BMC Medical Informatics and Decision Making

RESEARCH

Open Access

A cross domain access control model for medical consortium based on DBSCAN and penalty function

Chuanjia Yao[1,2,3], Rong Jiang[1,2,3], Bin Wu[4*], Pinghui Li[5] and Chenguang Wang[3,6]

Abstract

Background Graded diagnosis and treatment, referral, and expert consultations between medical institutions all require cross domain access to patient medical information to support doctors' treatment decisions, leading to an increase in cross domain access among various medical institutions within the medical consortium. However, patient medical information is sensitive and private, and it is essential to control doctors' cross domain access to reduce the risk of leakage. Access control is a continuous and long-term process, and it first requires verification of the legitimacy of user identities, while utilizing control policies for selection and management. After verifying user identity and access permissions, it is also necessary to monitor unauthorized operations. Therefore, the content of access control includes authentication, implementation of control policies, and security auditing. Unlike the existing focus on authentication and control strategy implementation in access control, this article focuses on the control based on access log security auditing for doctors who have obtained authorization to access medical resources. This paper designs a blockchain based doctor intelligent cross domain access log recording system, which is used to record, query and analyze the cross domain access behavior of doctors after authorization. Through DBSCAN clustering analysis of doctors' cross domain access logs, we find the abnormal phenomenon of cross domain access, and build a penalty function to dynamically control doctors' cross domain access process, so as to reduce the risk of Data breach. Finally, through comparative analysis and experiments, it is shown that the proposed cross domain access control model for medical consortia based on DBSCAN and penalty function has good control effect on the cross domain access behavior of doctors in various medical institutions of the medical consortia, and has certain feasibility for the cross domain access control of doctors.

Keywords Medical consortium, Blockchain technology, Medical informatization, Access control

*Correspondence:
Bin Wu
star_amethyst@qq.com
[1] Institute of Intelligence Applications, Yunnan University of Finance and Economics, Kunming 650021, China
[2] School of Business, Yunnan University of Finance and Economics, Kunming 650021, China
[3] Yunnan Key Laboratory of Service Computing, Kunming 650021, China
[4] Yunnan Academy of Scientific and Technical Information, Kunming 650021, China
[5] Kunming First People's Hospital, Kunming 650021, China
[6] School of Information, Yunnan University of Finance and Economics, Kunming 650021, China

Backgrounds

Current research divulges a universal healthcare dilemma: mismatched medical resources, a global challenge [1]. A key resolution lies in healthcare integration, epitomized by the Shenzhen Second People's Hospital's establishment of the Dapeng New District Medical and Health Group in 2017, a consortium connecting three hospitals and 21 health centers to enhance healthcare accessibility and tiered service delivery [2]. This trend resonates globally, seen in consortia like the China-Japan Friendship Hospital Medical Consortium, Wuxi People's

Hospital Consortium, and Ruijin Luwan Regional Consortium [3], and in the U.S. through Accountable Care Organizations (ACOs) [4, 5] and the Partners HealthCare System (PHS) [6], reflecting collaborative efforts to improve care quality and cost-efficiency. Japan's Tokushukai Group, the world's third-largest medical network, further illustrates the prevalence of medical group operations [6], underscoring the trend toward hospital cooperation amidst medical informatization [7]. Enhanced data access and hospital connectivity are imperative for superior care, spurring a demand for cross-domain data sharing among institutions for streamlined patient management. Meanwhile, eliminating cross domain inconsistencies in medical data could improve the efficiency and accuracy of diagnostic processes [8]. However, this also poses cybersecurity risks, accentuating the importance of robust access control for securing medical data. Thus, ensuring secure cross-domain healthcare data access has emerged as a paramount research focus in the medical sector.

Access control mechanisms fundamentally split into priori and posterior categories, differentiated by timing, objectives, and emphasis. Priori control verifies permissions upfront based on user identities, averting unauthorized invasion and maintaining security via restrictions. Posterior control, conversely, analyzes user activity post-event to detect anomalies and breaches, providing a forensic trail through detailed logging [9–14]. Research trends lean towards priori methods, including Discretionary (DAC), Mandatory (MAC), Role-Based (RBAC), and Attribute-Based Access Control (ABAC). While innovations like a host-level DAC scheme for mobile data protection exists [8], DAC's decentralized nature, scalability limits, and Trojan vulnerability pose risks, especially at scale [10]. MAC was introduced to counter DAC's weaknesses, enhancing OS security, yet its rigidity hampers agility, suiting hierarchical systems more than extensive networks [11]. RBAC and ABAC emerged as flexible alternatives [12–14], managing permissions through roles and policies within priori controls.

Medical consortia, while fostering collaboration and data sharing, introduce new security challenges, especially in cross-domain data access. Ensuring secure access and tracking authorized practitioners' post-access activities are getting crucial, while traditional role- and policy-based models could not handle post-authorization complexities adequately, hindering collaboration and risking data security and integrity. To address this, our research combines blockchain technology, DBSCAN algorithm, and penalty function principle to propose an innovative cross domain access control model for medical consortium based on DBSCAN and penalty function. The several contributions we might make are as follows:

1. We proposed an innovative cross domain access control model-A Cross Domain Access Control Model for Medical Consortium Based on DBSCAN and Penalty Function.
2. Blockchain technology is adopted to ensure the security and credibility of access logs. Leveraging blockchain's decentralized, transparent, and immutable properties, we propose a scheme that stores access logs immutably and executes access policies via smart contracts, fortifying log credibility and medical data privacy.
3. We create a posterior access control strategy. Unlike traditional access control that focuses on authentication and policy implementation, our proposed model emphasizes security auditing based on access logs and constructs a dynamic response penalty mechanism on this basis. This posterior control can not only detect potential security threats through fine-grained data analysis, but also take immediate measures to limit the spread of risks.

Collectively, our model innovates by leveraging DBSCAN for precise log analysis, a penalty function for nuanced anomaly control, and blockchain for log integrity, presenting a robust framework for medical consortium's cross-domain access management. This research contributes a fresh perspective and methodology to enhance medical information security and facilitate data collaboration within consortia.

The subsequent sections are organized as follows: Part II reviews related work. Part III delineates three cross-domain access scenarios in medical consortia. Part IV elaborates our proposed access control model. Part V conducts comparative analysis with pertinent literature. Part VI is about the implementation of our experiments. Finally, Part VII concludes the study, and put forwards the prospect of future research.

Related work

Medical consortium

Since 2017, an increase in medical group consolidations has sparked curiosity about its impact on service integration, with patient preferences leaning towards familiar caregivers within multidisciplinary teams, hinting at integration's potential for improved care [15]. Challenges in geriatric care coordination, such as information silos, inconsistent communication, and IT disparities, underscore the complexity of achieving true care integration [16]. Evidence of success, however, emerges from initiatives like South Carolina's "Regional Cooperation Quality Initiative", linking collaboration to enhanced surgical outcomes [17].

Domestic studies distinguish between tight and loose medical consortium models based on centralization [18, 19], highlighting tight structures for diagnostic precision and resource efficiency [20]. Amid China's prevalence of loose consortia, scholars advocate for IT enhancements, resource pooling, and talent cultivation inspired by international models like Kaiser Permanente [21], promoting a modular IT platform to enhance service delivery and primary care trust [19–22]. Yet, the stakeholders of the medical consortium include the government, core hospitals, elderly care institutions, grassroots hospitals, patients, doctors, and pharmaceutical equipment suppliers. They face hurdles: mismatched values, institutional gaps, and weak governance inflate costs [23–26], necessitating cooperative strategies for value alignment, efficient resource integration, and shared benefits to amplify public value [27, 28].

In summary, medical consortia worldwide offer a stage for cross-domain doctor collaboration, underscoring the global importance of robust cross-domain access control mechanisms in realizing the full potential of these collaborative platforms.

Blockchain technology

Since the Bitcoin white paper's vision materialized through code [29], global academia has been fervently unraveling the intricacies of its "peer-to-peer electronic cash system", revealing a backbone of blockchain technology. This has ignited extensive research on blockchain's decentralized, immutable, and traceable attributes, transcending its financial origins into domains like pension funds [30], supply chain finance [31], agricultural traceability [32], consumer credit systems [33], and notably, healthcare [34]. Domestic researchers advocate for integrating blockchain into Traditional Chinese Medicine(TCM) and pharmaceutical big data, thereby unlocking the entire medical workflow, enhancing data traceability, and facilitating information sharing [35]. Extensive exploration of blockchain in healthcare underscores its potential in managing Electronic Health Records (EHRs) crucial for remote patient care—be it chronic disease management or specialized long-term care [36–38]. Immutable blockchain ensures EHRs are shared securely and privately, enhancing diagnostic precision. Blockchain's decentralized, tamper-proof nature also enriches telemedicine services, heightening transparency, reliability, and security [39], transforming remote healthcare delivery. Amidst growing concerns over centralized medical data breaches, decentralized systems leveraging blockchain promise enhanced reliability, privacy, and security, bolstering data management quality and accountability [40]. Innovations include blockchain-supported EMR systems that interface with Wireless Body Area Networks (WBANs), enabling real-time health monitoring for the elderly and chronic patients [41], addressing limitations of conventional healthcare infrastructure.

In summary, blockchain's adoption in healthcare promises medically traceable data, fortified data sharing mechanisms, and robust security protocols, underscoring its transformative potential across the healthcare landscape.

Cross domain access control

Data sharing is paramount in modern medical research but confronts substantial barriers, primarily privacy issues [42]. Cross-domain data access emerges as a vital solution, necessitating robust cross-domain control mechanisms amidst multi-domain ecosystems. Traditional models falter due to unique challenges in autonomous management, uncertain interoperability, and heightened access risks. To address these, research has progressed along two fronts:

> Model augmentations: Innovations include the Action-based Access Control (RBAC adaptation) for cross-domain needs [43], a Dynamic User Trust-based model (TC-ABAC) for cloud security [44], the Role-based Cross-Domain System Access Control(RBAC-IC) for multi-domain platforms [45], and a unified attribute-based access control(ABAC) anonymous access control model [46]. Integration of Emerging Tech: Strategies involve blockchain and encryption, such as Multi-permission Attribute Encryption for social network big data [47], blockchain solutions for Big data access inefficiencies [48], a traceable blockchain mechanism for transparency [49], smart contract systems integrating blockchain and role mapping [50], and a blockchain-based access control scheme for reputation value attributes of the Internet of Things [51]. Additionally, a decentralized identity scheme based on blockchain and attribute passwords is proposed for granular control [52]. Rong Jiang et al. further explore medical big data access control with techniques like fuzzy trust prediction [53], evolutionary game theory [54], clustering-risk assessment [55], UCON-based risk management [56] and Intuitionistic Fuzzy Trust [57].

Despite these strides, a critical review indicates a skewed focus on priori access control, with posterior control being under explored. This synthesis highlights the dynamic evolution of cross-domain access strategies in healthcare, merging traditional models with frontier technologies, while pinpointing a research gap in post-access control mechanisms.

Access logs

Cross-domain access logs encapsulate server records detailing requests that traverse domains, implicating security considerations. These logs meticulously document elements like request origins, URLs, and headers to mitigate potential vulnerabilities inherent in inter-domain web page interactions. In healthcare, as highlighted by Lillian Rostad et al., reliance on role-based access control prompts exception handling, increasing privacy risks, but meticulous log analysis can inform strategies to curb anomalies [58]. Christopher Gates et al. expose access control's inadequacies, which lead to permissive policies and data leaks, emphasizing logs' role in detecting internal breaches [59]. YE TAO et al. link mass customization with cross-domain access growth, advocating for log analysis to adapt services dynamically [60]. Ge Zhihui et al. underscore system logs' importance in anomaly detection, noting the impracticality of manual inspection in large systems, hence the rise of data-driven analysis for enhancing detection efficiency and precision [61]. While In the field of education, Liu Yi et al. selected date, time, user account, and access address as feature attributes based on the real network user access logs obtained from a certain university. Through visual analysis of the access logs, they excavated the network behavior characteristics and interests of current college student users, revealed their network behavior patterns, and provided data support for teaching managers to make decisions [62]. Meanwhile, Chen Yun et al. believe that a large amount of website visit log data can be used as material for vocational college data analysis courses, and extracting cases for course implementation could enhance students' ability to analyze data, and exercise their network security thinking [63].

