the blockchain. The blockchain writes the shared ciphertext data into its distributed ledger in the transaction form. If a data consumer (a drone or a user) wants to access the ciphertext, the blockchain will use smart contracts to validate its identity and check whether his/her attributes satisfy the access policy of the ciphertext. If its identity is valid and his/her attributes satisfy the policy, an access credential is returned to the consumer. Then, the consumer can access the ciphertext in the cloud with the credential. The distribution of communication keys between drones has a similar process.

B. ABE Model With Parallel Outsourced Computations

To improve the encryption and decryption efficiency of ABE and to reduce the drones' power consumption, the computations are outsourced to the Spark platform deployed in edge devices where parallel computation is adopted.

The ABE model with parallel outsourced computation is defined by the following polynomial-time algorithms, as shown in Fig. 4. In this model, edge devices are assumed to be trusted. For this reason, the verification of outsourced computations is not considered. If edge devices are semitrusted or untrusted in some application environments, the verification method is given by the scheme instantiating the ABEM-POD.

(1) Setup. The setup algorithm takes a security parameter and an attribute universe as input parameters. It then generates a public key PK and a master secret key.

(2) KeyGen. The key generation algorithm outputs a private key. In this part, a public key, the master secret key, and an

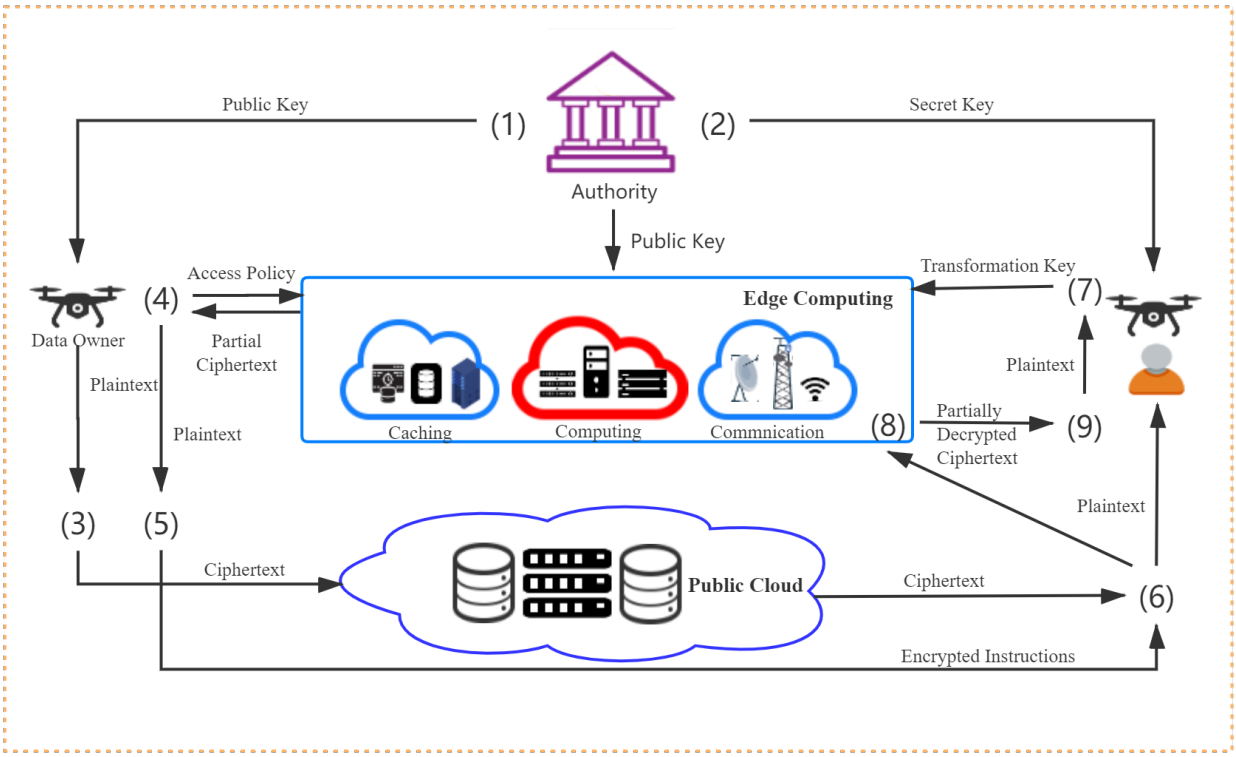


Fig. 4. ABE model with parallel outsourced computations

access structure for KP-ABE or an attribute set for CP-ABE should be set as input parameters.

(3) Encrypt. The encryption process takes a public key, a message, and an attribute set for KP-ABE or an access structure for CP-ABE as input parameters and finally outputs the ciphertext.

(4) OutEncrypt. The outsourced encryption algorithm inputs parameters including a public key, a message, and an access structure for CP-ABE. Finally, it outputs a partially encrypted ciphertext. This algorithm runs on edge computing servers and calls the generic algorithm of parallel computation for ABE, which is presented later.

(5) ClientEncrypt. The algorithm first runs **OutEncrypt** and then finishes the remaining computations. It outputs a ciphertext.

(6) Decrypt. The decryption algorithm takes a private key and a ciphertext as input and then outputs a message if the attribute set matches the access policy.

(7) TKGen. The input parameter of the transformation key generation algorithm is a private key. It outputs a transformation key and a corresponding retrieving key.

(8) OutDecrypt. The outsourced decryption algorithm's input includes a transformation key and a ciphertext. It outputs a partially decrypted ciphertext. This algorithm runs on edge computing servers and calls the generic parallel computation algorithm in ABE.

