Enhancing security by using GIFT and ECC encryption method in multi-tenant datacenters

Article

Published Version

Creative Commons: Attribution 4.0 (CC-BY)

Open Access

Identification Number/DOI: 10.32604/cmc.2023.037150 <https://doi.org/10.32604/cmc.2023.037150>

Publisher: Tech Science Press

Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.037150

Article

Enhancing Security by Using GIFT and ECC Encryption Method in Multi-Tenant Datacenters

Jin Wang[1], Ying Liu[1], Shuying Rao[1], R. Simon Sherratt[2] and Jinbin Hu[1,*]

[1]School of Computer & Communication Engineering, Changsha University of Science & Technology, Changsha, 410004, China
[2]School of Systems Engineering, The University of Reading, RG6 6AY, UK
*Corresponding Author: Jinbin Hu. Email: jinbinhu@csust.edu.cn

Received: 25 October 2022; Accepted: 08 February 2023

Abstract: Data security and user privacy have become crucial elements in multi-tenant data centers. Various traffic types in the multi-tenant data center in the cloud environment have their characteristics and requirements. In the data center network (DCN), short and long flows are sensitive to low latency and high throughput, respectively. The traditional security processing approaches, however, neglect these characteristics and requirements. This paper proposes a fine-grained security enhancement mechanism (SEM) to solve the problem of heterogeneous traffic and reduce the traffic completion time (FCT) of short flows while ensuring the security of multi-tenant traffic transmission. Specifically, for short flows in DCN, the lightweight GIFT encryption method is utilized. For Intra-DCN long flows and Inter-DCN traffic, the asymmetric elliptic curve encryption algorithm (ECC) is utilized. The NS-3 simulation results demonstrate that SEM dramatically reduces the FCT of short flows by 70% compared to several conventional encryption techniques, effectively enhancing the security and anti-attack of traffic transmission between DCNs in cloud computing environments. Additionally, SEM performs better than other encryption methods under high load and in large-scale cloud environments.

Keywords: Multi-tenant; datacenter; user privacy; transmission security; GIFT; ECC

1 Introduction

A crucial component of cloud computing is multi-tenancy [1]. Network services are installed on a public cloud server in a multi-tenant data center to offer tenants services like processing power and data storage. However, given the wide range of tenants on the platform and the profound openness of the cloud platform, there will undoubtedly be some nasty renters with bad intentions, which could potentially result in harmful interest competition among tenants. As a result, it is possible to exploit cloud computing resources and launch assaults against other tenants, which leads to poor human-computer interaction [2]. Encrypting data storage, paying attention to information protection, and enhancing network service quality are frequently used in the cloud computing to improve data security and user privacy protection. Therefore, how to improve communication security and user privacy among tenants has been a concerning topic in the multi-tenant public environment [3].

Some methods can effectively improve user privacy and data security of multi-tenant data centers. The most used is the Internet Protocol Security (IPSec) protocol [4], which encrypts data while it is transmitted to secure it from outsiders. Data Encryption Standard (DES), triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) are three well-known symmetric encryption methods that are included in IPSec encryption policies. The IPSec protocol is used in multi-tenant data centers to encrypt data and maintain privacy, successfully guarding against data theft and tampering. Consequently, tenants' experience of human-centric engagement has increased along with the security of tenants in multi-tenant data centers.

Although using the IPSec protocol to encrypt data between tenants can enhance the security of the overall multi-tenant data center, it also highlights the drawbacks of slow encryption times and crackability. The two encryption algorithms that are most frequently employed among them are DES and AES. However, the algorithm's full running speed is low because of the small grouping of S-boxes and the intricate nonlinear structure [5]. Additionally, some traffic in the multi-tenant data centers, like user requests and acknowledge character (ACK) confirmation messages, must reply quickly. These short flows have a modest initial transmission delay, but the addition of encryption will cause a noticeable rise in the overall time. However, there are still some security vulnerabilities because the cipher's short length makes it simple to attack with extensive blasting. Lightweight block encryption algorithms with high execution efficiency and minimal computing resource consumption arise as the times' demand when classic encryption methods cannot ensure time and security. Lightweight encryption algorithms provide relative security while using less processing power and resources than conventional encryption algorithms. Numerous top-notch lightweight encryption algorithms have appeared in the market as a result of increased study into cryptography, including TEA, GIFT, and other techniques [6,7]. Some encryption methods have been successfully cracked due to the advancement of cryptography research. As a result, the complexity of encryption algorithms and the difficulty of decoding them are becoming increasingly crucial.