In essence, cross-domain log analysis bolsters web and system security, reveals vulnerabilities, guides defensive strategies, and facilitates data-driven insights for user behavior comprehension and strategic planning. These logs are pivotal for maintaining security, reliability, and uninterrupted operations, arming administrators with tools to proactively tackle threats and reinforce digital defenses.

Specific scenarios of cross domain access inside the medical consortium

Within the consortium, cross domain access became the norm behavior between hospitals at all levels, with the main occurring scenarios being triage (graded diagnosis and treatment), referral as well as expert consultation, among others.

Scenario one: cross domain graded diagnosis and treatment

Cross domain graded diagnosis and treatment system is to grade the disease according to the severity, palliation, urgency and difficulty of treatment, and different levels of medical institutions undertake the treatment of different diseases to achieve primary first referral and two-way referral. The aim of graded medical treatment is to get the hospital focused on the care of patients with acute and severe illness, the populace has disease before the family doctor or nearby clinics, after doctor specialized diagnosis and treatment, if the condition requires, referral to other specialized clinics or hospital care, after the patient is referred for follow-up treatment, should be recommended by the doctor on referral back to the original hospital or other appropriate hospital. Hierarchical medical care through the division cooperation of all levels of medical institutes, borrowed by two-way referral, to provide continuous, integrated medical care of patients, assist the populace to find doctors and see pairs, and improve the quality of medical care. Bail out the crowded situation in hospitals, which promoted the effective use of medical resources, the division of labor and cooperation in hospitals, the populace receiving the best care, and slowly guided everyone with the disease to seek a primary doctor first and the condition to need further referral to the hospital. As Fig. 1 shows, for instance, a patient named Jack White went to see Doctor Williams, who worked at a first level hospital. After careful diagnosis, Doctor Williams thought Jack White should go to a Second-level hospital, or a Third-level one if necessary for better treatment. If Jack White got better treatment and began to recover with some nursing care. So he went back to the first level hospital for further nursing care. Such operation can help patients cut down medical expenses and reasonably utilizing medical resources. The three levels of hospitals are divided by the Chinese hospital level evaluation system. Based on the comprehensive evaluation of the hospital's technical strength, management level, equipment conditions, research capabilities, etc., from low to high, they are divided into first level, second level, and third level.

Scenario two: patients' cross domain referral

Patients' cross domain referral refers to the system of transferring patients to another medical institution. A medical prevention institution that transfers a patient diagnosed and treated by its own unit to another medical prevention institution for diagnosis, treatment or treatment according to the needs of the patient's condition is called a referral. If the patient is in a critical situation,

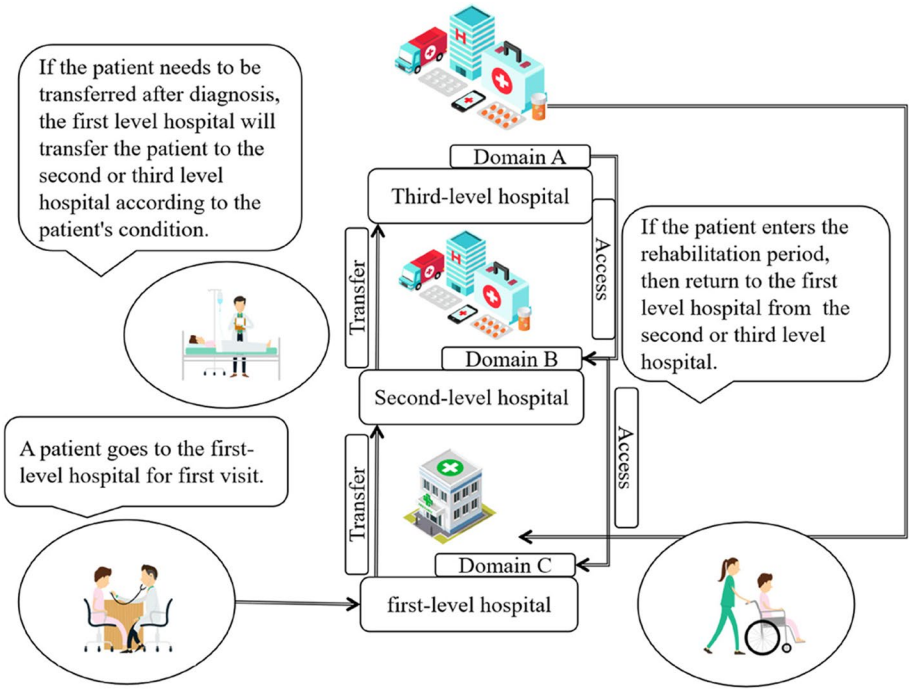


Fig. 1 Schematic diagram of graded diagnosis and treatment

accurately verifying their identity is vital to administer the appropriate treatment. For those already admitted, methods such as wristband identification, cross-referencing bedside charts, consulting electronic health records, or engaging family members or companions serve as standard practices. However, when confronted with a new patient lacking any prior identity records, establishing a provisional identity becomes imperative, enabling immediate medical intervention while alternative identification measures are pursued. The hospital would then contact with the police, furnishing them with details and, if possible, photographs of the patient to facilitate a search within their databases. Should conventional police inquiries prove unsuccessful, additional steps can be taken, including public announcements through various media platforms like the internet, television broadcasts, or social media channels such as WeChat, to broaden the search radius and potentially reach someone who can identify the patient. These measures underscore the multi-faceted approach employed to ensure that even in the absence of immediate identification, patients receive the care they urgently require while efforts to establish their true identity continue.

For instance, as Fig. 2 illustrates, a patient, Mr. Brown, required a transfer from a primary-level hospital to a secondary-level hospital due to the nature of his illness. The initial treating physician, Doctor Simith, communicated this need through an inter-domain communication platform to the secondary-level hospital. Upon agreement to accept the patient, the secondary hospital assigned an attending physician to familiarize themselves with Mr. Brown's case. Doctor Johnson, the new attending physician, then initiated a cross-domain access request in Domain B to retrieve Mr. Brown's pertinent records from Domain C. This included his basic information, previous diagnoses, treatment plans, and current health status, facilitating a comprehensive understanding of his prior treatments and informing future interventions.

While accessing Mr. Brown's data within the shared Domain C, Doctor Johnson also had the ability to review information from other relevant cases for comparative analysis. Nonetheless, excessive querying of unrelated patient data by Doctor Johnson would be flagged as inappropriate access. All such access attempts, including the full access history, were documented on an access behavior blockchain. This measure ensured accountability for Doctor Johnson's information retrieval actions and enabled the imposition of appropriate restrictions based on the actual usage pattern.

Scenario three: experts' cross domain consultation

Expert consultation means that several experts come together to discuss the patient's condition and give their own diagnosis and treatment opinions. When the patient's condition cannot be cured for a long time, or the

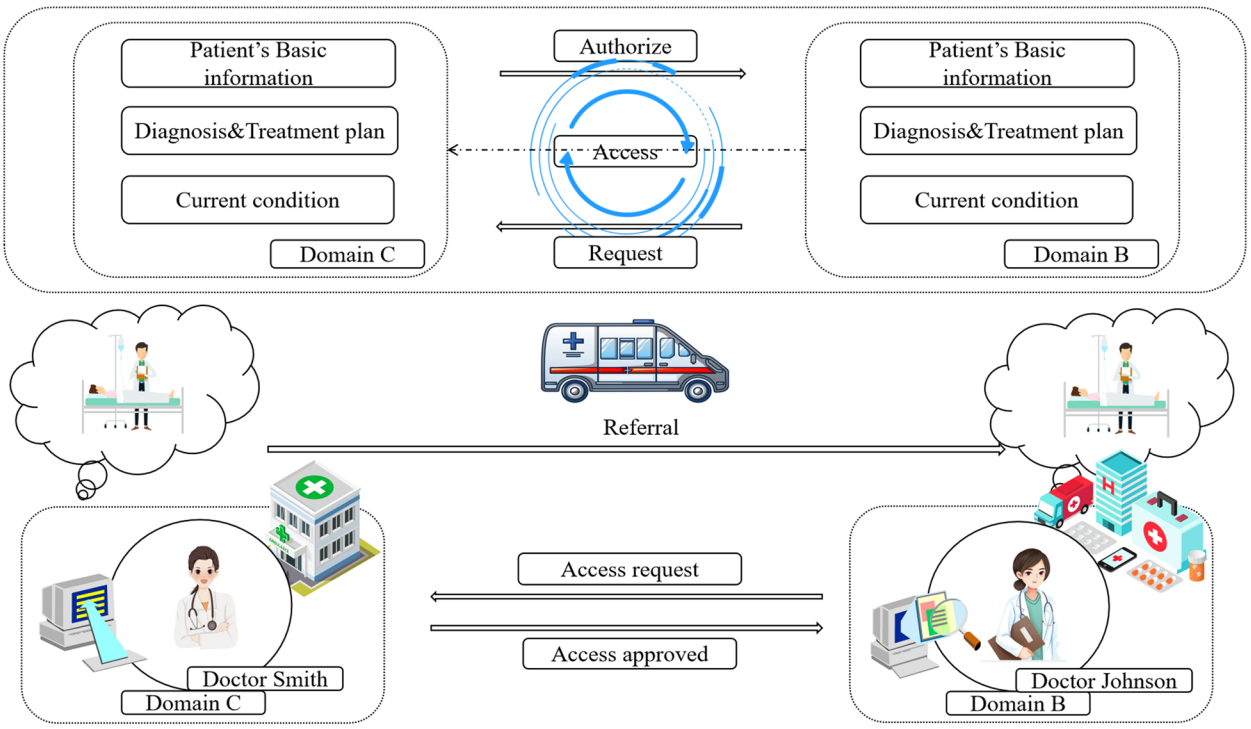


Fig. 2 Schematic diagram of referral between hospitals

diagnosis is still unclear after multiple examinations, the family members can propose consultation to the doctor in charge. The hospital or the patient can propose consultation. The hospital may notify the patient's family members when requesting consultation. The patient shall inform the doctor in charge of the consultation. Then the doctor in charge may determine, or the patient's family may propose one or several specific consultants. After confirming the consultants, the medical department of the hospital will send a consultation letter to the hospital where the consultant works. The consultation fee is generally paid by the patient. The specific number varies from region to region and the level of doctors, which can be determined through negotiation. When doctors encounter difficult cases or major clinical problems of major surgery, they will invite experts, professors and industry leaders in the hospital or outside the hospital to diagnose diseases, discuss treatment and adjust plans, so as to make patients' conditions more clear, avoid the risk of disease, and treat them more appropriately and effectively.

As shown in Fig. 3, Doctor Johnson, the attending doctor in the B domain, invited Doctor Davis, Doctor Smith, Doctor Thompson and Doctor Williams, the expert doctors in hospitals in other domains, after the application for organizing consultation was approved according to the patient's condition. After accepting the invitation, these experts visited the patient's medical information in the B domain hospital, learned about the patient's current situation, put forward different treatment opinions according to their own experience, and finally negotiated to adjust the original treatment plan. In order to ensure the authenticity and credibility of the entire expert consultation process, we would take several measures. Firstly, the attending physician's digital signature and timestamp techniques are used to verify the integrity and source of each medical record, ensuring the authenticity of the patient's medical records. Secondly, implement a multi expert self-examination and parallel review mechanism to ensure the diversity and accuracy of diagnostic opinions. In addition, establish an error correction process, and once any record errors are found, immediately notify all experts involved in the consultation through the system and make corrections. The entire verification process is expected to be completed within 24 to 48 h after receiving the medical records, to ensure the timeliness of consultation and maintain the high quality of expert consultation and medical decision-making.

