A Novel Cross-domain Access Control Protocol in Mobile Edge Computing

Quanwen He
College of Computer and Cyber Security,
Fujian Normal University,
Fuzhou, Fujian, China,
e-mail: heqw15890514263@163.com

Hui Lin
College of Computer and Cyber Security,
Fujian Normal University,
Fuzhou, Fujian, China,
Engineering Research Center of Cyber Security and Education Informatization,
Fujian Province University,
Fuzhou, Fujian, China,
e-mail: linhui@fjnu.edu.cn

Jia Hu
University of Exeter
Exeter, UK
e-mail: j.hu@exeter.ac.uk

Xiaoding Wang
College of Computer and Cyber Security,
Fujian Normal University,
Fuzhou, Fujian, China,
e-mail: wangdin1982@fjnu.edu.cn

GLOBECOM 2021 - 2021 IEEE Global Communications Conference | 978-1-7281-8104-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/GLOBECOM46510.2021.9685650

Abstract—With the development of smart mobile terminals and mobile communication technologies, Mobile Edge Computing (MEC) has been applied to a variety of fields. However, MEC also brings new data security threats including the data access threat. To solve the cross-domain access control problem in MEC, this paper proposes a cross-domain access control protocol, named CDAC. In CDAC, a new user reputation evaluation strategy is proposed, which dynamically evaluates the comprehensive reputation of users based on different access behaviors of users, so that gateway nodes can evaluate user cross-domain requests. Meanwhile, different priorities are assigned according to user security levels to encourage users to regulate access behaviors to improve their reputations. Then, different gateway nodes implement cross-domain access control for users. The experiment results show that the proposed CDAC can provide efficient cross-domain access controls and achieve excellent system performances.

Index Terms—Mobile Edge Computing, Access Control, Reputation Management

I. Introduction

In recent years, with the development of smart mobile terminal technologies (such as smart phones, tablet computers, various Internet of Things devices) and mobile communication technologies such as 5G, the types of mobile applications such as facial recognition, augmented reality, virtual reality, and real-time web broadcasting have been constantly enriched. However, many mobile terminal devices only have relatively limited resources such as computing, storage, network, and power, they cannot meet service application requirements. As an inevitable product to conform to this development trend, Mobile Edge Computing (MEC) [1] is a technology that integrates and deeply integrates mobile access networks with various network services. It emphasizes closer proximity to users by migrating servers from a centralized cloud data center to the edge of the mobile network. The physical distance between servers, on the one hand, reduces the transmission delay of the network and the pressure on the backbone network; On the other hand, it shares the heavy load of the centralized server. Thereby, MEC has attracted widespread attention from the industry and academia, and it has been applied to a variety of fields such as intelligent transportation, smart city, and real-time big data analysis [2].

However, MEC also brings new data security threats, especially security threats during data access, which can easily lead to unauthorized access to data, alteration, and leakage, thereby affecting the confidentiality and integrity of data [3][4]. In order to solve the above problems, access control, as one of the important methods to ensure data security during the access process, has been applied to MEC. The existing access control researches have shortcomings and cannot meet the data security requirements in the applications of MEC [5]. For example, there might be a lot of regions in MEC such that the cross-domain access control poses a great challenge. Based on the above analysis, this paper studies the access control in multi-region scenarios. We propose a cross-domain data access control protocol CDAC.

The main contribution of this paper is summarized as follows:

- To realize cross-domain access control, we introduce the reputation management server, the cross-domain request server and the cross-domain relay server for each edge area. In addition, by establishing the collaboration between edge gateways, users of different edge areas can apply for the cross-domain access.
- To increase access control accuracy, users' reputations

978-1-7281-8104-2/21/$31.00 ©2021 IEEE

are dynamically evaluated according to their different access behaviors. And different priorities are assigned to users based on users' security levels. According to users' reputations and priorities, the efficient access control is executed on users.
- The experiment results show that the proposed CDAC can provide efficient cross-domain access controls and achieve excellent system performances.