We propose a fine-grained Security Enhancing Method (SEM) for heterogeneous traffic in this paper. We categorize flows in multi-tenant data centers according to various criteria, and we encrypt and transmit flows using various encryption methods according to various features. A lightweight packet encryption technique called GIFT is utilized to lower the overhead of encryption and considerably lowers the ratio of encryption time for Intra-DCN short flows. To improve the security performance of data transmission for Intra-DCN long flows and Inter-DCN traffic, elliptical curve cryptography (ECC), a more complex elliptic encryption method, is implemented at the same time. This fine-grained encryption method decreases the overall transmission time of data and enhances the security of multi-tenant data. The multi-tenant data centers in a cloud computing benefit from increased security and transmission efficiency due to the fine-grained security enhancement method (SEM) suggested in this paper. Meanwhile, applying SEM to large-scale and multi-tenant data centers with massive traffic and load in cloud environment allows us to more thoroughly investigate the efficacy of distinguishing traffic for fine-grained security processing in this paper.

The main contributions of this paper are as follows:

1. To address the issue of heterogeneous traffic security transmission, we perform a thorough simulation-based study: short flows are sensitive to high latency owing to protracted encryption. In contrast long flows are vulnerable to attacks due to a complex transmission environment.

2. We introduce the characteristics of different flows in DCN and the necessity of differentiation. At the same time, the shortcomings of traditional encryption algorithms are analyzed, and the lightweight encryption algorithm GIFT and the more secure elliptic encryption algorithm ECC are introduced to meet the needs of multi-tenant data centers.

3. The proposed fine-grained security enhancement method (SEM) in this paper can improve the security of multi-tenant data centers. We demonstrate using NS-3 simulation that SEM performs significantly better than many standard encryption transmission techniques and that SEM can lower the FCT of short flows by 70%. By adjusting the topology and load strength, we further confirm the broad applicability of this technique in multi-tenant data centers.

The rest of the paper is organized as follows. In Section 2, we introduce the background and motivation about this research. In Section 3, we introduce the SEM framework in detail. In Section 4, show the experimental setup and network environment, conduct NS-3 simulation, and further analyze and discuss the experimental results. In Section 5, we introduce the related work briefly. Finally, we summarize the work of this paper and the prospect.

2 Background and Motivation

2.1 Background

Multi-tenant data centers. To reduce computing resources, effectively help reduce costs, and allocate resources based on actual application usage. A popular and effective multi-tenant approach, software as a service (SaaS), has been applied in many different contexts, such as distributed systems and online machine learning [8,9]. Tenants' data is stored in numerous databases connected in environments with multiple tenants in a single data center. As a result, data security is a significant issue in multi-tenant cloud infrastructures. For security reasons, a separate database is given to each tenant; however, this is not as cost effective. The network architecture of a multi-tenant system is seen in Fig. 1.

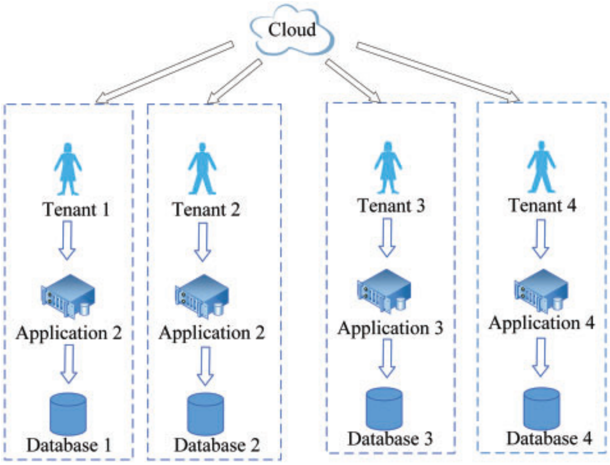

Figure 1: Multi-tenant system

Traffic characteristics. Traffic in multi-tenant data centers has its characteristics, and different applications have different network transmission requirements [10,11]:

(1) Intra-DCN short flows. Some applications require a low delay in a short time, such as short flow responses to user requests in the data center [12,13]. These short flows are delay-sensitive and bandwidth sensitive.

(2) Intra-DCN long flows. Some applications require stable throughput for a long time, such as regular backups of massive data updates inside the data center. For these long flows, data that complete sooner than the deadline does not necessarily bring more excellent value, so long flows within the data center do not require low latency.

(3) Inter-DCN traffic. A large amount of traffic must be transmitted between data centers in addition to communicating within the same data center. Such long-distance transmission pays more attention to traffic security and prevents data leakage and malicious tampering.