(9) ClientDecrypt. The input of the client decryption algorithm includes a retrieving key, a ciphertext, and a corresponding partially decrypted ciphertext. It outputs a message if the attribute set matches the access policy. This algorithm runs on user terminals.

C. Generic Parallel Computation Method for ABE

As stated above, both the outsourced encryption function **OutEncrypt** and the outsourced decryption function **OutDecrypt** employ the generic parallel computation method, which applies the component MapReduce on Spark to speed up ABE encryption and decryption. The generic parallel computation method for ABE is shown in Fig.5 and described as follows.

Each node in the access tree is assigned a **Map** worker, while each leaf node in the access tree is assigned a **Reduce** worker. The Map procedure and the Reduce procedure corresponding to a node are defined as follows.

Map Procedure

Case 1: The node is a nonleaf node.

Input: The input key is equal to the serial number of the nonleaf node, and the input value is a set that consists of the subsets of all the leaf nodes of each subtree of the nonleaf node.

Process: For decryption, calculate the Lagrange coefficient belonging to each leaf node. For encryption, select a polynomial without a constant term at random and then calculate the secret share belonging to each leaf node in each subtree.

Output: The output key is equal to the serial number of the leaf. The output value is equal to the share of the secret value for encryption or the Lagrange coefficients of all the nodes but the root in the path from the root to the leaf node for decryption.

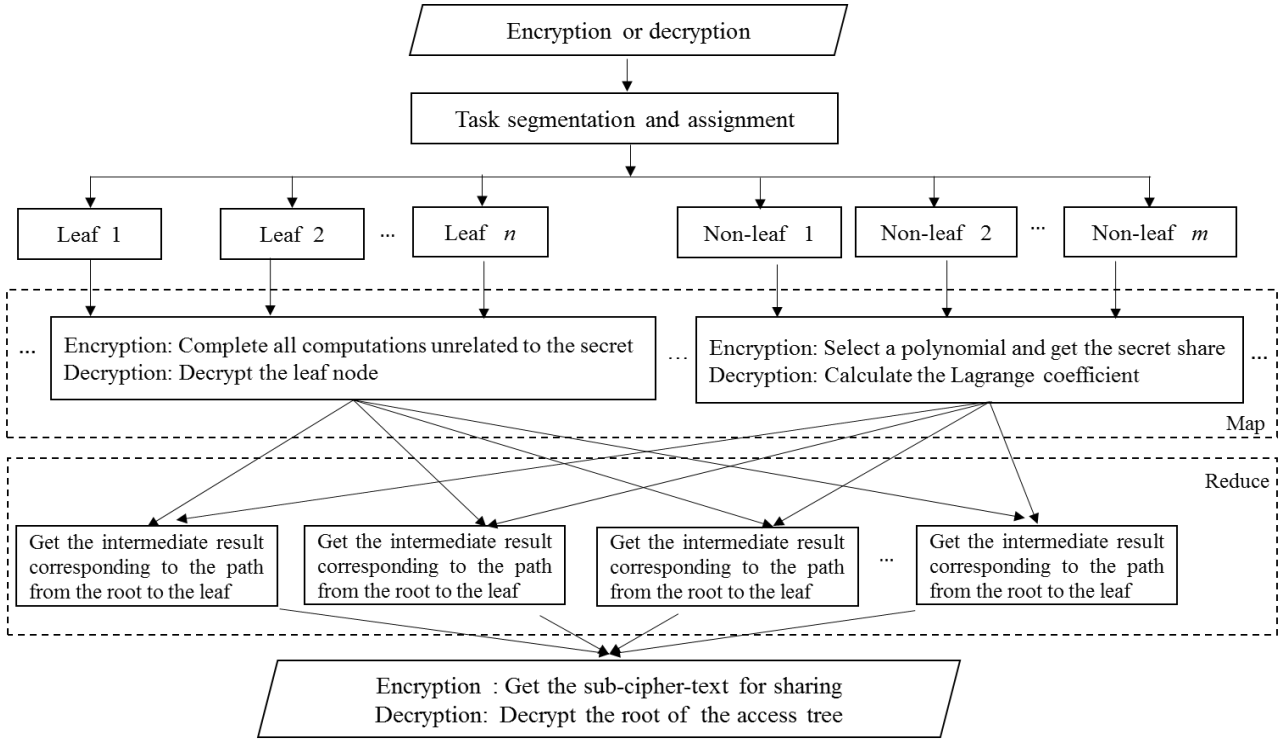


Fig. 5. Generic parallel computing method for ABE

Case 2: The node is a leaf node.

Input: The input key is equal to the serial number of the leaf, leaf. For encryption, the input value is related to the special scheme. For decryption, the input key is the ordered pair of the subciphertext and subprivate key.

Process: For encryption, all computations unrelated to the secret are completed. For decryption, decrypt the leaf node following the decryption algorithm for the leaf.

Output: The output key is equal to the number of leaves. The output value is equal to the intermediate result of encryption or decryption.

Reduce Procedure

Input: The input key is equal to the serial number of the leaf node, and the input value is the ordered pair of the share for encryption (or the Lagrange coefficient for decryption) and the intermediate result.

Process: Calculate the intermediate result corresponding to the path from the root to the leaf.

Output: The output key is equal to the serial number of the leaf node, and the output value is the encryption or decryption result of the leaf.

Thus, the outsourced encryption is completed. For decryption, the root is also decrypted by the servers.