Methods

This section will provide a detailed explanation of the blockchain medical consortium cross domain access control model based on DBSCAN and penalty functions

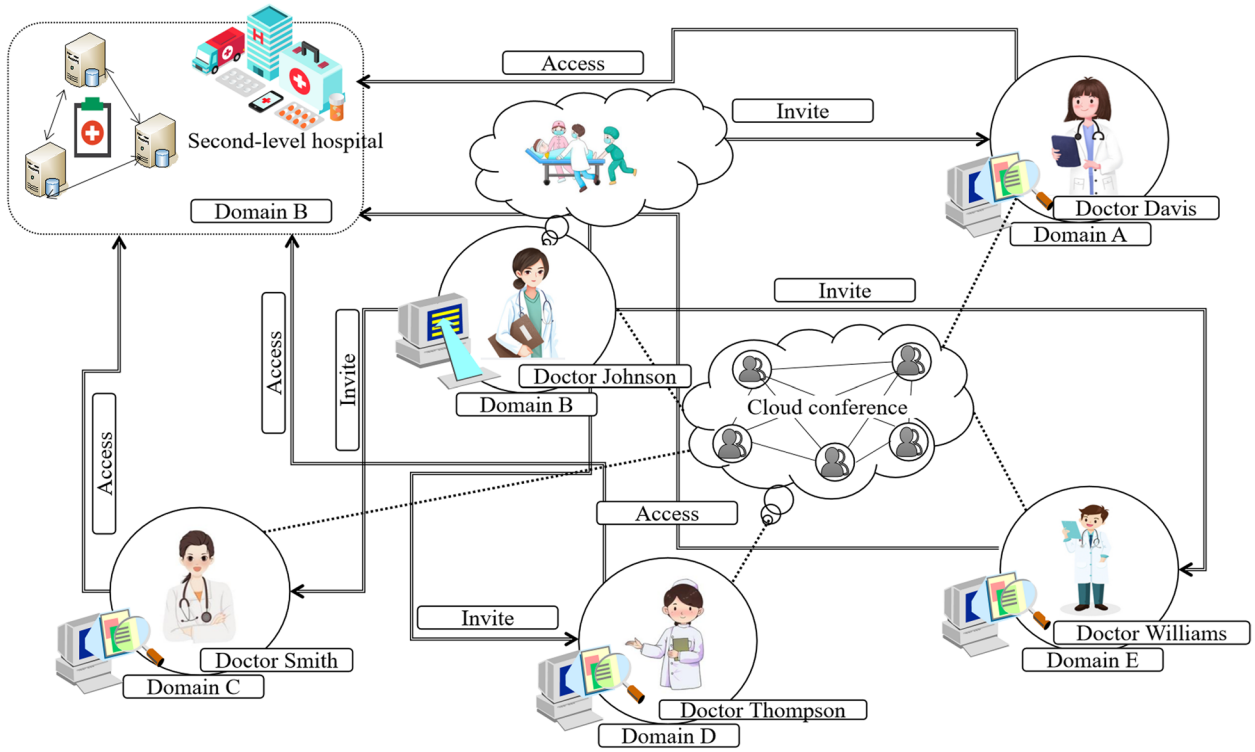


Fig. 3 Schematic diagram of experts' consultation

shown in Fig. 4, including symbol descriptions in Table 1 and specific implementation steps as follows:

Symbol definition

(1) DU (Data user): A data user is a doctor authorized to access medical resources.
(2) DO (Data owner): The data owner refers to the medical institution that owns medical resources.
(3) LR (Log recorder): A log recorder is deployed by the log management center to collect information related to cross domain access.
(4) SC (Smart Contract): By deploying smart contracts, it enables identity authentication for doctor users, uploading access logs, and achieving intelligent queries.
(5) CAL (Cross access log): Cross access log is the collection and recording of data user information.
(6) LMC (Log Management Center): The log management center is responsible for deploying log recorders, monitoring and analyzing access logs, and developing strategies for control.
(7) UCA BCSyslog (User cross access Blockchain log system):The blockchain log system we designed is a consortium blockchain with Dpos consensus and 21 nodes. It is a synchronized system mounted on the cross domain data sharing system of the medical consortium, which is used to store and query the access logs of cross domain access users, and ensure the authenticity and reliability of log data by taking advantage of the blockchain's Tamper resistance and traceable characteristics.
(8) CDDSS (Cross domain data sharing system for medical consortium): the cross domain data sharing system of the medical consortium, a cross domain sharing system built to achieve the sharing of medical and health Big data, allows doctors in all medical institutions within the medical consortium to achieve cross domain access to medical resources according to work needs.

Model description

The blockchain medical consortium cross domain access control model based on DBSCAN and penalty function proposed in this article is shown in Fig. 4. The model mainly consists of five entities: data user (DU), CDDSS, log management center (LMC), blockchain log system (BCSyslog), and log recorder (LR), SC and DL are

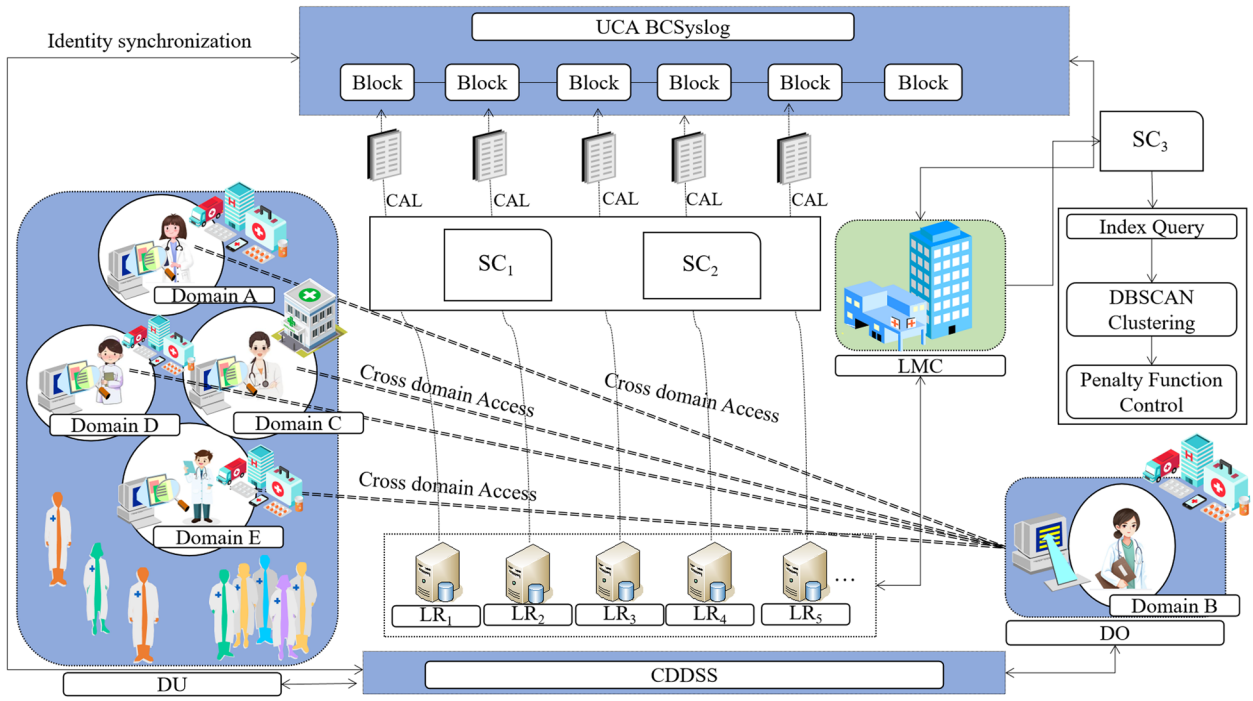


Fig. 4 Cross domain access control model for medical consortium based on DBSCAN and penalty function

Table 1 Symbol definition

Symbol	Description
DU	Data user
DO	Data owner
LR	Log recorder
SC	Smart contract
DL	Distributed ledger of Blockchain
CAL	Cross access log
LMC	Log management center
CDDSS	Cross domain data sharing system for medical consortia
UCA BCSyslog	User cross access Blockchain system log

functions that integrated into the blockchain. In order to make the workflow more clearly. We extracted the two functions and made them the roles for interaction. When data users need cross domain access for patient referrals, triage, and expert consultations, and after the data users are verified and authorized, the blockchain log system starts to run synchronously. The log management center deploys multiple log recorders to record the cross domain access logs of doctors from different medical institutions within the medical consortium, And through smart contract 1 (identity verification contract) and smart contract 2 (log upload contract), the doctor user's cross domain access logs are uploaded to the blockchain log system for storage, ensuring that the logs are not tampered with and traceable. After a period of log data collection, the log management center can use smart contract 3 (query contract) to query, analyze, and take measures for single or multiple cross domain access logs. The workflow of our model is divided into 5 steps, and the detailed flowchart of the model is shown in Fig. 5.

Step 1. Initialization

After initialization of UCA BCSyslog and CDDSS, new data users will register in the CDDSS, CDDSS will send them (pk, sk) as their certificates. UCA BCSyslog synchronizes with the certificates of DU in CDDSS.

Step 2. Identity verification

Due to the synchronization between UCA BCSyslog and CDDSS, the identity of the doctor user logging in to the CDDSS is the same as that of UCA BCSyslog, and there is no need to re-register the identity. As long as the doctor user logs in to the CDDSS, UCA BCSyslog automatically synchronizes the identity and starts running. We deploy a smart contract- SC1 to realize the identity synchronization.

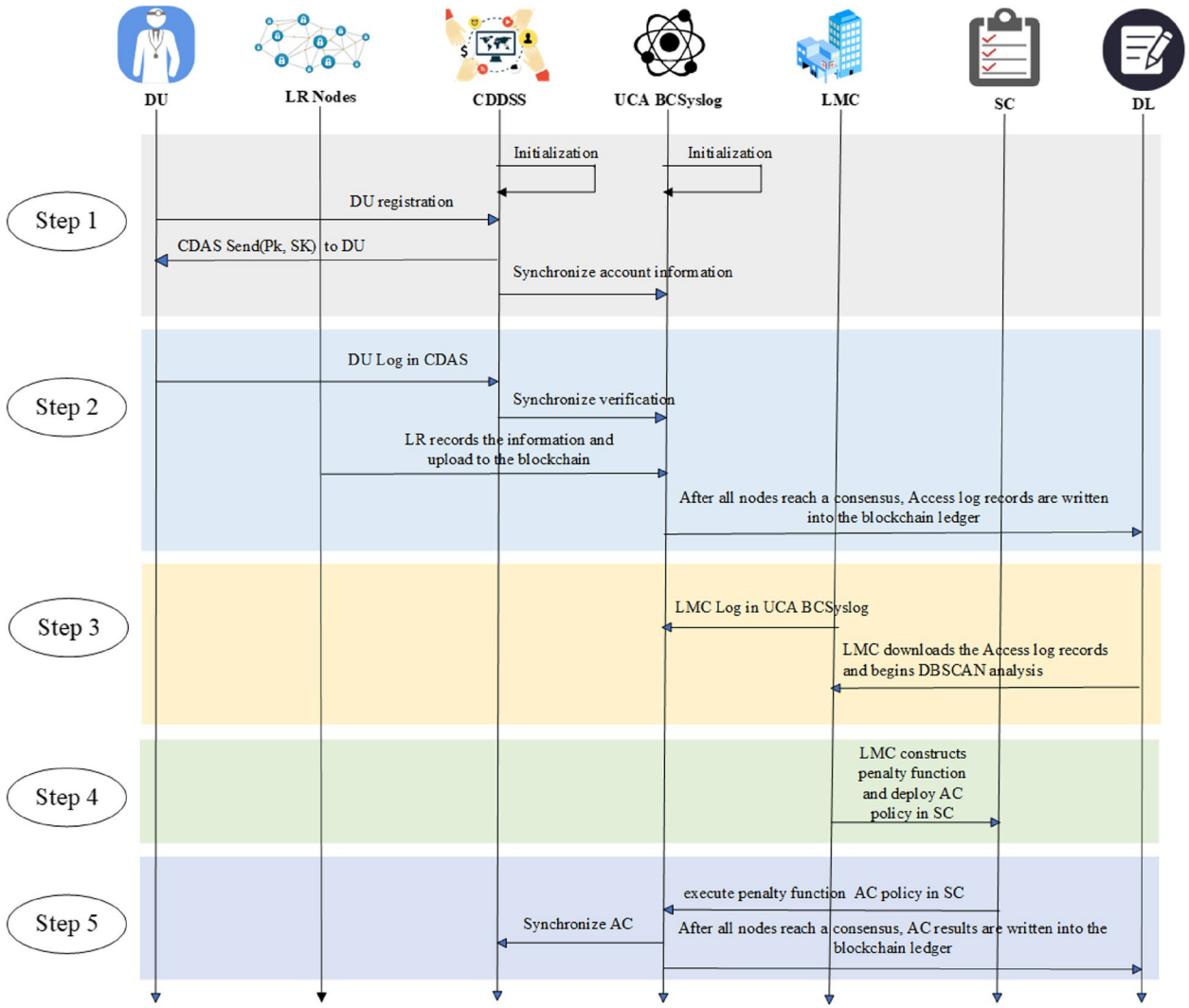


Fig. 5 Workflow diagram of the proposed model

Smart Contract 1: Blockchain access log system identity synchronization authentication

```
# Blockchain access log system identity synchronization authentication
def block_chain_auth():
    # Obtain blockchain account information from the blockchain account system
    block_chain_info = get_block_chain_info()
    # Send blockchain account information to the doctor's cross domain
data sharing system for verification
    auth_request = create_auth_request(block_chain_info)
    send_auth_request(auth_request)
    # Waiting for a response from the doctor's cross domain data sharing system
    auth_response = receive_auth_response()
    # Verify the response of the doctor's cross domain data sharing system
    if validate_auth_response(auth_response, block_chain_info):
# If the verification is successful, store the blockchain account informa-
tion in the database of the blockchain access log system
        store_block_chain_info(block_chain_info)
        # Return information on successful verification
        return " Verification successful "
    else:
        # If the validation fails, return the message that the validation failed
        return " Validation failed "
```