We organize the rest of this paper as follows. The related work is given in section II. The system model is presented in section III. The implementation of the proposed CDAC is elaborated in section IV. The performance evaluation of the CDAC is given in section V. Section VI concludes this paper.

II. Related Work

The cross-domain access control problem has drawn a great attention with plenties of excellent works proposed.

Zhang et al. [6] propose an Attribute-Based Access Control (ABAC) model for cross-domain access control, in which a boundary control server is designed to provide cross-domain access control capability. Gogna and Krishna [7] develop a model that enables cross-domain mutual authentication between X.509 domain and Kerberos 5 domain using Elliptic Curve Cryptography(ECC) and Public Key Cryptography for Initial Authentication (PKINIT). Jia et al. [8] design an identity-based cross-domain authentication scheme for IoT, in which the identity-based self-authentication algorithm is employed to replace the traditional PKI authentication algorithm to guarantee the autonomy and initiative of the security domain. Ullah et al. [9] propose a lightweight and provable secure cross-domain access control scheme which implements the certificateless signcryption at the application provider side and identity based signcryption at the WBAN side. Yang et al. [10] develop a two-fold access control mechanism self-adaptive for both normal and emergency situations. The healthcare staff with proper attribute secret keys can have the data access privilege in normal application, while patient' s historical medical data can be recovered using a password-based break-glass access mechanism in emergency applications. Ahmed et al. [11] design a Wi-Fi based cross domain authentication mechanism that achieves confidentiality, scalability and privacy through mutual authentication.

There exist some blockchain based cross-domain access control mechanisms. Ma et al. [12] proposed a distributed key management mechanism based on blockchain, running multiple blockchains in the cloud to achieve cross-domain access, and introduced a variety of permission distribution and group access modes to enhance the Extensibility. Ali et al. [13] proposed a distributed blockchain-based cross-domain authority delegation access control mechanism xDBAuth, which provides access rights for internal and external users based on local and global smart contracts. Jiang et al. [14] implemented a shared cross-MEC node model based on blockchain technology, thereby improving the performance of cross-domain object detection. Yu et al. [15] proposed a multi-layer security access control model BC-BLPM, which uses a "multi-chain" structure to divide the network into different access domains and allows cross-domain interaction, thereby improving the efficiency of resource maintenance.

All these studies contribute to cross-domain access control. However, there are still two problems: (i) how to efficiently organize gateways to perform efficient cross-domain access control and (ii) how to improve the access control accuracy with the consideration of users' reputations and priorities. To solve these problem, a novel cross-domain access control protocol CDAC is proposed.

III. System Model

In this paper, we consider the cross-domain access control scenario. In this scenario, the cross-domain relay server is deployed to process cross-domain accesses. The cross-domain relay server is mainly responsible for dealing with users' cross-domain requests. And edge gateway nodes of the source area and the destination area must cooperate with each other to process the cross-domain request together. The system model is given in Figure 1. In this paper, in addition to the cross-domain relay server outside the domain, each domain also contains the following entities:

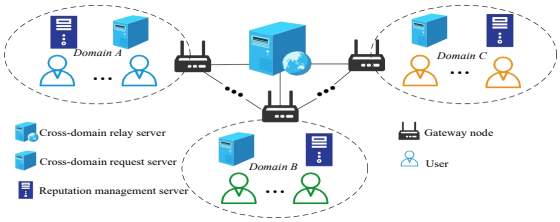

Fig. 1. System Model.

- Reputation management server: It updates and manages the reputation of users in the domain in a hierarchical manner. New users who join the domain need to register their identity on the reputation management server of the domain to generate new corresponding reputation.
- Cross-domain request server: The server used by users to initiate cross-domain request applications.
- Gateway node: The gateway node needs to apply the corresponding data analysis technology to process the user's resource data, and is also responsible for data storage. Secondly, before each user's resource data is shared in domain, the authenticity and integrity of the shared data need to be verified on the intra-domain gateway.
- Users: The users include intra-domain users and cross-domain users.