GIFT. Banik et al. [7] presented the updated, lightweight encryption method GIFT in ches2017 to commemorate the 10th anniversary of PRESENT [6]. Its structure is similar to the substitution-permutation network (SPN) structure of PRESENT. According to the packet length, the algorithm has two versions: GIFT-64 and GIFT-128. The round function of GIFT algorithm, each round of encryption is composed of three parts: nonlinear layer S-box, bit permutation layer and key XOR layer. GIFT is composed of only S-box and bit-wiring, but its natural bitslice data flow ensures excellent performances in all scenarios, from area-optimised hardware implementations to very fast software implementation on high-end platforms. The S-box and algorithm's structure are optimized via GIFT. The GIFT algorithm performs incredibly well and has a more compact structure that is easy to utilize. Given its strong security capability and fast processing speed, GIFT has attracted the attention of researchers from different backgrounds.

ECC. Ellipse Curve Cryptography is a public cipher encryption algorithm based on elliptic curve mathematics [14]. The mathematical principle of ECC: Given a point G on the elliptic curve and an integer k, it is easy to solve $K = kG$ (note that K solved according to kG is also a point on the elliptic curve). On the other hand, if you have two points K and G, on the elliptic curve and $K = kG$, it is challenging to figure out the integer k. The elliptic curve discrete logarithm problem is the mathematical issue that ECC is built. The public cipher is not an integer; instead, the public cipher is the point K on the elliptic curve, and the private cipher is the integer k. (actually a large integer).

2.2 Motivation

As previously indicated, the data of tenants in multi-tenant data centers is stored in a public cloud database. Therefore, achieving secure data transmission and security between tenants in a multi-tenant public environment has become a critical challenge. By encrypting and authenticating data packets during communication, IPSec safeguards user security. However, due to its slow encryption speed and low-security index, the IPSec encryption protocol cannot meet multi-tenant application demands as network demand continues to increase. Thus, there is a pressing need for transmitting traffic with different needs to be more precisely targeted and encrypted.

Encryption overhead is excessive. Intra-DCN short flows demand low delay and high-speed transmission, this is, extremely low transmission delay and response time requirements. However, due to the lengthy encryption time, it takes longer than the transmission time. Fig. 2 displays two-time types for Intra-DCN short flows. According to Fig. 2, IPSec employs AES and DES encryption methods, resulting in total encryption and decryption time accounting for 68% to 77% of total transmission time, significantly reducing the transmission performance of multi-tenant data centers.

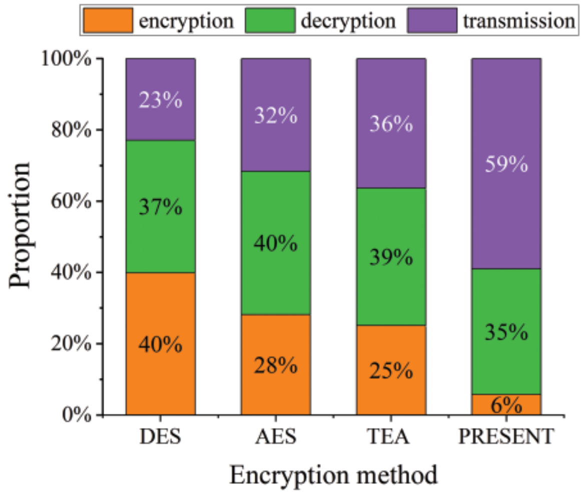

Figure 2: Using different encryption algorithms, the ratio of encryption and decryption time to flow transmission time

Differences in flow transmission delay. In addition to the Intra-DCN short flows, there are some long flows and Inter-DCN traffic. These flows are less sensitive to transmission delays. Intra-DCN long flows, most of which are some files transfer and information backup, transmission resources are enormous, and they do not need to respond in time; For Inter-DCN traffic, the delay of data transmission links between different DC is longer, and they tend to be at higher risk of cyber attacks and be stolen by crawlers [15]. The transmission delay of three different types of traffic is shown in Fig. 3, which can fully reflect the low delay and high response of short flow transmission in DCN.

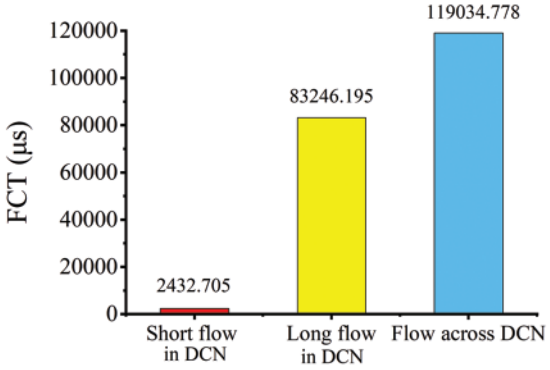

Figure 3: Transmission time of different flows

3 Design Overview

In this section, we describe the structure and algorithm of SEM. SEM is intended to improve the security of long flows and Inter-DCN traffic while lowering the encryption overhead of short flows. In particular, the transmitted packet size is used to discriminate between the long flows and the short flows. Then the suitable encryption method is chosen following their various requirements. The lightweight packet encryption technique GIFT can reduce the encryption time for short flows, satisfying the demand for low latency. We select the more complex and challenging-to-crack asymmetric encryption technique, ECC, for long flows and Inter-DCN traffic. Figs. 4 and 5 shows the SEM structure.