Step 3. Data uploading

LMC deploys numerous log recorders LR to record the access information of medical users and automatically uploads it to UCA BCSyslog for storage by executing smart contract Smart Contract 2(SC_2). After uploading the log data, it also needs to be confirmed by the alliance chain nodes. Compared to Pow, the Dpos algorithm is more efficient and can avoid the consumption of a large amount of computing resources generated by mining. We have decided to use the Dpos consensus mechanism and set 21 alliance chain nodes to verify the log data. Every 100 logs are packaged into a block, which is confirmed by consensus and stored in the distributed ledger of the blockchain for auditing.

Smart Contract 2: Automatically upload doctors' cross domain access logs to the BCSyslog

```
// Define log structure
struct AccessLog {
    address doctor;
    address domain;
    string resource;
    uint timestamp;
}
// Define blockchain log contracts
contract BlockchainLog {
    // Store all access logs
    mapping (address => AccessLog[]) accessLogs;
    // Add a new access log
    function addAccessLog(address doctor, address domain, string
resource, uint timestamp) public {
        // Store access logs into contracts
        accessLogs[doctor].push(AccessLog{doctor, domain, resource,
timestamp});
    }
    // Obtain access logs for a doctor
    function getAccessLogs(address doctor) public view returns (Access-
Log[]) {
        return accessLogs[doctor];
    }
}
// Automatically upload access logs to the blockchain logging system
when doctors access a certain resource
contract AutoUploadAccessLog {
    BlockchainLog public logContract;
    // Set blockchain log contracts when deploying contracts
    constructor(address logContractAddress) public {
        logContract = BlockchainLog(logContractAddress);
    }
    // Automatically upload access logs when doctors access a resource
    function accessResource(address doctor, address domain, string
resource) public {
        // Get the current timestamp
        uint timestamp = now;
        // Add access logs to blockchain log contracts
        logContract.addAccessLog(doctor, domain, resource, timestamp);
    }
}
```

Step 4. Data query and analysis

LMC has the rights to manage UCA BCSyslog and can download the access log to local storage, queries the cross domain access logs of doctors over a period of time through intelligent query contract Smart Contract 3(SC_3), and then performs DBSCAN clustering analysis on the query results.

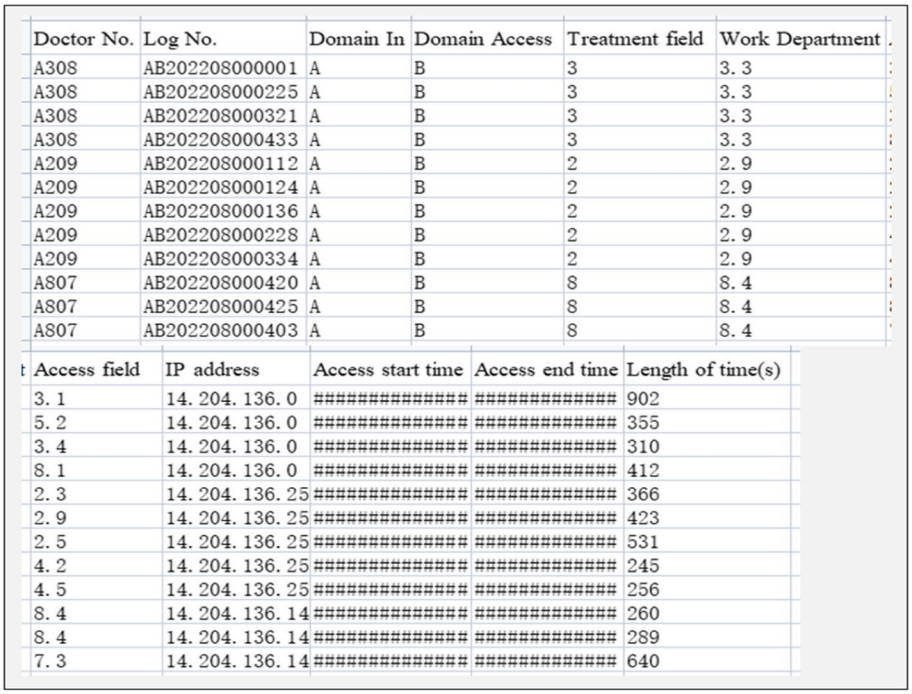
Smart Contract 3: Blockchain access log system access log query

```
// Define log structure
struct AccessLog {
    address doctor;
    address domain;
    string resource;
    uint timestamp;
}
// Define blockchain log contracts
contract BlockchainLog {
    // Store all access logs
    mapping (address = > AccessLog[]) accessLogs;
    // Add a new access log
    function addAccessLog(address doctor, address domain, string
resource, uint timestamp) public {
        // Store access logs into contracts
        accessLogs[doctor].push(AccessLog{doctor, domain, resource,
timestamp});
    }
    // Obtain access logs for a doctor
    function getAccessLogs(address doctor) public view returns (Access-
Log[]) {
        return accessLogs[doctor];
    }
}
// Query the cross domain access logs of all doctors in the blockchain
logging system and export data in SCV format
contract ExportAccessLogs {
    BlockchainLog public logContract;
    // Set blockchain log contracts when deploying contracts
    constructor(address logContractAddress) public {
        logContract = BlockchainLog(logContractAddress);
    }
    // Query cross domain access logs of all doctors and export data
in SCV format
    function exportAccessLogs() public view returns (string) {
        // Define header for SCV format
        string header = " Doctor address, domain name, resources, times-
tamp ";
        // Query the access logs of all doctors and generate CSV format data
        string data = "";
        for (address doctor in logContract.accessLogs) {
            AccessLog[] logs = logContract.getAccessLogs(doctor);
            for (int i = 0; i < logs.length; i + +) {
                AccessLog log = logs[i];
                data + = doctor.toString() + ",+ log.domain.toString() + ",+ log.
resource + ",+ log.timestamp + '\n';
            }
        }
        // Splice the header and data into complete SCV format data
        string scvData = header + '\n'+ data;
        // Returns data in SCV format
        return scvData;
    }
}
```

The data exported from the blockchain distributed ledger, as Fig. 6 shows, includes attribute values such as doctor number, log number, domain, access domain, treatment domain, work department, access domain, IP address, access start time, access end time, and duration.

Step 5. Deploying functions for control

By clustering the results, a penalty function is constructed, and the penalty function algorithm is deployed in a SC as a AC policy to control the cross domain access of doctors. The CDDSS synchronizes the AC policy and execute the operation of refusing or allowing access. Finally, the control results will be written into the DL after the nodes reaching consensus.



Doctor No.	Log No.	Domain In	Domain Access	Treatment field	Work Department
A308	AB202208000001	A	B	3	3. 3
A308	AB202208000225	A	B	3	3. 3
A308	AB202208000321	A	B	3	3. 3
A308	AB202208000433	A	B	3	3. 3
A209	AB202208000112	A	B	2	2. 9
A209	AB202208000124	A	B	2	2. 9
A209	AB202208000136	A	B	2	2. 9
A209	AB202208000228	A	B	2	2. 9
A209	AB202208000334	A	B	2	2. 9
A807	AB202208000420	A	B	8	8. 4
A807	AB202208000425	A	B	8	8. 4
A807	AB202208000403	A	B	8	8. 4

Access field	IP address	Access start time	Access end time	Length of time(s)
3. 1	14. 204. 136. 0	##############	##############	902
5. 2	14. 204. 136. 0	##############	##############	355
3. 4	14. 204. 136. 0	##############	##############	310
8. 1	14. 204. 136. 0	##############	##############	412
2. 3	14. 204. 136. 25	##############	##############	366
2. 9	14. 204. 136. 25	##############	##############	423
2. 5	14. 204. 136. 25	##############	##############	531
4. 2	14. 204. 136. 25	##############	##############	245
4. 5	14. 204. 136. 25	##############	##############	256
8. 4	14. 204. 136. 14	##############	##############	260
8. 4	14. 204. 136. 14	##############	##############	289
7. 3	14. 204. 136. 14	##############	##############	640

Fig. 6 Example diagram of cross domain access data by doctors in Hospital A

Table 2 Comparison of access control literature

Scheme	Theoretical basis	Combining blockchain	Authentication	Access control	Security Log Audit	Priori AC	Posterior AC
literature [43]	RBAC	×	√	√	×	√	×
literature [44]	ABAC	×	√	√	×	√	×
literature [45]	RBAC	×	√	√	×	√	×
literature [47]	ABAC	√	√	√	×	√	×
literature [51]	ABAC	√	√	√	×	√	×
Scheme proposed in this papaer	ALBAC	√	√	√	√	×	√

Theoretical analysis

In this section, the scheme proposed in this article is compared with the scheme proposed in the relevant literature in terms of theoretical basis, whether it is combined with blockchain, whether authentication is used, whether permission control is carried out, whether security log auditing is used, whether prior access control or posterior access control belongs, etc. As Table 2 indicates, References [43–45] are not combined with blockchain and do not focus on security log auditing, all of which belong to prior access control. Reference [47] adopt a combination of blockchain, identity verification and permission control, but they also do not use security log auditing, both of which belong to prior access control. Among them, references [43, 45] adopt role-based access control, while references [47, 51] adopt attribute based access control as their theoretical basis. Currently, research on role-based access control and attribute-based access control is relatively concentrated. Especially attribute-based access control, which can achieve fine-grained access, is often used in combination with data sharing and has broader application prospects than role based access control. The scheme proposed in this paper is to audit and analyze the user's access logs in the medical and health Big data sharing system after the user is authorized, and then implement the control, which belongs to the posterior access control. At the same time, because the access log system is combined with the blockchain, the purpose of the access log can not be tampered with and traceable to the source is realized, ensuring the authenticity and

reliability of cross domain access logs. There are significant differences and innovations compared to other literature on access control. At the same time, it can also compensate for the deficiency of priori access control that cannot monitor authorized users.

Results

Data and implementation

This paper relies on the National Natural Science Foundation of China, and the data used in this experiment is from a third-level hospital in Kunming, the cooperative unit of the author's project team. At present, the third-level hospital in Kunming and the relevant hospitals in the region are gradually promoting the construction of the regional medical consortium based on the willingness of mutual benefit and mutual assistance. The data of most of its departments have been shared within the medical consortium. The cooperative hospital shares 1200 GB of medical data with us. There are 1360 tables and 2139373 records in the database. In this paper, we prepared two experiments according to our research. The first experiment is about the time consumption of uploading access log to the blockchain. The second experiment is about the combination of DBSCAN and Penalty function. This experiment has extracted more than 860 records of doctors' cross domain visits from 11 internal departments, to simulate and analyze the cross domain access behavior of doctors within the medical consortium. We implemented both the experiments in Python 3.12 and IDE platform Pycharm 2023 professional.