The symbols and their descriptions are given in Table I.

TABLE I

Symbols	Descriptions
$R_a^{dis_j}$	Regional reputation of user of a in region j
ξ_i	User reputation dynamic change value
m	Total number of data levels
i	Data levels
κ_s^i	The weight of i-level access success
κ_s^f	The weight of i-level access failure
AF_s^i	The number of i-level access success
AF_f^i	The number of i-level access failure
$Q_a^{dis_j}$	The cross-domain reputation in area j of user a
R_a^{syn}	The Comprehensive reputation of user a
$SubD_B$	The subdomain set of domain B
$C.attr_a$	The cross-domain attributes of user a
$C.Attr_B$	The cross-domain attributes of domain B

IV. The Implementation of the Proposed CDAC

A. Priority allocation

In this section, we introduce a hierarchical reputation management mechanism, in which the reputation management server maintains the user reputation level. Specifically, the user identity level and the accessible level of resources in the domain are divided into three levels, level 0, level 1, and level 2. For example, user A with security level 1 can access resource data in security levels 0 and 1, while user B with security level 0 can only access resource data in security level 0.

In order to encourage users to improve their own reputations, in addition to restricting the scope of their access to data resources, a new attribute "priority" is assigned to each user according to the security level. In the process of data access, users with different priorities are treated differently. The corresponding relationship between the security and the priority is shown in Table II. Specifically, we assume the priority of a user higher than another. If both users access the resource data of security level 0 at the same time, then the access request of the user with a higher priority will be processed first.

TABLE II

Security Level	Priority
$L0$	$pl = 0$
$L1$	$pl = 1$
$L2$	$pl = 2$

B. Reputation Evaluation

In order to dynamically challenge the user's reputation based on the user's access condition, we propose a dynamic reputation evaluation strategy. The proposed method can periodically update the user reputation according to the user's access condition. There are two cases of user access conditions, i.e., the successful access and the failed access. Note that the failed accesses are mainly caused by result from the unsatisfactory of the access policy based on user's attributes.

If the user a is in area A, then the regional reputation $R_a^{dis_j}$ of user a is defined as

$$R_a^{dis_j} = R_a^{sum_j} + \xi_i \tag{1}$$

with

$$\begin{cases} \xi_i = \frac{1}{m} * \sum\limits_{\text{int}=1}^{m} (\kappa_s^i * AF_s^i + \kappa_f^i * AF_f^i) \\ AF_s^i + AF_f^i = AF_{total}^i \end{cases} \tag{2}$$

where ξ_i is the dynamic change the user reputation based on the data level i; m is the total number of categories of the data level; κ_s^i and κ_s^f is the weight set for different data levels for access success and access failure; AF_s^i and AF_f^i are the number of user access successes and failures corresponding to different data levels, respectively; AF_{total}^i is the total number of user accesses of different data levels; $R_a^{sum_j}$ is the original reputation of user a in the edge area j.

If the user a is a cross-domain user at the same time, the user a comprehensive reputation R_a^{syn} is calculated as follows:

$$R_a^{syn} = \frac{1}{k} * \sum_{\text{j}=1}^{k} Q_a^{dis_j} \tag{3}$$

where k is the number of areas that user a has been in; $Q_a^{dis_j}$ is the cross-domain reputation of user a in edge area j, and the calculation method is as follows:

$$Q_a^{dis_j} = \frac{pl_a}{pl_{\max}} * R_a^{dis_j} \tag{4}$$

where pl_a and pl_{max} are the priority of user a in the edge area j and the maximum priority in the edge area j, respectively; $R_a^{dis_j}$ is the regional reputation of the user a in the edge area.