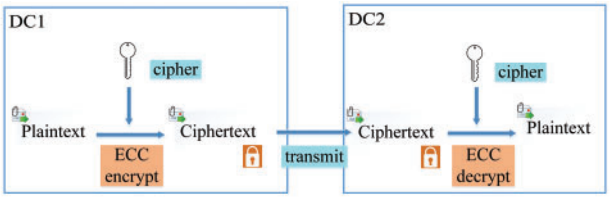

Figure 4: Inter-DCN encryption

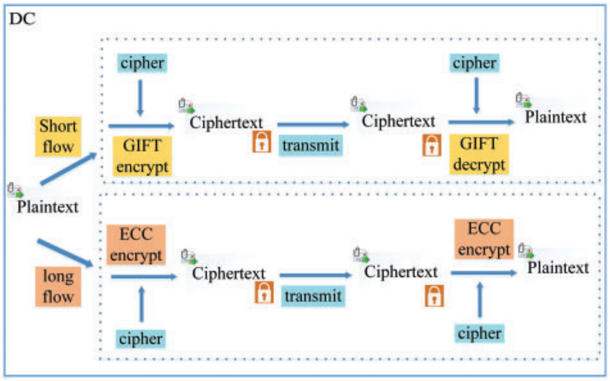

Figure 5: Intra-DCN encryption

(1) **Distinguish flows:** The typical encryption algorithm is too time-consuming for data security transmission in multi-tenant data centers due to the various traffic requirements, and it cannot meet the needs of tenants. However, long traffic and DCN traffic have significant transmission delay. Therefore, they do not need to pay close attention to the time required for data security processing, but more need to pay attention to the security problems in the transmission process. As a result, it's important to discriminate between different types of traffic and choose the most appropriate encryption technique. The size of the data packets allows for the distinction between long and short flows. The maximum threshold of the data packets for the short flows is set to 100 kb following the pertinent operational parameters.

(2) **Reduce encryption cost for Intra-DCN short flows:** Low delay and high transmission are necessary for Intra-DCN short flows in multi-tenant data centers. The FCT of the entire flow is significantly impacted by the old encryption techniques' poor computational efficiency and significant resource overhead. As a result, the requirements of low delay and high transmission of Intra-DCN short flows cannot be fully satisfied by the usual encryption technique for secure transmission. In contrast, faster computing and less resource consumption in lightweight encryption techniques allow security processing to be completed more quickly, better meeting the requirements of intra-DCN short flows [16,17]. In this paper, we encrypt a short flow in a multi-tenant data center using the GIFT packet encryption algorithm. This strategy can ensure safe transmission, reduce short flow encryption overheads, and thus reduce the FCT of short flow.

(3) **Enhance the security of Inter-DCN traffic transmission:** For Inter-DCN traffic in the data center network, they are not sensitive to transmission delay. However, the traffic across the DCN needs to pass through some public switches and data centers, and there is a greater risk of being stolen and read by illegal personnel [18,19]. Osvik et al. proposed a method of cache timing attack [20], which only takes 65 ms to get the complete AES cipher. Therefore, the research shows that the data processed by the encryption algorithm is still not too secure, and there is still a risk of theft. However, asymmetric encryption uses different ciphers for encryption and decryption. Compared with single cipher processing, private cipher decryption technology is more secure and reliable in data transmission. ECC performs with the maximum level of security compared to the widely used asymmetric encryption Rivest-Shamir-Adleman (RSA) [21]. Its mathematical basis is the computational difficulty of the discrete elliptic logarithm on Abelian addition group by using rational points on elliptic curves, which also determines that the ECC encryption algorithm is more difficult to crack than other public key ciphers. To better ensure the security of Inter-DCN traffic during transmission, this paper adopts the ECC encryption algorithm.

To ensure the other party's authenticity during the encryption procedure, both sides shake hands and confirm the other user's identification. The data has mac verification for each part. Calculate the mac of the data and compare it to the received mac to determine whether the data is complete when verifying the identity of the other party. Furthermore, for the encryption side to encrypt and the receiver to decrypt, both sides agree on a cipher if the symmetric encryption technique is employed to encrypt the communication between the two sides. Encryption is useless if the cipher is stolen while being sent. As a result, SEM uses session cipher technology to protect data transmission between users and other computers. Users of communication acquire randomly generated encryption and decryption ciphers through negotiation. Typically, it is only generated dynamically when session data encryption is necessary.