Uploading of doctors' cross domain access log

5G is not only much faster than 4G, but more importantly, it reduces network latency significantly. Domestic and foreign 5G research institutions have proposed millisecond level end-to-end network latency requirements for 5G. Ideally, the end-to-end network latency is 1 ms, while the typical end-to-end network latency is 5 to 10 ms. The ideal end-to-end network latency for the 4G network we are currently using is around 10 ms, while the typical end-to-end network latency for LTE is 50 to 100 ms. Obviously, these data mean that 5G reduces end-to-end network latency to one tenth of 4G [64, 65].

Log loading is an important part of the system, in this section, we simulated the experiment of uploading of doctors' cross domain access log to the blockchain. The Dpos consensus mechanism is included. The number of consensus nodes we designed is 21. Every 100 access log will be put in one block. The block producing time is set at 1.5 s. We run five times to see the changes of time consumption with Dpos consensus mechanism. Then, we compared the impact of Internet speed on the results. We found that 5G could decrease the time consumption. For instance, in sub-plot(a) of Fig. 7, we can see the consumption of uploading 1000 access logs is between 51.31 s and 75.37 s under 4G, while in sub-plot(b) between between 6.02 s and 9.11 s.

DBSCAN clustering analysis of doctors' cross domain access log

Based on the cross domain access records of over 860 doctors from 11 departments, including department

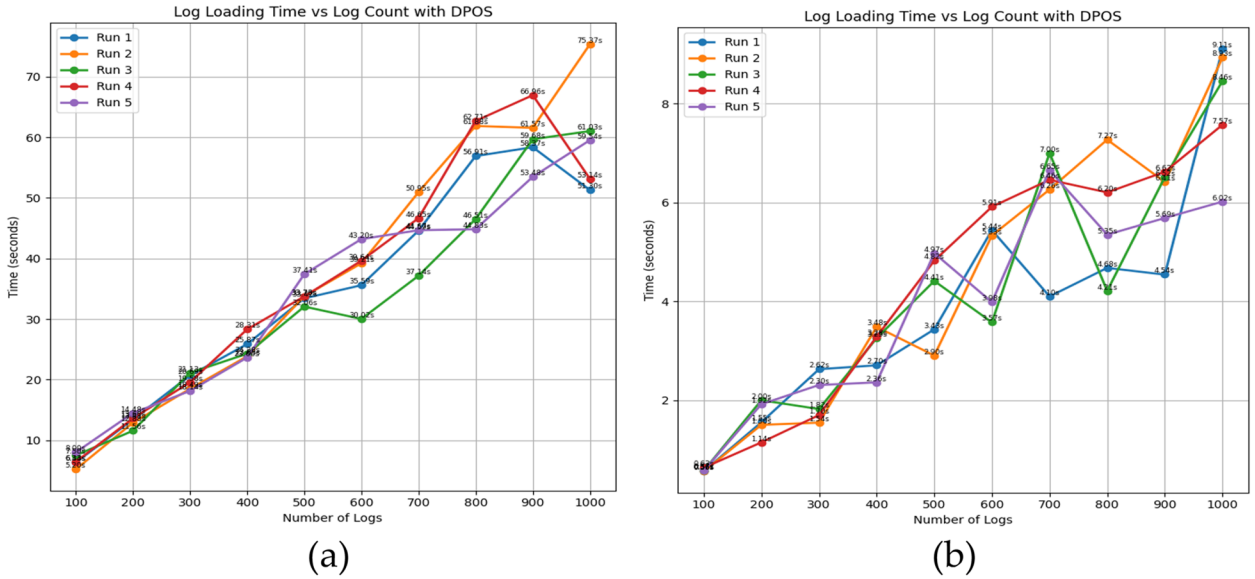


Fig. 7 Plots of uploading of doctors' cross domain access log are generated under 4G (**a**) and 5G (**b**). The value X-axis represents the number of access logs, and the value of Y-axis represents time consumption of uploading to the blockchain distributed ledger. The latency of 4G is in the range of (0.05,0.08) second, while the latency of 5G is in the range of (0.005,0.01) second

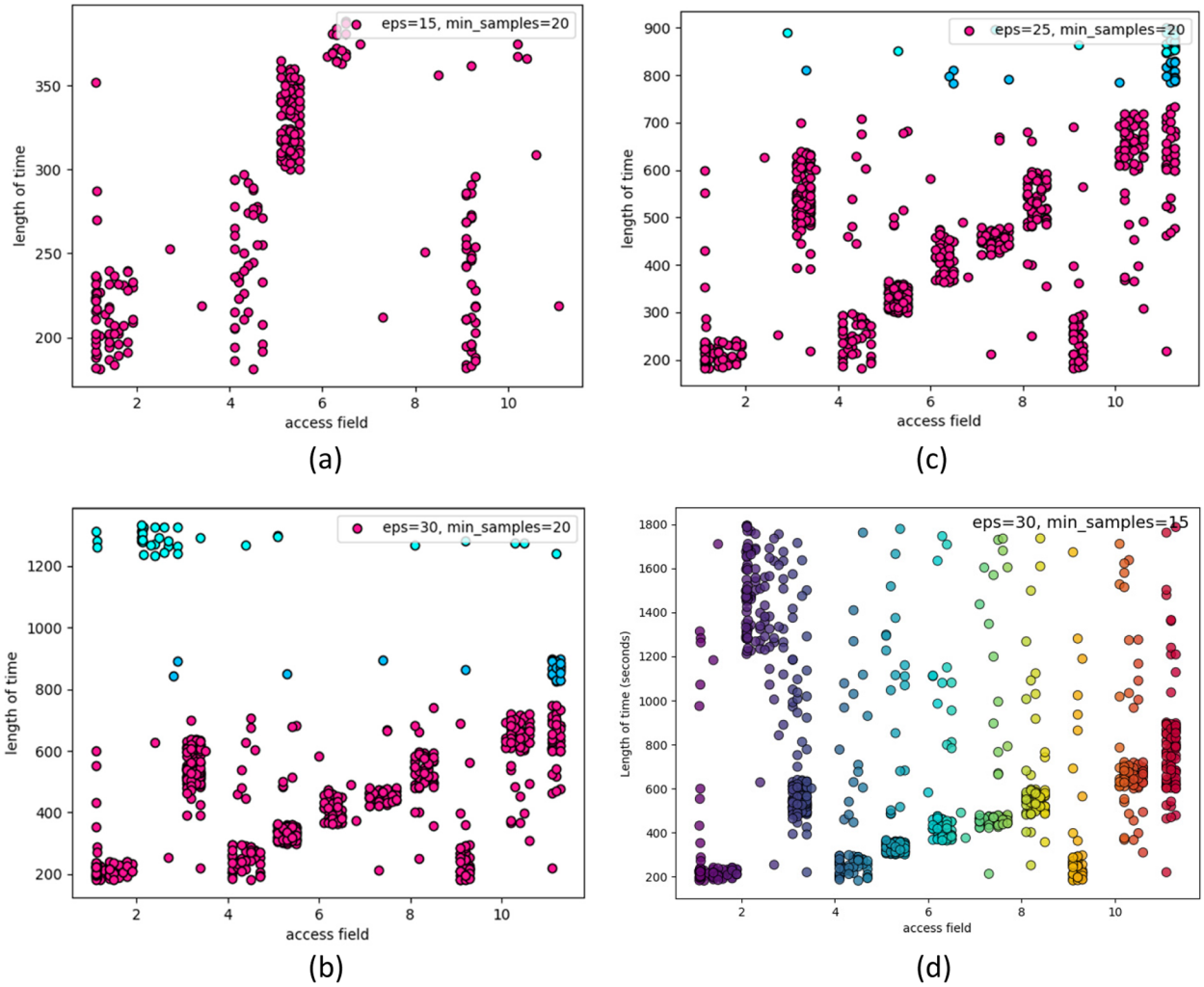


Fig. 8 DBSCAN clustering sub-plots were generated under different parameters (eps, min_s). In the sub-plots, the value X-axis represents the access time of a doctor, and the value of Y-axis represents department labels. Sub-plot (**a**)'s generation depends on parameter (15, 20), sub-plot (**b**)'s generation depends on parameter (30, 20), sub-plot (**c**)'s generation depends on parameter (25, 20), and sub-plot (**d**)'s generation depends on (30, 15)

labels (X-axis) and access time (seconds) length (Y-axis), we conducted DBSCAN clustering analysis on two important attributes of the access field. For instance, if a doctor accesses data from department 3.3, which represents pediatric otolaryngology in pediatrics and spends a length time of 590 s, then the record coordinates for this access behavior is (3.3,590) in the figure. After four parameter adjustments, we obtained different clustering results. The result of each parameter adjustment is shown in Fig. 8. Given the satisfactory clustering results of sub-plot (d) in Fig. 8, we selected it as the foundation for our clustering analysis, as it effectively illustrates the access behaviors across the 11 departments of our selected hospitals. Following the processing and annotating of sub-plot (d) in Fig. 8, we arrived at Fig. 9. In Fig. 9, upon observation, we can draw the following conclusion:

1. Figure 9 illustrates a total of 11 clusters, each representing the overall situation of medical data access for a specific department.
2. Almost every department has abnormal points of cross domain access.
3. Most doctors are more focused on the fields involved in their work.
4. Based on the consistency between the domain and access domain of traditional Chinese medicine students in cross domain access records, it was found that many doctors' visit time to other departments or undergraduate departments deviated from the normal level.

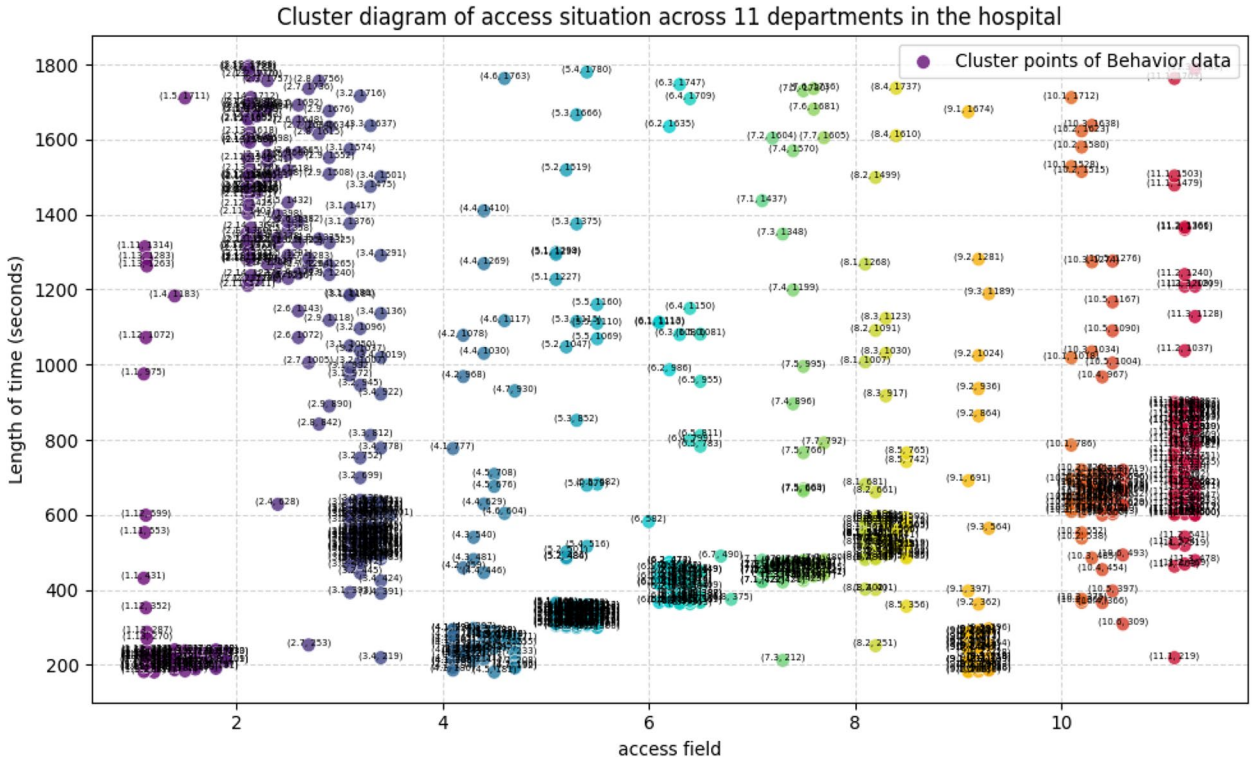


Fig. 9 DBSCAN clustering sub-plot generated under parameter (eps=30, min_samples=15). The coordinate values of each point represent the positioning of the doctor's access behavior in the figure. The value X-axis represents the access time of a doctor, and the value of Y-axis represents department labels

Based on the clustering results, we divide doctors into two categories: normal activity doctors and abnormal activity doctors.