Therefore, we update the comprehensive reputation of the cross-domain user a as follows:

1) When user a needs to cross-domain access the edge domain B, the domain A where user a initially resides updates the user's regional reputation $R_a^{dis_A}$, and then calculates the cross-domain reputation $Q_a^{dis_j}$ of user a according to formula (4) and sends it to the domain B;
2) If domain B accepts, the user a registers his identity with the reputation management server in domain B, and the reputation management server in domain B records the current cross-domain reputation of user a. The gateway node informs other edge gateways by broadcasting that the user is already in domain B;
3) When user a needs to cross-domain access the domain C, the domain B updates the user a cross-domain reputation $Q_a^{dis_B}$, and at the same time obtains the cross-domain reputation $Q_a^{dis_A}$ in the record, calculates comprehensive reputation R_a^{syn} of user a according to formula (3) and sends it to the domain C;
4) If the domain C is accepted, repeat step 2;

5) When the user wants to cross-domain access again, repeat steps 3 and 2.

C. Cross-domain access control

In fact, the user's attribute required in all areas is the same. The cross-domain relay server will broadcast these attributes to all gateway nodes, which avoids the problem that cross-domain requests cannot be processed due to the attributes of the destination area and the source area are inconsistent. The resource data access process of cross domain users is shown in Figure 2.

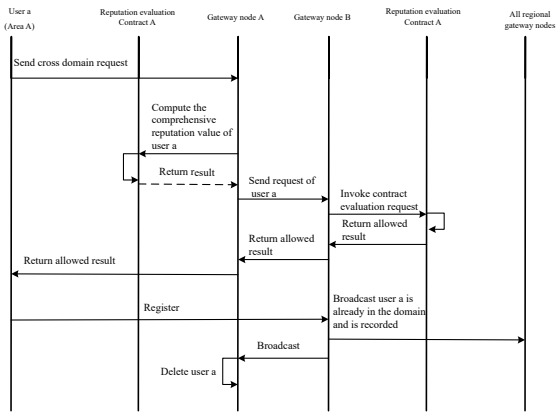

Fig. 2. Cross Domain Access Process.

1) User a in area A sends a cross-domain access request to the gateway node of domain A so as to access the data in area B;
2) After the gateway node of domain A receives it, it calls the reputation management server of domain A to re-evaluate the regional reputation $R_a^{dis_j}$ and the comprehensive reputation R_a^{syn} of user a;
3) The cross-domain relay server sends the user's comprehensive reputation R_a^{syn} and its required cross-domain attributes to the gateway node of domain B in an unified format;
4) After the gateway node of domain B receives it, it calls the cross-domain protocol to verify and evaluate the user a relevant attributes, and returns the evaluation result (access granted or denied) to the gateway node of domain A;
5) The gateway node of domain A further returns the evaluation result to the user a;
6) If the user a receives the result of allowing access, he/she needs to register with the reputation management server in domain B in the next step to join the domain B and further access the required resource data;
7) After the user a registers in domain B, the gateway node of domain B will broadcast to all other gateway nodes, and the user a is already in domain B. The cross-domain relay server records user a related information in an uniform format for subsequent evaluations;
8) After the gateway node of domain A receives the broadcast message from gateway node of domain B, it deletes the user a access authority in the domain A.

The process of the cross-domain access control is summarized in Algorithm 1.

Algorithm 1 Cross-Domain Access Control Protocol

Input: the number of successful accesses AF_s^i; the number of failed accesses AF_f^i; the identification ID_a; the area AD_a; the comprehensive reputation R_a^{syn}; the cross-area attributes $C.attr_a$
Output: access granted or access deny