4 Implementation and Evaluation

To verify the effectiveness of the SEM proposed in this paper, we simulate and verify it under the leaf-spine network topology through network simulation. In the experiment, we use NS-3 for network simulation. It mainly includes the following four parts:

(1) Simulation Setting
(2) Proportion of Encryption Time on Intra-DCN Short Flows
(3) Security Analysis of Long Flows and Inter-DCN Traffic
(4) Further Discussion

We distinguish and handle the traffic in the multi-tenant data centers during the transmission process and use the FCT as an essential indicator to evaluate the transmission performance of the data center. In addition, we also decompose the FCT of the short flows (<100 kb) in the data center, and compare the proportion of encryption overhead of different encryption algorithms in the whole FCT. We consider the transmission of Inter-DCN traffic from the perspective of security. We are comparing the decoding difficulty, anti-attack and other vital indicators.

4.1 Simulation Setting

Network topology refers to the physical layout structure of communication lines and communication nodes in the network, which is used to reflect the structural relationship of each node. People also have higher expectations for the network's performance and security due to the rapid growth in the size of data centers and the number of services. To achieve the effects of high throughput, low delay, safety, and stability of the network, choosing a suitable topology can significantly improve the transmission quality of the data center [22,23].

In this experiment, we chose the leaf-spine topology. It is a new network topology which solves the bottleneck of the traditional three-layer network structure, such as limited transmission bandwidth and network congestion. We use the topology shown in Fig. 6 for simulation. There are three spine switches, two leaf switches, three sending terminals and two receiving terminals. The transmission bandwidth of each link is 4 gbps, and the round-trip delay of the link is 100 us. It is worth noting that during transmission, flows with packet sizes less than 100 KB are considered short flows; otherwise, they are called long flows.

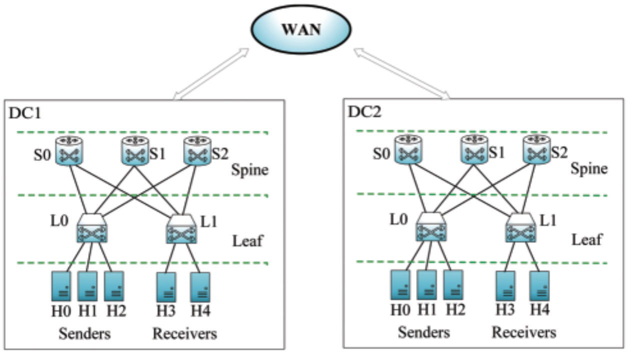

Figure 6: Leaf-Spine topology in multi-tenant data centers

4.2 Applicability of GIFT Encryption Algorithm to Intra-DCN Short Flows

In this section, we discuss in details the impact of employing the lightweight encryption algorithm GIFT for the secure transmission of short flows in multi-tenant data centers, and we also evaluate the efficiency of SEM on short flows. We select four classical encryption algorithms for experimental comparison with GIFT. The five encryption algorithms involved in the comparison are shown in Table 1.

Table 1: The five encryption algorithms

Algorithms	Describe	Structure	Safety
DES [24]	Data Encryption Standard	Feistel	Weak
AES [25]	Advanced Encryption Standard	SPN	Weak
TEA [26]	Tiny Encryption Algorithm	Feistel	Relatively weak
PRESENT [6]	A lightweight block encryption algorithm	SPN	Relatively weak
GIFT [7]	A lightweight block encryption algorithm	SPN	Relatively weak

To ensure the fairness of experimental comparison, the five encryption algorithms employ the same parameter settings to encrypt short flow packets, such as cipher length, data block size, flow size, and hardware and software environments. Each encryption method safely processes 20 different types of traffic simultaneously, reducing experimental error and ensuring the accuracy of the results.

As seen in Fig. 7, the FCT generated by various encryption techniques for short flows differs when utilized as the reference index of experimental results in the small leaf-spine topology.