Choice, construction of penalty function and cross domain access control

Based on the Fig. 9, we use dashed lines to delineate the normal activity boundary of doctors' cross domain access, as shown in Fig. 10. We name the dash line as boundary line, all the doctors' activity below the boundary line considered to be normal. On the contrary, those activity points above the line considered to be abnormal. Objectively speaking, once the access behavior happens, the risk of leakage exists. We can take measures to bring down the risks but can not exterminate them. Firstly and in fact, we also can not predict that a doctor's cross domain access behavior must have risks of leakage just by his access field and length of time. However, if we look at all the doctors' access behavior and their access records by DBSCAN, it is not difficult to see some doctors' access behavior is seriously deviating from most doctors. We consider this deviation as abnormal and think these abnormal behaviors points have more risks than those normal points. Normal points means most doctors can finish their access within reasonable time in a specific medical field. This is the premise of our research and explanation to why we need to constraint the doctors' access behavior even though their access has been authorized.

Aiming at the clustering situation of the resulting graph from clustering in the sub-plot (d) of Fig. 11, we randomly selected 79 cross domain access points along the dashed line and fitted multiple polynomial functions to the area formed by the normal active range of motion of the vast majority of doctors, and the fitted renderings were partially displayed as above. From the fitted graph contrasts, the function fit to sub-plot (d) of Fig. 11 performed better and was able to cover the doctor normal range of motion areas, and its fitted function results were as follows:

$$h(x) = 0.01645x^8 - 0.93x^7 + 21.82x^6 - 273.2x^5 + 1964x^4 - 8083x^3 + (1.776e+04)x^2 - (1.762e+04)x + 6263 \quad (1)$$

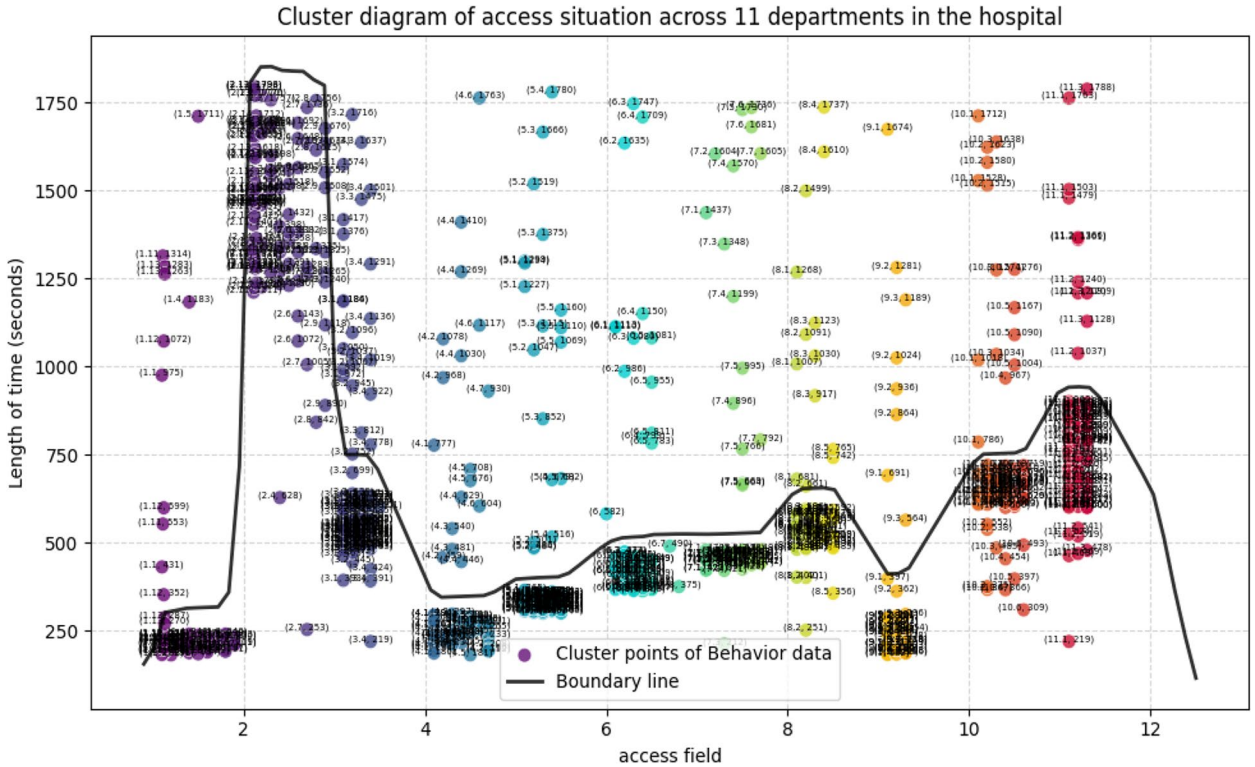


Fig. 10 DBSCAN clustering sub-plot generated under parameter (eps=30, min_samples=15). The coordinate values of each point represent the positioning of the doctor's access behavior in the figure. The value X-axis represents the access time of a doctor, and the value of Y-axis represents department labels. The black line is the boundary line to distinguish normal behavior and abnormal behavior

We used the fit function as a constraint function and, because of the risk of doctor visits across domains, on the one hand from the active domain of inter-domain visits, and on the other hand from the time of visits with the inter-domain, we used sectoring to describe the recurrent active range of doctor visits, assuming that the area of the sectoring is a measure of the risk of doctor visits across domains. Its schematic is as follows in Fig. 12:

So we get a measure of the doctor's risk across domains:

$$s = \frac{\pi(x_1^2 + x_2^2)}{4} \tag{2}$$

The lower the s coverage, the lower the risk value of doctor cross domain visits, and the greater the s coverage, the higher the risk value of doctor cross domain visits. We set s as the objective function.

Let:

$$f(x) = s = \frac{\pi(x_1^2 + x_2^2)}{4} \tag{3}$$

Based on the known conditions obtained, we adopt the interior point penalty function method to constrain the points of behavior within the viable domain constituted by the constraint function, and the known conditions for constructing the penalty function are as follows:

$$\begin{cases} h(x_1) = 0.01645x_1^8 - 0.931x_1^7 + 21.82x_1^6 - 273.2x_1^5 + 1964x_1^4 - 8083x_1^3 \\ +(1.776e+04)x_1^2 - (1.762e+04)x_1 + 6263 \\ g(x) = x_2 - h(x_1) \le 0 \\ min\, f(x) = \frac{\pi(x_1^2+x_2^2)}{4} \\ 1.1 \le x_1 \le 11.3 \end{cases}$$

An interior point penalty function is constructed based on the above known conditions as follows:

$$\varphi\left(X, r^{(k)}\right) = \frac{\pi\left(x_1^2 + x_2^2\right)}{4} - r^{(k)} \ln\left(x_2 - h(x_1)\right) \tag{4}$$

Take $r^1 = 1 * 10^{-6}, r^{(k+1)} = r^{(k)} - 0.1 * 10^{-6}, k = 1, 2, 3.....$, the calculation results are as follows in Table 3:

Each value in the Table 3 corresponds to one feasible interior point in the int S, where $f(x) = \frac{\pi(x_1^2+x_2^2)}{4}$,When k approaches infinity, namely $r_k \to 0$,the optimal solution point $\{x_k\}$ of the unconstrained problem (1) is listed inside a viable domain of the constrained problem (4),

int $S = D = \left\{(x_1, x_2)^T \middle| x_2 - h(x_1) \le 0, 1.1 \le x_1 \le 11.3\right\}$, is approaching to the best Optimization point (1.1, 79.55) on the viable domain boundary.

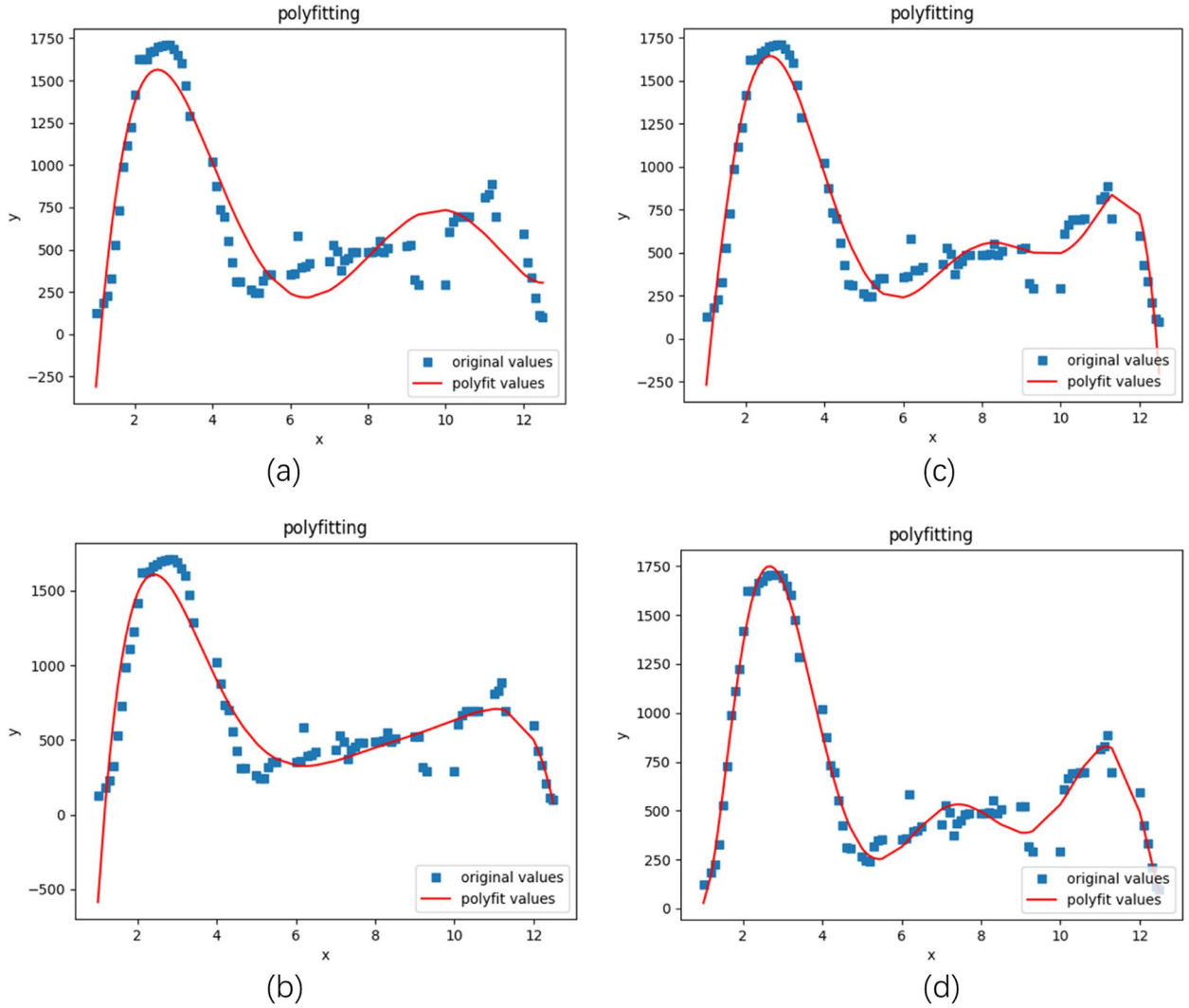


Fig. 11 The function fitting sub-plots were automatically generated by Python through polynomial regression. The value X-axis represents the access time of a doctor, and the value of Y-axis represents department labels. The blue dots represent 79 random points distributed along the boundary line of Fig. 10. Sub-plot (**a**) illustrates the result of fitting with a 5th-degree polynomial. Sub-plot (**b**) illustrates the result of fitting with a 6th-degree polynomial. sub-plot (**c**) illustrates the result of fitting with a 7th-degree polynomial. Sub-plot (**d**) illustrates the result of fitting with a 8th-degree polynomial

As Fig. 13 shows, we constructed a schematic diagram of the penalty function optimization results as above. First, the area above the red line is where the access point cannot be reached, which we call "forbidden area". The region below the red line is the region where the access point can be active and we refer to it as the "feasible area". In the case of the red line boundary under the penalty function, a boundary wall is built so that the optimization point can approach the boundary, but it does not reach the boundary and cross the boundary because once the boundary is reached, the penalty function is not solved due to the constraint of the penalty function, meaning the end of a doctor's cross domain access. Since each optimization point represents a doctor's access behavior, various boundary adjustments that can make full use of the penalty function are also verified computationally to restrict the visit behavior to the feasible domain, that is, within the scope of the domain doctor's normal activities, thus reducing the risk of doctor visits across domains and achieving the purpose of doctor cross domain access control. From Fig. 14, we can see that under the constraint of penalty function, the abnormal access behavior points get greatly decreased and optimized from sub-plot(a) to sub-plot(b) in Fig. 14.