1: calculate the reputation variation ξ_i according to m, AF_s^i and AF_f^i
2: calculate the regional reputation $R_a^{dis_j}$ according to ξ_i
3: calculate the cross-area reputation $Q_a^{dis_j}$ according to pl_a and pl_{max}
4: if $k = 1$ then
5: $\quad R_a^{syn} = Q_a^{dis_j}$
6: else
7: $\quad R_a^{syn} = \frac{1}{k}\sum_j^k Q_a^{dis_j}$
8: end if
9: if $AD_a \in SubD_B$ then
10: $\quad$ if $R_a^{syn} \geq \sigma_1$ then
11: $\quad\quad$ access granted
12: $\quad$ else
13: $\quad\quad$ access deny
14: $\quad$ end if
15: else
16: $\quad$ if $AD_a \notin SubD_B$ then
17: $\quad\quad$ if $R_a^{syn} \geq \sigma_2$ then
18: $\quad\quad\quad$ if $C.attr_a \equiv C.Attr_B$ then
19: $\quad\quad\quad\quad$ access
20: $\quad\quad\quad$ else
21: $\quad\quad\quad\quad$ access deny
22: $\quad\quad\quad$ end if
23: $\quad\quad$ else
24: $\quad\quad\quad$ access deny
25: $\quad\quad$ end if
26: $\quad$ end if
27: end if

Algorithm 1 describes the execution process of the cross-chain access control, in which lines 1-8, describes the reputation evaluation and lines 9-27 describe the corresponding cross-domain access control. To be specific, algorithm 1 regularly updates the user a's regional information $R_a^{dis_j}$ and comprehensive reputation R_a^{syn} according to the number of successful access AF_s^i and the number of failed accesses AF_f^i during a period of time. In addition, when the user a requests cross-domain access, the gateway node A will obtain the user's latest $R_a^{dis_j}$ and R_a^{syn}. In lines 1-2,

the reputation evaluation mechanism uses formula (2) to calculate the dynamic change ξ_i of the user's reputation based on AF_s^i and AF_f^i, and further calculate the user's regional reputation $R_a^{dis_j}$ using formula (2). In line 3, the reputation evaluation mechanism uses the formula (4) to calculate the cross-domain reputation $Q_a^{dis_j}$ of the user a based on pl_a and pl_{max}. In lines 4-8, the reputation evaluation mechanism discovers the number k of the area where the user has been located. If $k = 1$, then the user a requests a cross-domain access for the first time. And the user a originates from area A, thereby we have $Q_a^{dis_j} = R_a^{dis_j}$. If $k \neq 1$, then the formula (4) is used to calculate a's comprehensive reputation $R_a^{dis_j}$.

In addition, the algorithm evaluates cross-domain access request of the user a based on a's area, comprehensive reputation value, and cross-domain attributes, and returns the corresponding result (access granted or denied) in lines 9-27. If the user a requests the cross-domain access to area B, in lines 9-15, the algorithm first discovers the area AD_a where the user a is located, and checks whether the area AD_a belongs to the sub-domain set $SubD_B$ of area B. If it is so, then the algorithm examines whether the user a's comprehensive reputation R_a^{syn} meets the threshold σ_1. If it is satisfied, then the algorithm grants the access; otherwise, the algorithm denies the access. In lines 16-27, the algorithm aims to deal with the case that the user's area AD_a does not belong to $SubD_B$. It first determines whether the user a's comprehensive reputation R_a^{syn} meets the threshold σ_2, where the threshold σ_2 is set for users in the external domains and $\sigma_2 > \sigma_1$. If it is satisfied, then it is necessary to check whether the user a's cross-domain attributes $C.attr_a$ matches the attributes $C.Attr_B$ of area B. If it is matched, then the access is granted result; otherwise the access is denied.

V. Performance Evaluation

A. Experiment Setup

This section comprehensively evaluates the proposed CDAC in python on the computer of Inter i7 processor of 6.4GHZ, 16G memory, and Windows 7 system. The performance metrics, namely throughput, delay, CPU utilization, are adopted in performance evaluation. In addition, we also evaluate the regional reputation and the access control accuracy of the proposed protocol.

B. Experiment Result

The experiment results are shown in Figure 3 in terms of throughput, delay, and CPU utilization under different number of user requests. It can be observed from Figure 3 that as the number of requests increases from 100 to 300, the throughput increases from 80 to 300, the delay increases from 1.5s to 5s, and the CPU utilization increases from 7.5% to 13% for cross-domain access controls.