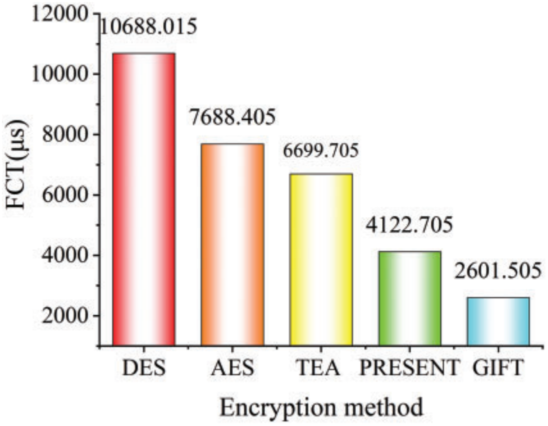

Figure 7: The FCT of short flows processed by different encryption algorithms

The FCT of several encryption techniques is displayed in Fig. 7. The time required for encryption and decryption of the two related encryption techniques is represented by the height difference between the two columns. DES and AES have far higher FCTs than the three lightweight encryption algorithms, according to the data in Fig. 7. They both use simple encryption techniques, but their FCTs differ. The GIFT has the least FCT, which is followed by Present. TEA's FCT is 1.68 times more than both PRESENT and GIFT's FCTs. Unrelatedly, the present FCT is roughly 1.68 times more than the value of gifts. Data is continuously transformed using the golden ratio as part of the TEA algorithm's encryption concept to ensure that each encryption operation is unique. The TEA method has a straightforward structure and is simple, although it takes 32 iterations. As a result, TEA encryption takes longer than other quick techniques. The newer, more condensed variant of PRESENT is called GIFT. Its FCT is 40% lower than PRESENT, and it processes security requests more quickly.

We also examine how different encryption algorithms affect the FCT of short flows. The percentage of security processing overhead for five encryption techniques on short flows is shown in Fig. 7 and is expanded in Fig. 8. The transmission delay on the link, the packet decryption time, and the packet encryption time should all be divided into the FCT of short flows. We incorporate the encryption time and decryption time into the security processing cost of the encryption algorithm to more easily observe the effect of the encryption technique on short-flow transmission. The security processing overhead of GIFT, which is relatively minimal for the whole FCT, amounts to only 6% of the total FCT of short flows, as seen from the percentage stacking column.

The GIFT encryption algorithm can process data quickly and reliably. Compared with other algorithms, GIFT can significantly reduce the time required to encrypt and decrypt short flows during transmission. It can better meet the demands of rapid and little delayed short flows.

4.3 Security Analysis of Long Flows and Inter-DCN Traffic

Heavy-tailed distribution [27,28] is a characteristic of multi-tenant Inter-DCN communication, meaning that 90% of flows are short and 10% are long, but only 10% of long flows cover 90% of the data. Because of this traffic distribution, long flows exhibit the trait of being sensitive to data throughput. A variety of data information is being transmitted simultaneously across multiple data centers. Due to security flaws, this long-distance transmission is susceptible to harmful assaults, including data leaks and information tampering. As a result, the criteria for this type of traffic are the same as those for Intra-DCN long flows in multi-tenant data centers. Data security needs to be strengthened to prevent damage from hostile assaults, increase traffic flow, and secure data. In this paper, there are strict security requirements for communication between DCNs. We weigh the benefits and drawbacks of several encryption methods before selecting an asymmetric approach with a high level of security.

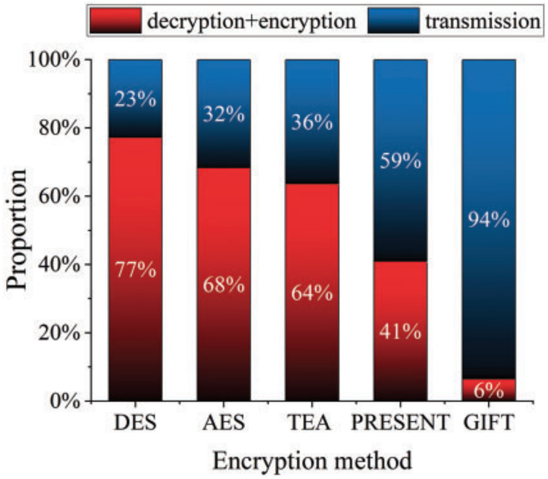

Figure 8: The proportion of encryption and decryption time and transmission time processed by different encryption algorithms

Current asymmetric encryption techniques frequently use the RSA encryption algorithm, the first generation of modern encryption algorithms [29]. The concept of prime number decomposition serves as the foundation for the significant mathematical premise. Public ciphers are created using the product of two prime numbers and two private ciphers. Prime number multiplication is pretty straightforward throughout the entire procedure; however, reverse decomposing the result is quite challenging and intricate. The transmission security of long flows will be strengthened as the cipher length increases. Still the same time, the computation will become more sophisticated, and the essential multiplication operation will become more complex.

In the new generation algorithm trend, ECC is a well-liked encryption algorithm [14]. It is a public cipher encryption technique built on the theory of elliptic curves. The main benefits of ECC include its ability to use fewer ciphers, high-level security, quick processing, reduced storage requirements, and limited transmission bandwidth. For a thorough comparison of RSA, ECC, and GIFT [7], see Table 2.