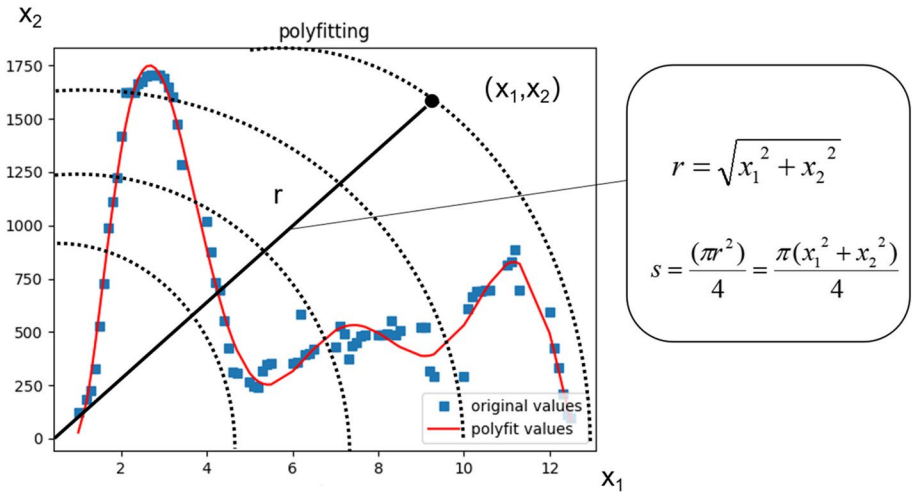


Fig. 12 Schematic of doctor risk measurement across domains. The value X_1-axis represents the access time of a doctor, and the value of X_2-axis represents department labels. In order to adapt to the construction of penalty function, we use X_2 to substitute Y

Table 3 Solution corresponding to *r* value

k	r^k	x_k
1	$1*10^{-6}$	$(4.73,193.14)^T$
2	$0.9*10^{-6}$	$(4.37,452)^T$
3	$0.8*10^{-6}$	$(4.12,669.29)^T$
4	$0.7*10^{-6}$	$(3.86,916.24)^T$
5	$0.6*10^{-6}$	$(3.57,1196.03)^T$
6	$0.5*10^{-6}$	$(3.26,1465.40)^T$
7	$0.4*10^{-6}$	$(2.92,1672.09)^T$
8	$0.3*10^{-6}$	$(2.52,1715.38)^T$
9	$0.2*10^{-6}$	$(2.06,1412.27)^T$
10	$0.1*10^{-6}$	$(1.46,540.43)^T$

Conclusions

In the paper, we proposed a novel cross-domain access control model tailored for medical consortia, leveraging the synergies between DBSCAN clustering and a penalty function within a blockchain infrastructure. This innovative integration not only underscores the importance of post-access control measures, but also demonstrates its practical utility in enhancing the security and privacy of medical data sharing across multiple institutions. In terms of real-life applicability, our model stands to significantly contribute to the medical informatics landscape by providing a robust framework for managing cross-domain access by healthcare professionals. By dynamically identifying and responding to atypical access patterns, our system can effectively deter unauthorized activities and safeguard sensitive patient information. It paves the way for safer collaboration and knowledge exchange among medical institutions, supporting graded diagnosis, referrals, and expert consultations while respecting the confidentiality and privacy requirements inherent to medical data.

During the implementation phase, several challenges emerged, chief among them being the fine-tuning of DBSCAN parameters to accurately reflect legitimate versus anomalous access behaviors without generating excessive false positives or negatives. Additionally, integrating this advanced analytic layer within a scalable and secure blockchain environment posed technical hurdles related to data handling efficiency and system interoperability. Secondly, The computation of high-dimensional functions necessitates substantial computational resources, thereby augmenting the operational burden on blockchain systems. To alleviate this load and streamline blockchain network operations, we might adopt a hybrid strategy for the future. This strategy entails offloading intricate computational tasks to off-chain environments, eliminating the need to replicate the entire computation process on-chain. Instead, only the essential results or proofs are uploaded onto the blockchain for verification and decision-making.

Looking ahead, there remains room for further refinement and expansion of this work. Future endeavors could explore the integration of machine learning techniques to enhance the accuracy of anomaly detection, potentially through predictive models that learn from historical access patterns to proactively predict and prevent security breaches. Moreover, extending the study to evaluate the scalability and generalizability of our model across larger medical consortia and diverse healthcare systems would be instrumental in validating

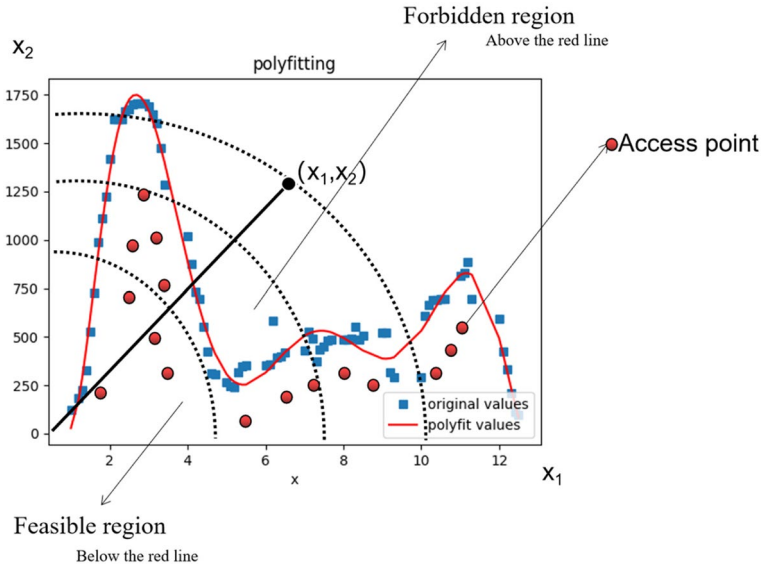


Fig. 13 Interior point penalty function optimizes results for cross domain access. The value X_1-axis represents the access time of a doctor, and the value of X_2-axis represents department labels. In order to adapt to the construction of penalty function, we use X_2 to substitute Y. The red points stands for access points

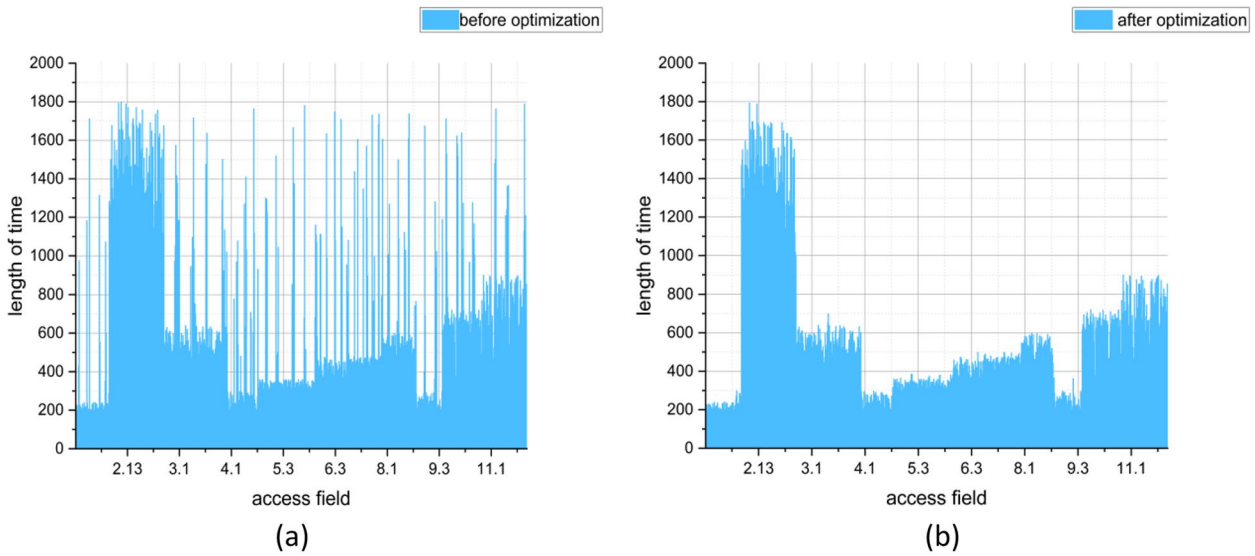


Fig. 14 Cross domain access situation sub-plots of comparison before and after control. The value X-axis represents the access time of a doctor, and the value of Y-axis represents department labels

its broad applicability. Furthermore, investigating user feedback mechanisms and incorporating user reputation metrics to build a deeper, more resilient model can enhance user adaptability, acceptance, and trust. The integration of advanced visualization tools to more effectively communicate access control decisions to healthcare providers would facilitate understanding and compliance, thereby contributing to a more seamless and secure collaboration environment within medical consortia. In summary, the cross domain access control model based on DBSCAN and penalty function proposed for medical consortia provides a potential feasible solution to address the evolving challenges of healthcare data protection in multi institutional cooperation.

Abbreviations

DU	Data user
DO	Data owner
LR	Log recorder
SC	Smart contract
DL	Distributed ledger of Blockchain
CAL	Cross access log
LMC	Log management center
UCA BCSyslog	User cross access Blockchain system log
CDDSS	Cross domain data sharing system for medical consortia

Acknowledgements
We would like to express our gratitude for the support and cooperation from all the participants. We would also like to express our gratitude to Chenguang Wang for his constructive suggestions on major revision and the support by all the projects in funding our research.

Authors' contributions
All authors contributed to the study's conception and design. Rong Jiang proposed the idea of this paper and designed the study. Chuanjia Yao designed the study and wrote the manuscript. Rong Jiang reviewed and edited the paper. Bin Wu and Pinghui Li offered constructive suggestions. Rong jiang, Chuanjia Yao, Bin Wu, and Pinghui Li prepared Figs. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 14 and Tables 1, 2 and 3. Chenguang Wang offered constructive suggestions on major revision. We confirmed that Bin Wu had the authority to act on behalf of all co-authors. All authors reviewed the manuscript. All authors have read and agreed to the final version of the manuscript.

Funding
This work was supported by the National Natural Science Foundation of China (Nos. 72471206, 71972165, 61763048), Key Projects of Basic Research for Science and Technology Foundation of Yunnan Province (No. 202001AS070031), the Central Government's Special Program for Guiding Local Science and Technology Development (No. 202307AB110009), Young and Middle aged Academic and Technical Leaders' Reserve Talent Project of Yunnan Province (No. 202305AC160011), the project of Yunnan Provincial Department of Education (No.2023Y0656).