Given two users, the initial regional reputation of each user R^{dis_j} is set to 0.5. In addition, we assume one user succeeds in more than 50% of overall attempts, while the

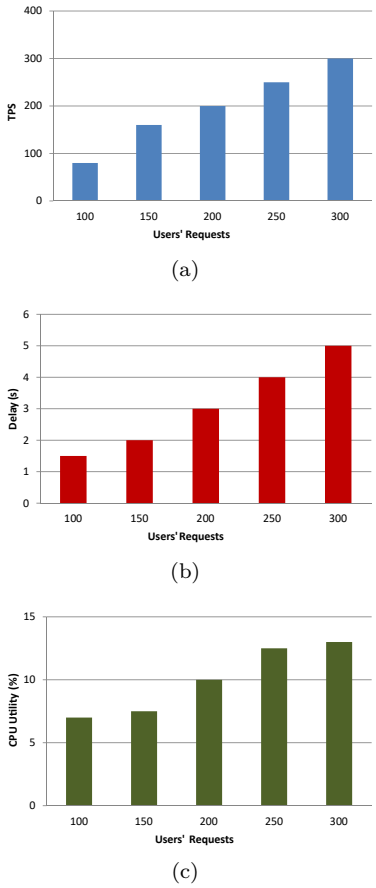

Fig. 3. The throughput, delay, and CPU utilization of access controls.

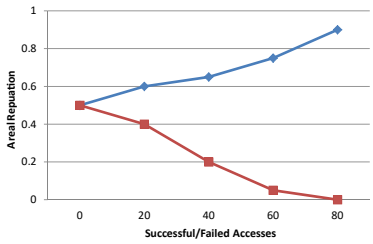

Fig. 4. The variation of the regional reputation.

other fails in more than 50% of overall attempts. The regional reputation variations under different number of success accesses and that of failed accesses are given in Figure 4. Observed from Figure 4, we find that more successful accesses results in a higher R^{dis_j} while more failed accesses contribute to a lower R^{dis_j} as we expected. In addition, when the number of failed accesses reaches 70, the R^{dis_j} drops to 0. The reason for that is as follows. The weight of successful access k_s^i is deliberately set to be lower than that of failed access k_f^i such that failed accesses affect the R^{dis_j} more than successful accesses so as to reduce the number of failed accesses.

Because the priority directly affects user's regional reputation, we also compared the time spent in dealing

with access requests sent by users of different priorities. The experiment evaluates the time spent by 6 users in cross-domain access control, where the first three users have the the same priority that is higher that that of the last three users who have the same priority. The evaluation results are shown in Figure 5. It is clearly that users with high priority spend less time than users with low priority. That indicates that assigning different priorities to users will greatly reduce the execution time of users with high priority.

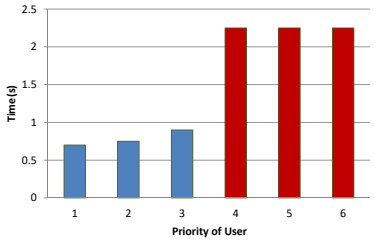

Fig. 5. The time spent for dealing with access requests.

Figure 6 shows the access control accuracy in terms of false alarm rate (FAR) and miss detection rate (MDR). Observed from Figure 5, we find that as the number of users' requests increases far and mdr grows. The maximum far and mdr of the propose CDAC are about 16% and 9%, respectively. To sum up, the proposed CDAC achieves a

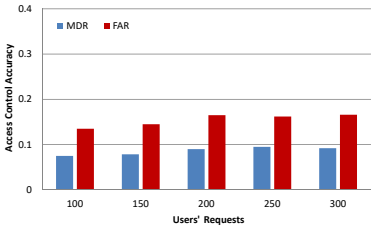

Fig. 6. The access control accuracy.

high accuracy in cross-domain access control with excellent system performances.