As shown in Table 2, as the latest symmetric encryption algorithm in recent years, GIFT has the advantages of short encryption and decryption time and fast speed, but it lacks in ensuring data security. Therefore, if the GIFT encryption technique is employed for Intra-DCN long flows and Inter-DCN traffic, compared to ECC and RSA, it will present a higher risk of cipher leakage. Additionally, we must accept a greater chance of data leakage; once the data is destroyed, traffic in multi-tenant data centers will suffer from poor throughput. Additionally, as security performance improves, the cipher length of RSA will grow exponentially, resulting in high encryption and decryption complexity, longer processing times, and more significant network loss. Simply put, neither the popular asymmetric encryption technique RSA nor the most recent symmetric encryption scheme GIFT is appropriate for DCN. To achieve high-throughput application effects, we apply the ECC encryption technique in Inter-DCN long flows and the Inter-DCN traffic to ensure secure transmission and quick encryption and decryption of traffic packets for each flow.

Table 2: Comparison of RSA, ECC, and GIFT

Reference index	ECC	RSA	GIFT
Safety intensity	Strong	Relatively strong	Relatively weak
CPU usage	Relatively low	High	Low
Memory usage	Relatively low	High	Low
Network consumption	Relatively low	High	Low
Encryption speed	Relatively fast	Slow	Fast

4.4 Further Discussion

In the above experiments, we simulate SEM in a small leaf-spine topology, and the experimental results have shown the effectiveness of this method. Here, we will further discuss the applicable scenarios and some potential problems.

As we all know, DCN consists of two crucial components: Intra-DCN and Inter-DCN, and tens of millions of bytes of data are transmitted via it daily. It happens all the time, whether during requests and responses between different users, backup procedures to prevent data loss, or information transmission between data centers [30,31]. Additionally, the transmission requirements of traffic within and between data centers also differ significantly. Therefore, it is crucial to figure out how to meet their transmission needs while ensuring traffic safety. We do not consider DCN as a whole in this paper. Instead, we start with the flow characteristics and transmission requirements, understanding the delicate needs of low-latency, Intra-DCN short flows and the security and high throughput needs of Inter-DCN traffic. We separate it into two pieces and encrypt them with various encryption algorithms. The heterogeneity in DCN and the experimental data findings show that the scheme can satisfy the needs for information transmission in multi-tenant data centers.

Since the flows in DCN is dynamic, and the number of flows is variable. To further verify the applicability of the GIFT encryption method for short flows transmission under different topologies or loads, we take the size of the load as the experimental variable to test whether the GIFT encryption method is still suitable for short flows encryption.

4.4.1 Different Loads

In the experiment, we also use the leaf-spine topology in the design experiment. Meanwhile, we use DCTCP (Data Center TCP) [32] as the congestion control protocol and ECMP (Equal-Cost Multipath Routing) [33] as the load balancing protocol. For the experiment's integrity, we test the ratio of the sum of encryption and decryption time to short flows transmission time under different loads and test the difference in the ratio of encryption and decryption time to the transmission time of different encryption algorithms under a particular load.

Fig. 9 shows that even when the load is increased from 0.3 to 0.7, the ratio of the flows' transmission time to the total time is maintained at almost 90%. The combined time for encryption and decryption makes up less than 10% of the entire time when the load is between 0.3 and 0.4. As can be observed, the GIFT encryption algorithm is still applicable to Intra-DCN short flows regardless of the load size. In other words, adopting the GIFT has no impact on the transmission effectiveness of short flows under various loads. Additionally, the proportions of different encryption techniques in terms of the transmission time of short flows vary. As shown in Fig. 10, when the transmission load is kept at 0.7, the full encryption and decryption time for DES and AES can reach 80%, but the typical transmission time only accounts for less than 20% of the total time. The link will only be partially utilized, wasting resources, and being particularly unfavorable to the transmission of short flows. GIFT is more suitable to short flows in DCN than other encryption algorithms, and its encryption and decryption time only makes up 14% of the overall FCT. It can both guarantee its security and maintain its regular transmission.

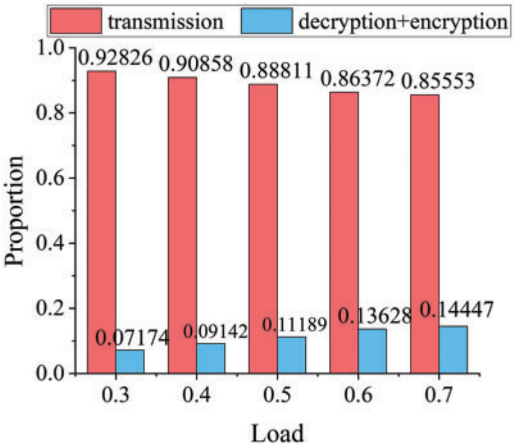

Figure 9: The proportion of encryption and decryption time to flow transmission time using the GIFT encryption algorithm under different loads