VI. Experiments and Analysis

To evaluate the ABEM-POC, we conduct an experiment using Spark and implement the two schemes in [8] and [9] together with their modified schemes in Java, referencing the Java pairing base class (JPBC) library and the CP-ABE toolkit. The implementation uses a 160-bit elliptic curve group based on the supersingular curve over a 1024-bit finite field. The experimental environment consists of a Spark cluster to simulate the edge computing environment, in which there are a master node and ten worker nodes, and a server assembling all the outputs of the function **Reduce** and making the relevant calculation. The experimental terminals used for simulating drones include a Lenovo PC with a dual Intel Core i5-6200U CPU@2.4 GHz and 8 GB RAM, a ThinkPad Ultrabook with an Intel Core i5-3337U CPU@1.8 GHz and 4 GB RAM, and a HUAWEI Mate 10 smartphone with a Hisilicon Kirin 970 CPU and 4 GB RAM running Android OS 9. All the nodes in the Spark cluster are performed by virtual machines equipped with two Intel Core E5-2620 CPU@2.0 GHz, 4G RAM, and running 64-bit CentOS6.5. The server is equipped with the same as except for 2G RAM.

To compare the serial and parallel computations, two typical ABE schemes are modified, and the logical operations of the access policy are all set with AND. The access policies are generated and expressed in the form of (A_1 and $\ldots$ and A_n), where each represents an attribute. The number of attributes of the first access policy is 1, and the number of attributes in the remaining access policies increases from 10 to 100 every 10 intervals. Considering the dynamics of the experimental machines, we repeat the experiments 50 times under the same conditions and take the average value. As shown in Fig. 6, "Serial" denotes that the servers compute with serial computation, and "Parallel" refers to servers computing with parallel computation. The results are shown in Fig. 6. Specifically, Fig. 6(a) and Fig. 6(b) are the comparisons between serial encryption

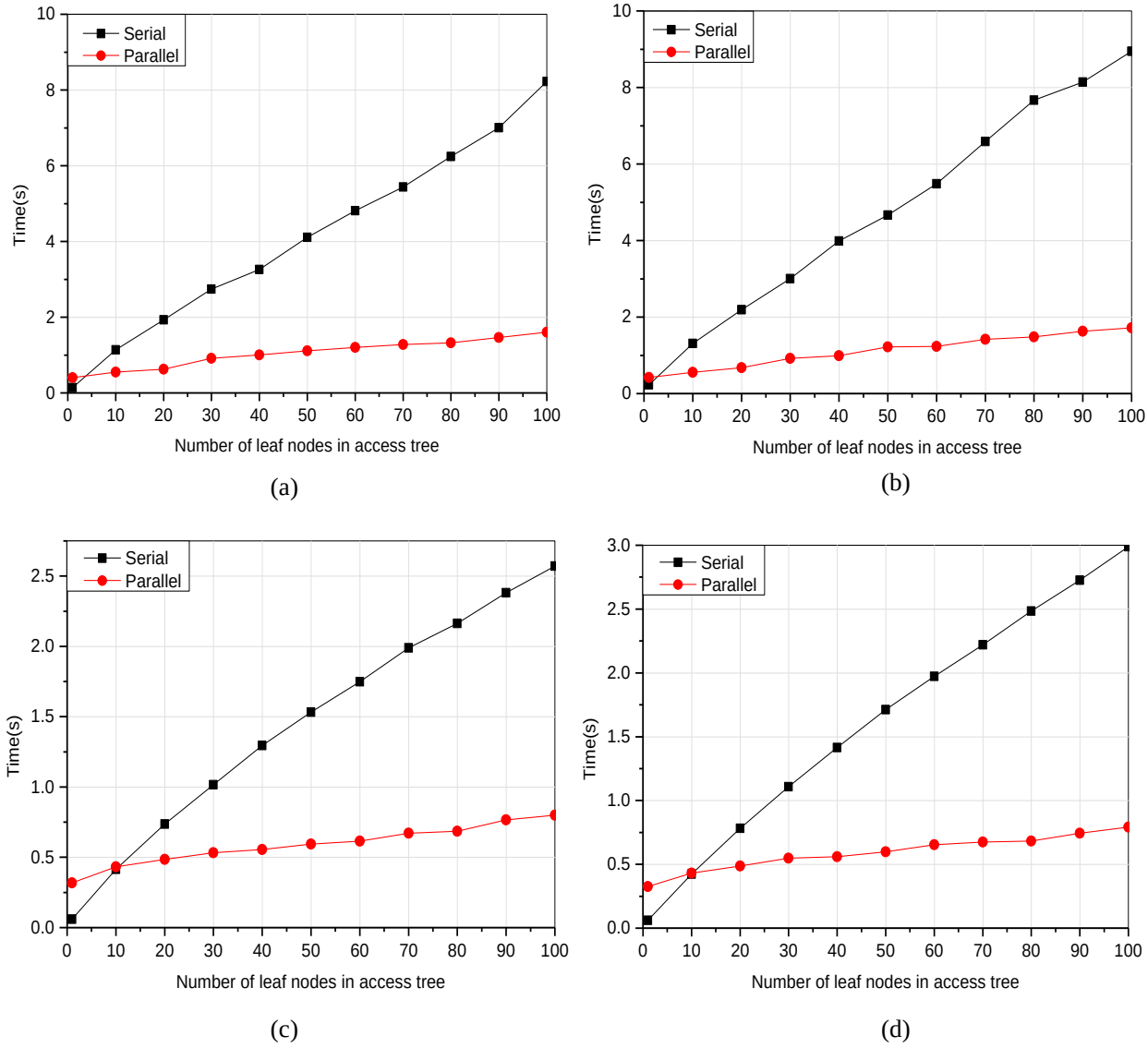


Fig. 6. Comparison between the serial computation and the parallel computation: (a) encryption time of Ref. [9] and the modified scheme; (b) encryption time of Ref. [8] and the modified scheme; (c) decryption time of Ref. [9] and the modified scheme; (d) decryption time of Ref. [8] and the modified scheme.

and parallel encryption, while Fig. 6(c) and Fig. 6(d) are the comparisons between serial and parallel decryption. When the number of attributes in the access policies is beyond a certain threshold (e.g., 2 for encryption and 10 for decryption), the computing time of the parallel computations is shorter than that of the serial computations. As the number of attributes increases, the gap in computing time between the parallel computations and serial computations becomes increasingly evident.