Availability of data and materials
Not applicable.

Declarations

Ethics approval and consent to participate
Ethics committee of Yunnan Key Laboratory of Service Computing approved the study. All experimental protocols were approved by Ethics committee of Yunnan Key Laboratory of Service Computing. All methods were carried out in accordance with relevant guidelines and regulations. Informed consent was obtained from the doctors involved in our collaboration.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Received: 5 August 2023 Accepted: 19 August 2024
Published online: 16 September 2024

References

1. Haowen Y, Li Y. Integrated medical theory, practice, and effectiveness evaluation at home and abroad. Chin J Evid Based Med. 2020;20(05):585–92.
2. Lei Y, et al. Exploring strategies for responding to sudden public health incidents under the mode of group medical Alliance China. Hosp Manage. 2020;40(04):33–4.
3. Yinying Y, et al. SWOT analysis and strategies for the development of traditional Chinese medicine consortia in China. Med Content. 2019;10(05):70–3.
4. Cooper MI, Attanasio LB, Geissler KH. Maternity care clinician inclusion in Medicaid Accountable Care Organizations. PLos One. 2023;18(3):e0282679.
5. Kerrissey M, et al. Integration on the frontlines of Medicaid accountable care organizations and associations with perceived care quality, health equity, and satisfaction. Med Care Res Rev. 2023;80:519–29.
6. Shimoyama R, et al. Real-World Outcomes of Systemic Therapy in Japanese Patients with Cancer (Tokushukai REAI-World Data Project: TREAD): study protocol for a nationwide cohort study. Healthcare. 2022;10(11):2146.
7. Canaway R, et al. Identifying primary care datasets and perspectives on their secondary use: a survey of Australian data users and custodians. BMC Med Inform Decis Mak. 2022;22(1):94.
8. Sheng H, Ma L, Samson JF, et al. BarlowTwins-CXR: enhancing chest X-ray abnormality localization in heterogeneous data with cross-domain self-supervised learning. BMC Med Inform Decis Mak. 2024;24:126. https://doi.org/10.1186/s12911-024-02529-9.
9. Hsieh G, Patrick G, Foster K, Emamali G, Marvel L. Integrated mandatory access control for digital data. In Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008 (Vol. 6973, p. 13-22). SPIE; 2008.
10. Wilson D, Lavine MK. A discretionary access control method for preventing data exfiltration (DE) via removable devices. In: Digital Forensics and Cyber Crime: First International ICST Conference, ICDF2C 2009, Albany, NY, USA, September 30-October 2, 2009, Revised Selected Papers 1. Springer; 2010
11. Li N, Mao Z, Chen H. Usable Mandatory Access Control for Operating Systems. Information Assurance, Security and Privacy Services. 2009. 335.
12. Sandhu RS. Role-based access control. In Advances in computers (Vol. 46). Elsevier; 1998. p. 237-286.
13. Yuan J, et al. Role-based access control technology for digital cultural media platform. Adv Electron Commerce Web Applic Commun. 2012;2:349–54.
14. Anwar H, Shibli MA. Attribute based access control in DSpace. In 2012 7th International Conference on Computing and Convergence Technology (ICCCT). IEEE; 2012. p. 571-576.
15. Kerrissey MJ, Clark JR, Friedberg MW, Jiang W, Fryer AK, Frean M, Singer SJ, et al. Medical group structural integration may not ensure that care is integrated, from the patient's perspective. Health Affairs. 2017;36(5):885-92.
16. Svensson A. Challenges in using IT systems for collaboration in healthcare services. Int J Environ Res Public Health. 2019;16(10):1773.
17. Lockett MA, Mauldin PD, Zhang J, Marsden JE, Taber DJ, Gebregziabher M, Baliga PK, et al. Facilitated regional collaboration and in-hospital surgical complication. J Am Coll Surg. 2021;232(4):536-43.
18. Yinan Z, Huixin Ge, Ge B, Xuechen X, Xiaolin C, Shiying He, Li L. Evaluation of the operational effectiveness and internal game analysis of the loose medical joint venture China health. Resources. 2020;23(1):84–7.
19. Hejing, Qiao M, Peng L, Liu Y, Liu D. Analysis of satisfaction and existing problems of tight medical alliance from a grassroots perspective - taking the "West China Chenghua Urban Regional Medical Service Alliance" as an example modern. Prev Healthc. 2021;48(05):854–7.
20. Su M, Zhou Z, Hongliang. The influence of medical consortium and its model on the quality of urban primary medical service: based on the simulated patient approach research on China's health policy. 2021;14(09):41–46.
21. Xiong M, Wu J, Liu L, Liao X, Zhao Q. Inspiration of typical integrated medical models abroad on the construction of health management consortia in China. Chin Gen Med. 2020;23(22):2741–8+2756.
22. Wang Z, Liu Y, Jiang Y, et al. Analysis of the Impact of Patient Policy Perception in Medical Institutions on Grassroots First Visit Intention. Health Econ Res. 2019;36(06):24-27+31.
23. Jiang X, Liang R. Problems and Countermeasures in the Construction of China's Medical Consortium from the Perspective of Transaction Costs. China Health Economy. 2020;39(02):26-9.
24. Zhongjin Y, Yan D. Research on the difficulty of interest coordination and collaborative governance mechanism in the construction of medical joint venture. Chin Hosp Manage. 2021;41(01):15–8.

25. Tao He, Jian T. From "Loose" to "Tight": the implementation path of collaborative governance of medical and nursing union from the perspective of stakeholder theory. Dongyue Cong. 2023;44(05):137–47.
26. Lan W, Haibin W. Huang Longjian analysis of policy text for China's Medical Service Community - NVivo analysis based on policy tools and stakeholder perspectives. J Youjiang Ethnic Med Coll. 2024;46(02):221–6.
27. Wang C. Research on the operation dilemma and optimization strategy of China's public internet hospitals based on stakeholder theory. Med Soc. 2024;37(01):92–8.
28. Chang Li, Xue B. Fang Pengqian research on the internal interest characteristics and distribution mechanism of traditional Chinese Medicine medical federations in China. Chin Hosp Manag. 2024;44(01):14–8.
29. Wu Z. Blockchain: A Long Way to Go in the Future. Finance and Accounting. 2019;(24):77-80.
30. Dang X, Zhou Z. Path selection of blockchain technology to assist in the intelligent upgrading of China's elderly care service finance. Southwest Finance. 2021;(12):69-79.
31. Jiang R, et al. A trust transitivity model of small and medium-sized manufacturing enterprises under blockchain-based supply chain finance. Int J Prod Econ. 2022;247:108469.
32. Cui T, Yao W. Evolutionary Game Study of Agricultural Product Supply Chain Based on Blockchain Technology. Computer Application Res. 2021;38(12):3558-63.
33. Liu H, Liu Y, Yu X. Research on the Construction of China's Commercial Consumer Credit System from the Perspective of Blockchain. Credit Reporting. 2021;39(12):32-9.
34. Chen M, Xu X, Zhu X, et al. Design and implementation of a blockchain based collaborative management system for medical consortium nursing. Med Health Equip. 2024;45(03):47–55.
35. Yu J, Hu K, Ding Y. A blockchain security and privacy protection solution for clinical data of traditional Chinese medicine. World Science and Technology - Modernization of Traditional Chinese Medicine. 2021;23(10):3688-95.
36. Shamshad S, Mahmood K, Kumari S, Chen CM. A secure blockchain-based e-health records storage and sharing scheme. J Inf Secur Appl. 2020;55:102590.
37. Senshan P, Wang J. Blockchain based anti collusion sharing scheme for electronic medical records. Comput Digit Eng. 2023;51(11):2700–6.
38. Songze L, Chen L. Design of electronic medical record system based on blockchain technology. Modern Inform Technol. 2024;8(08):64–6835.
39. Ahmad RW, Salah K, Jayaraman R, Yaqoob I, Ellahham S, Omar M. The role of blockchain technology in telehealth and telemedicine. Int J Med Inform. 2021;148:104399.
40. Yaqoob I, et al. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput Appl. 2022;34(14):11475–90.
41. Wang JC, et al. A blockchain-based eHealthcare system interoperating with WBANs. Future Gener Comput Syst Int J Esci. 2020;110:675–85.
42. Wirth FN, Meurers T, Johns M, Prasser F. Privacy-preserving data sharing infrastructures for medical research: systematization and comparison. BMC Med Inform Decis Mak. 2021;21:1-13.
43. Huang Y. A behavior based cross domain access control model. J Liaoning Univ Sci Technol. 2021;23(01):1–3.
44. Ruijie P, Gaocai W, Hengyi H. Attribute access control based on dynamic user trust in cloud computing computer. Science. 2021;48(05):313–9.
45. Li Y, et al. Role-based access control model for inter-system cross-domain in multi-domain environment. Appl Sci. 2022;12(24):13036.
46. Das S, Namasudra S. Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure. IEEE Trans Industr Inform. 2023;1(19):821–9.
47. Fan K, Bai Y, Xu H, Pan Q, Li H, Yang Y. A secure cross-domain access control scheme in social networks. In ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE; 2019. p. 1-6.
48. Aodi L, et al. Big data access control mechanism based on blockchain. J Softw. 2019;30(09):2636–54.
49. Xie R, Guo Y, Li F, et al. Extended Access Control Mechanism for Cross Domain Data Flow. J Commun. 2019;40(07):67-76.
50. Sun S, Chen S, Du R. Trusted and Efficient Cross-Domain Access Control System Based on Blockchain. Sci Program. 2020;2020(1):8832568.
51. Tian H, Tian J. A blockchain-based access control scheme for reputation value attributes of the internet of things. Comput Mater Contin. 2024;1(78):1297–310.
52. Chen CM, Deng X, Kumar S, Kumari S, Islam SH. Blockchain-based medical data sharing schedule guaranteeing security of individual entities. J Ambient Intell Humaniz Comput. 2021;1-10.
53. Jiang R, Xin Y, Chen Z, Zhang Y. A medical big data access control model based on fuzzy trust prediction and regression analysis. Appl Soft Comput. 2022;117:108423.
54. Jiang R, et al. Medical big data access control model based on UPHFPR and evolutionary game. Alex Eng J. 2022;61(12):10659–75.
55. Jiang R, et al. An access control model for medical big data based on clustering and risk. Inf Sci. 2023;621:691–707.
56. Jiang R, Chen X, Yu Y, Zhang Y, Ding W. Risk and UCON-based access control model for healthcare big data. J Big Data. 2023;10(1):104.
57. Jiang R, Liu R, Zhang T, Ding W, Tian S. An electronic medical record access control model based on intuitionistic fuzzy trust. Inf Sci. 2024;658:120054.
58. Rostad L, Edsberg O. A study of access control requirements for healthcare systems based on audit trails from access logs. In 2006 22nd Annual Computer Security Applications Conference (ACSAC'06). IEEE; 2006. p. 175-186.
59. Gates C, et al. Detecting insider information theft using features from file access logs. In: 19th European Symposium on Research in Computer Security (ESORICS). Wroclaw: Wroclaw Univ Technol; 2014.
60. Tao Y, et al. User behavior analysis by cross-domain log data fusion. IEEE Access. 2020;8:400–6.
61. Zhihui GE, et al. An automated log analysis method for anomaly detection. Small Micro Comput Syst. 2022;43(03):555–60.
62. Yi L, Ming G, Liangliang T, et al. Interactive visualization analysis of network user behavior based on web log mining. J Yan'an Univ. 2023;42(03):78–85.
63. Yun C, Zhenjun Li, Haiwei Z, et al. The application of website access logs in data analysis courses in vocational colleges. Chin J Multimed Online Teach. 2023;02:13–6.
64. Liu G, Ge H, Zhang Y, et al. Perception technology based on mobile communication networks. Modern Radar. 2023;45(06):98–102.
65. Jian Z, Yu J. Smart radiotherapy scenarios in the 5G era based on blockchain architecture. Chin J Cancer Prev Treat. 2024;31(06):320–4.

Publisher's Note