VI. Conclusion

In order to solve the problem of the cross-domain access control in MEC, we propose a novel access control protocol, named CDAC. In CDAC, a new user reputation evaluation mechanism is designed, which dynamically evaluates the users' comprehensive reputations. And different priorities are assigned according to user security levels to encourage users to regulate access behaviors to improve their reputations. Then, different gateway nodes implement cross-domain access control for users. The experiment results show that the proposed CDAC can provide efficient cross-domain access controls and achieve excellent system performances.

Acknowledgment

This work is supported by National Natural Science Foundation of China under Grant No. 61702103 and U1905211, Natural Science Foundation of Fujian Province under Grant No. 2020J01167 and 2020J01169.

References

[1] K. Kaur, S. Garg, G. Kaddoum, M. Guizani and D. N. K. Jayakody, "A Lightweight and Privacy-Preserving Authentication Protocol for Mobile Edge Computing," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9013856.

[2] N. Abbas, Y. Zhang, A. Taherkordi and T. Skeie, "Mobile Edge Computing: A Survey," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 450-465, 2018.

[3] Y. Mao, C. You, J. Zhang, K. Huang and K. B. Letaief, "A Survey on Mobile Edge Computing: The Communication Perspective," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2322-2358, 2017.

[4] T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu and T. Hayajneh, "Preserving Balance Between Privacy and Data Integrity in Edge-Assisted Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2679-2689, 2020.

[5] X. Li, S. Liu, F. Wu, S. Kumari and J. J. P. C. Rodrigues, "Privacy Preserving Data Aggregation Scheme for Mobile Edge Computing Assisted IoT Applications," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4755-4763, 2019.

[6] Y. Zhang and X. Liu, "An Attribute-Based Cross-Domain Access Control Model for a Distributed Multiple Autonomous Network," International Journal of Software Engineering and Knowledge Engineering, vol.30, no. 11, pp. 1851-1865, 2020.

[7] M. Gogna and C. R. Krishna, "Cross-Domain Authentication and Interoperability Scheme for Federated Cloud. In Smart Systems and IoT: Innovations in Computing, (pp. 451-461). Springer, Singapore, 2020.

[8] X. Jia, N. Hu, S. Su, et al., "IRBA: an identity-based cross-domain authentication scheme for the internet of things," Electronics, vol. 9, no. 4, pp. 634, 2020.

[9] I. Ullah, S. Zeadally, N. U. Amin, et al., "Lightweight and provable secure cross-domain access control scheme for internet of things (IoT) based wireless body area networks (WBAN)," Microprocessors and Microsystems, vol. 81, pp. 103477, 2021.

[10] Y. Yang, X. Zheng, W. Guo, et al., " Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," Information Sciences, vol. 479, pp. 567-592, 2019.

[11] F. Ahmed, X. Li, Y. Niu, C. Zhang, L. Wei and C. Gu, "UniRoam: An Anonymous and Accountable Authentication Scheme for Cross-Domain Access," 2020 International Conference on Networking and Network Applications (NaNA), Haikou City, China, 2020, pp. 198-205, doi: 10.1109/NaNA51271.2020.00042.

[12] M. Ma, G. Shi and F. Li, "Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario," IEEE Access, vol. 7, pp. 34045-34059, 2019.

[13] G. Ali et al., "xDBAuth: Blockchain Based Cross Domain Authentication and Authorization Framework for Internet of Things," IEEE Access, vol. 8, pp. 58800-58816, 2020.

[14] X. Jiang, F. R. Yu, T. Song, Z. Ma, Y. Song and D. Zhu, "Blockchain-Enabled Cross-Domain Object Detection for Autonomous Driving: A Model Sharing Approach," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3681-3692, 2020.

[15] X. Yu, Z. Shu, Q. Li and J. Huang, "BC-BLPM: A multi-level security access control model based on blockchain technology," China Communications, vol. 18, no. 2, pp. 110-135, 2021.