VII. CONCLUSIONS

Secure and efficient data sharing is a critical problem in drone networks. In this article, a blockchain-enabled efficient and secure data-sharing model is proposed. The model applies a blockchain-enabled identity authentication mechanism and a secure data-sharing model for drones. The authentication mechanism uses a smart contract for authentication and access control, public-key cryptography for account generation and ensuring accounts security, and a distributed ledger for a security audit. In addition, to accelerate the outsourced computations, ABEM-POC is proposed based on the Spark cluster and the MapReduce framework. If an ABE scheme is constructed based on the ABEM-POC, it can support parallel outsourced computations. If an existing ABE scheme with serial outsourced computation is modified according to the ABEM-POC, it will feature parallel outsourced computations. The modification of two typical ABE schemes based on ABEM-POC shows that ABEM-POC and generic methods are effective and easy to use. The analysis of the experimental results shows that the proposed ABEM-POC can significantly improve the efficiency of outsourced computations.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*. IEEE, 2007, pp. 321–334.

[5] S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, A. K. Bashir, S. Mumtaz, and S. A. Otaibi, "Blockchain-enabled reliable osmotic computing for cloud of things: Applications and challenges," *IEEE Internet of Things Mag.*, vol. 3, no. 2, pp. 63–67, 2020.

[6] J. Chen, J. Wu, H. Liang, S. Mumtaz, J. Li, K. Konstantin, A. K. Bashir, and R. Nawaz, "Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation," *IEEE Trans. Ind. Appl.*, pp. 1–1, 2019.

[7] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *International Workshop on Public Key Cryptography*. Springer, 2011, pp. 53–70.

[8] Y. Rouselakis and B. Waters, "New constructions and proof methods for large universe attribute-based encryption." *IACR Cryptology EPrint Archive*, vol. 2012, p. 583, 2012.

[9] R. Ahuja and S. K. Mohanty, "A scalable attribute-based access control scheme with flexible delegation cum sharing of access privileges for cloud storage," *IEEE Trans. Cloud Comput*, 2017.

[10] S. Lin, R. Zhang, H. Ma, and M. Wang, "Revisiting attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2119–2130, 2015.

[11] B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1384–1393, 2015.

[12] X. Mao, J. Lai, Q. Mei, K. Chen, and J. Weng, "Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Dependable Secure Comput*, vol. 13, no. 5, pp. 533–546, 2015.

[13] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE network*, vol. 32, no. 6, pp. 184–192, 2018.

[14] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical iot systems: A blockchain-based approach," *IEEE Network*, vol. 33, no. 5, pp. 27–33, 2019.

[15] Q. Xia, E. B. Sifah, K. O.-B. O. Agyekum, H. Xia, K. N. Acheampong, A. Smahi, J. Gao, X. Du, and M. Guizani, "Secured fine-grained selective access to outsourced cloud data in iot environments," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10 749–10 762, 2019.

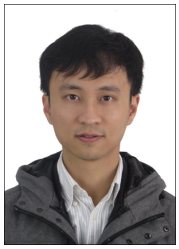
Chaosheng Feng is a professor and master tutor in the Department of computer science, Sichuan Normal University, China. He received his Ph.D. degree in information and communication engineering from University of electronic science and technology of China in June 2010. He worked in the post-doctoral mobile station of University of electronic science and technology of China and the post-doctoral workstation of Chengdu high-tech zone during September 2010 to August 2012. His research interests include cloud computing, privacy protection and data security.

Keping Yu (S'11-M'17) received his Ph.D. degrees from Waseda University, Japan, in 2016. He is currently a researcher at Waseda University, Japan. He is an Editor for IEEE Open Journal of Vehicular Technology and Guest Editor for Sensors, Peer-to-Peer Networking and Applications, Energies, and IEICE Transactions on Information and Systems. His research interests include smart grids, information-centric networking, the Internet of things, blockchain, and information security.

Ali Kashif Bashir is a senior lecturer in the Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom. He is a senior member of IEEE and a Distinguished Speaker of ACM. His past assignments include associate professor of information and communication technologies, Faculty of Science and Technology, University of the Faroe Islands, Denmark; Osaka University, Japan; Nara National College of Technology, Japan; the National Fusion Research Institute, South Korea; Southern Power Company Ltd., South Korea; and the Seoul Metropolitan Government, South Korea.

Yasser D. Al-Otaibi is currently an Assistant Professor in the Department of Information Systems at the Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah, Saudi Arabia. He received a PhD degree in Information Systems from Griffith University, Australia in 2018. His current research interests include IT adoption and acceptance, wireless sensor networks, and IoT.

Yang Lu is a Research Associate at University of Kent. Her research interests include, but not limited to, privacy computing, privacy risk assessment, usable privacy, privacy preserving AI, semantic web technology as well as security in distributed systems.



Shengbo Chen (S'11–M'13) received the B. E.and M. E. degrees in electronic engineering department from Tsinghua University, Beijing, China, in 2006 and 2008, respectively, and the Ph.D from the Ohio State University, Columbus, OH, USA, in 2013. Currently, he is a professor at the School of Computer and Information Engineering, Henan University, China. From 2013 to 2019, he was a senior research engineer at Qualcomm research center, San Diego, CA, USA. Dr. Chen received the best student paper award for Wiopt 2013, and holds more than 50 US patents on 5G and AI area.

Di Zhang (dr.di.zhang@ieee.org) currently is an Assistant Professor with the Zhengzhou University, Zhengzhou, China. He is the editor of IEEE ACCESS, KSII Transactions on Internet and Information Systems and IET Quantum Communication. He has served as the guest editor of IEEE WIRELESS COMMUNICATIONS, IEEE NETWORK, IEEE ACCESS, chair of IEEE WCNC 2020, IEEE/CIC ICCC 2020, etc. In 2019, he received the ITU Young Author Award and the IEEE Outstanding Leadership Award. His research interests include information theory, signal processing, Internet of things and e-health.

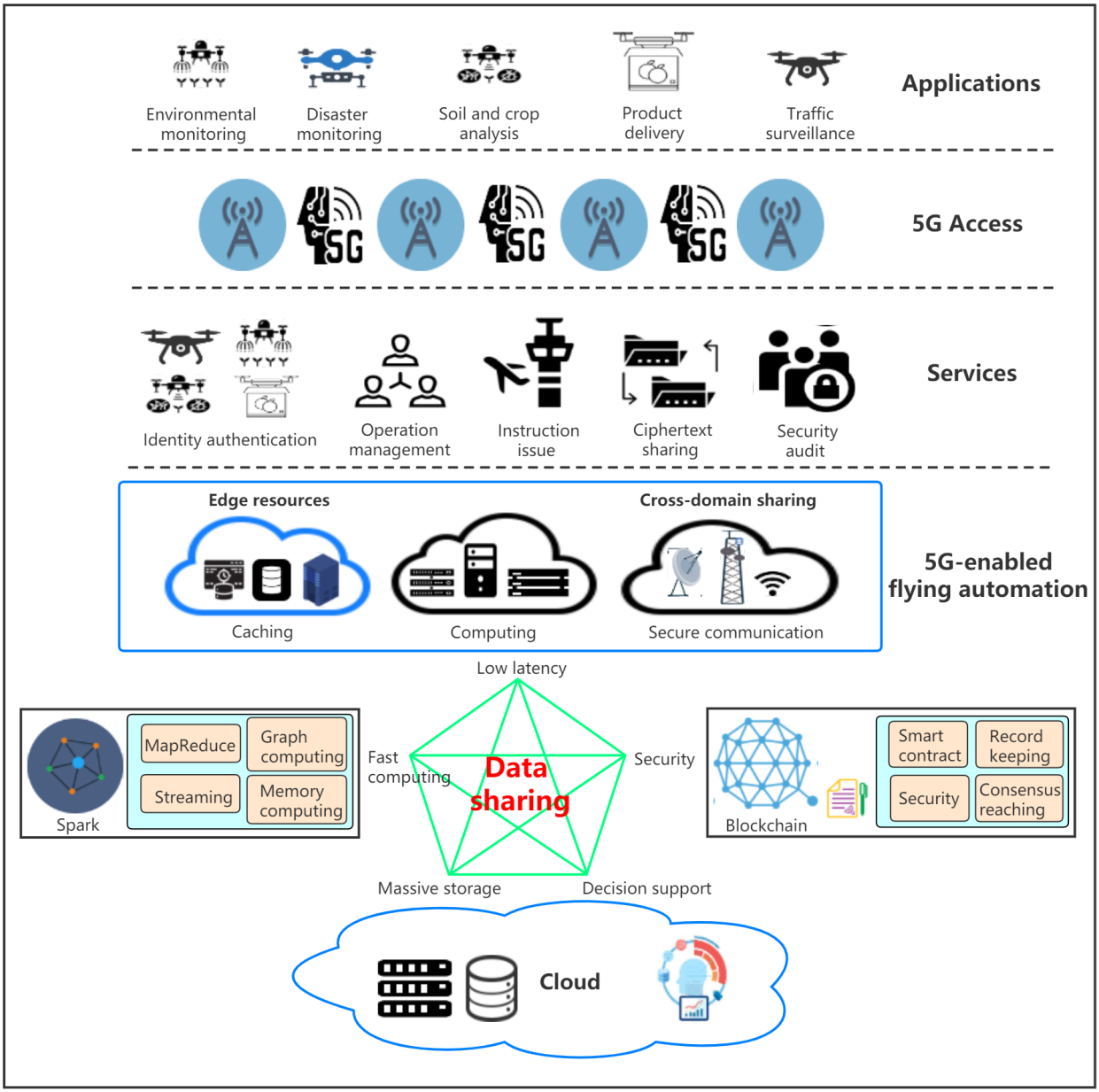


Fig. 1. A blockchain-enabled efficient and secure data-sharing framework for drones

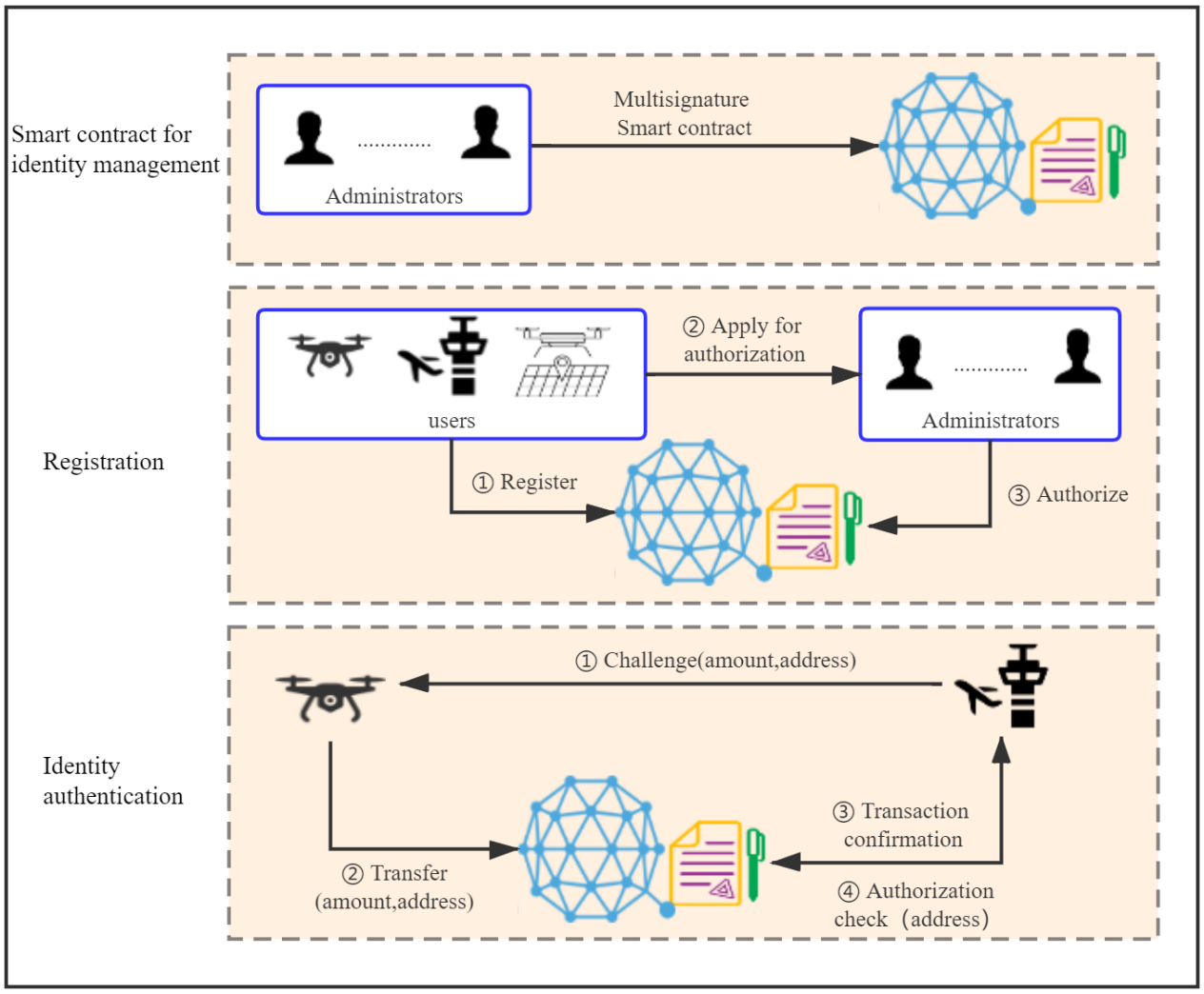


Fig. 2. Blockchain-enabled identity authentication mechanism for drones

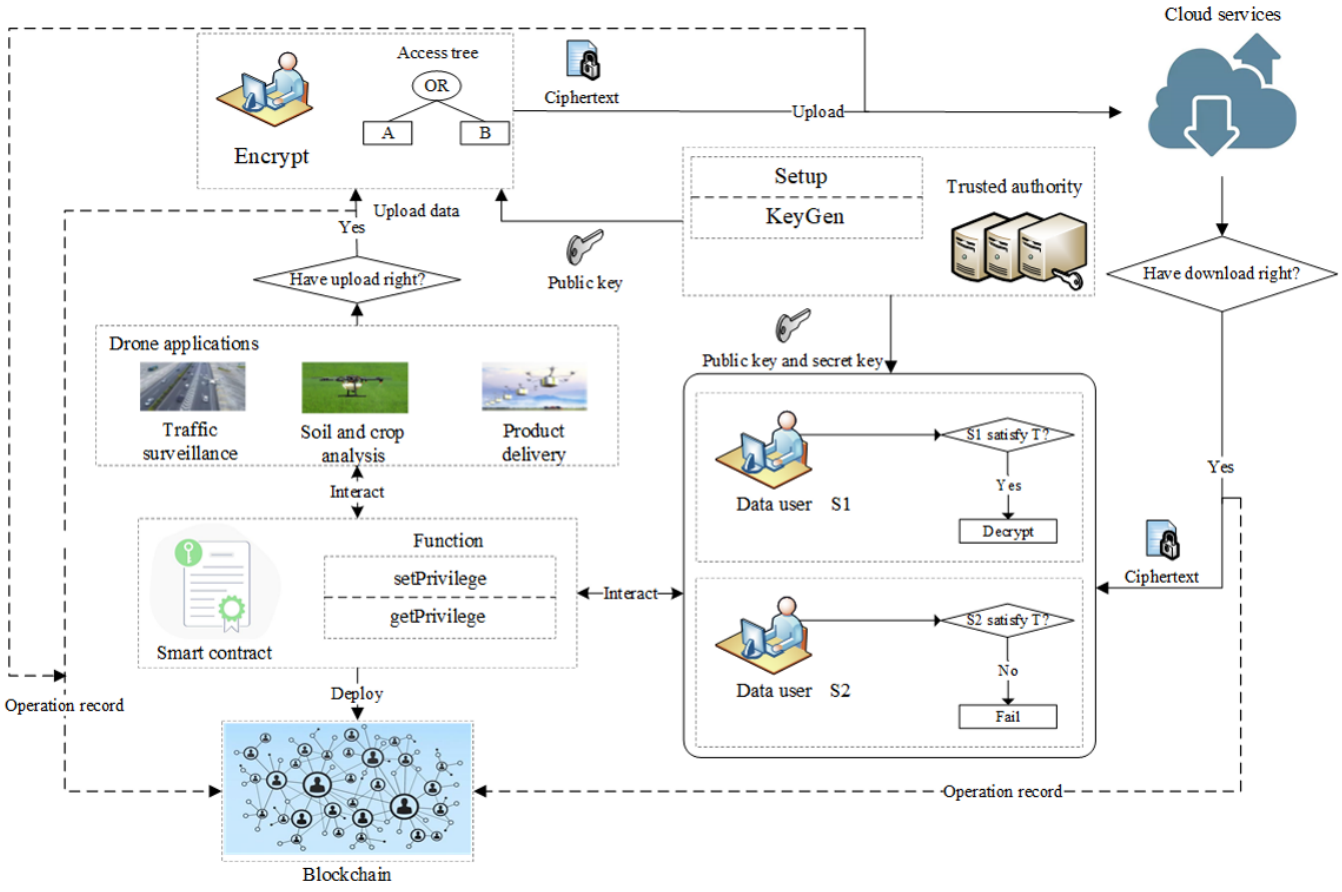


Fig. 3. Blockchain-enabled secure data sharing for drones

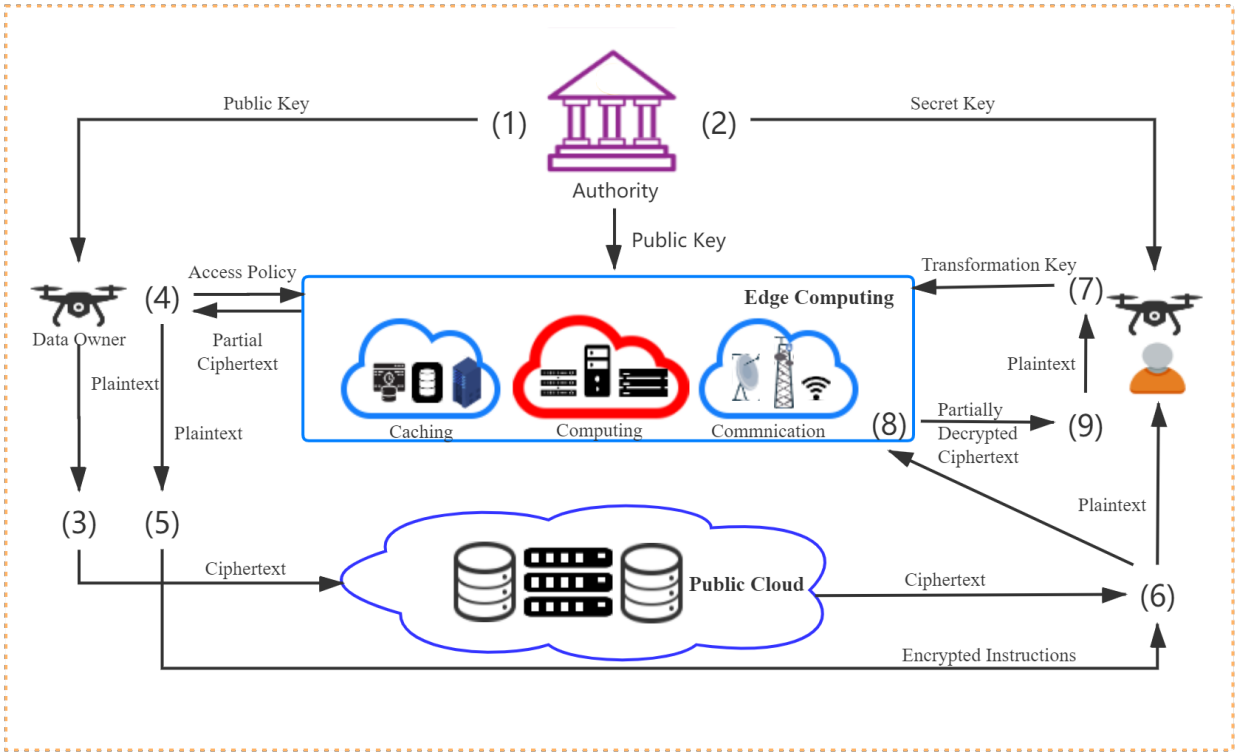


Fig. 4. ABE model with parallel outsourced computations

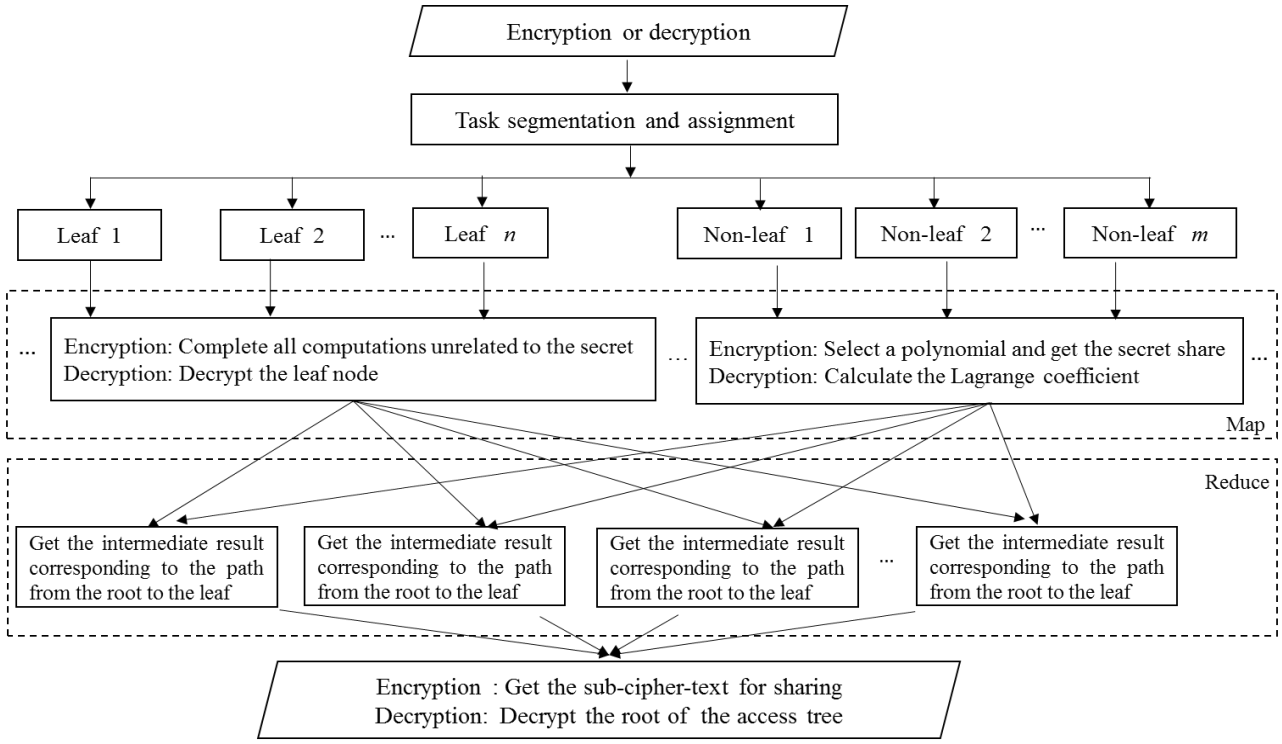


Fig. 5. Generic parallel computing method for ABE

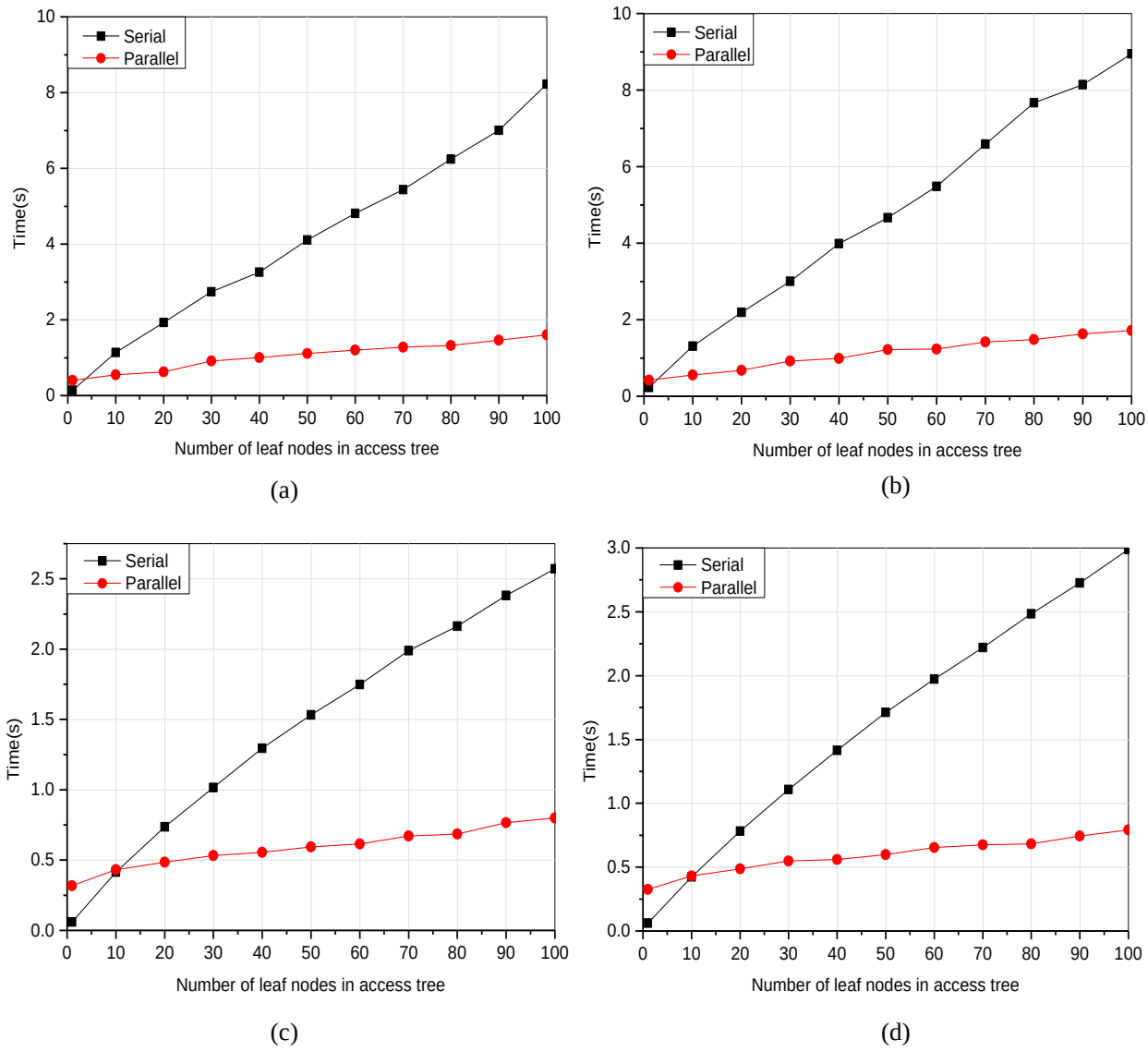


Fig. 6. Comparison between the serial computation and the parallel computation: (a) encryption time of Ref. [9] and the modified scheme; (b) encryption time of Ref. [8] and the modified scheme; (c) decryption time of Ref. [9] and the modified scheme; (d) decryption time of Ref. [8] and the modified scheme.