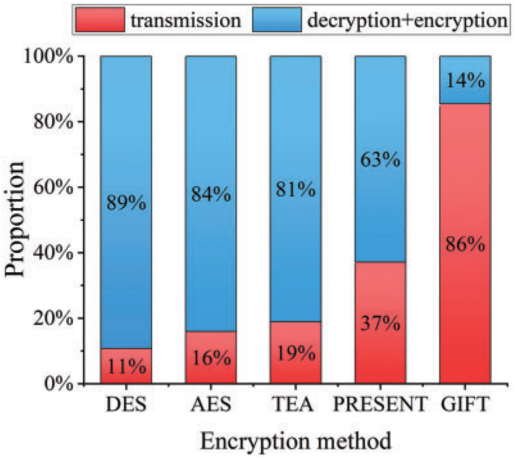

Figure 10: At 0.7 load, the proportion of encryption and decryption time and transmission time processed by different encryption algorithms

4.4.2 Different Topologies

In DCN, topology is the hub of data transmission. Different topology structures will produce different transmission results. Therefore, in order to verify the wide applicability of SEM, we expand the leaf-spine topology used above to 4 times the original under the condition that other parameters remain unchanged. And consistent with the above experimental test, we still test the ratio of the sum of the encryption and decryption time of GIFT to short flows transmission time and the difference in the proportion of the two times between different algorithms.

As demonstrated in Fig. 11, even when the load is lowered to 0.1, the proportion of transmission time is as high as 97%. Even though the topology is stretched by four times, the fraction of short flow transmission corresponding to different loads remains over 85%. Therefore, the GIFT encryption's applicability to Intra-DCN short flows is unaffected by the topology change. Additionally, in line with the previous experiments, DES, AES, and TEA all have excessively long encryption and decryption times. In fact, the fraction of encryption and decryption times exceeds 70% of the overall duration. The FCT will be twice as long as the initial transmission time when the current algorithm is employed for Intra-DCN short flows because, despite its outstanding performance, the encryption and decryption time proportions are nearly equal to the transmission time proportions. Overall, the Intra-DCN short flows cannot be encrypted using traditional DES and AES encryption methods or the cutting-edge TEA and PRESENT techniques. Please see Fig. 12 for more information.

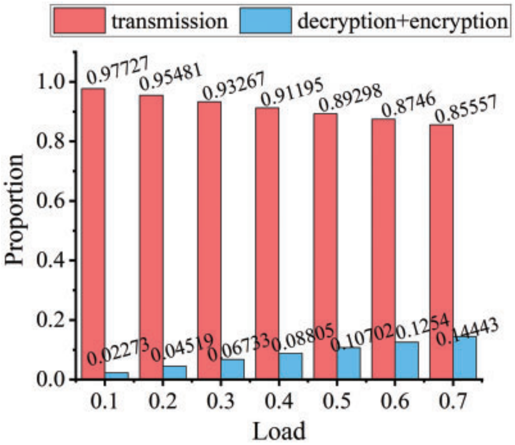

Figure 11: Using the GIFT encryption algorithm, the proportion of encryption and decryption time to flow transmission time under the condition that the topology becomes four times larger and different loads

In conclusion, although topology and load change, the applicability of the GIFT encryption algorithm to Intra-DCN short flows will not be affected. And according to the experimental results, compared with other encryption algorithms, the GIFT encryption algorithm has more advantages in the encryption of Intra-DCN short flows.

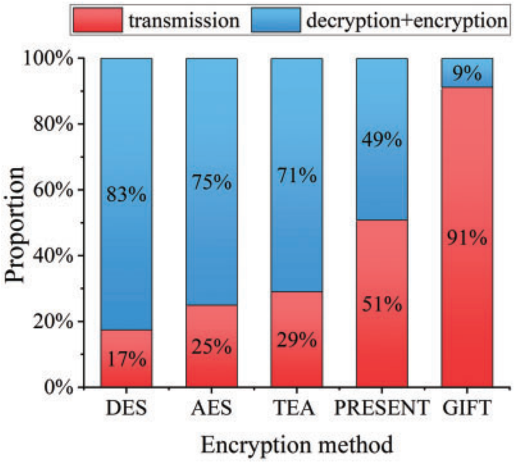

Figure 12: At 0.4 load, the proportion of encryption and decryption time and transmission time processed by different encryption algorithms

5 Related Works

There are many types of research on data centers security under multi-tenancy. In this regard, we only discuss some representative work close to the research in this paper. We can roughly divide those representative works into the following three categories.

(1) **Encryption algorithm.** With the progress of science and technology, tenants have higher and higher requirements for network security and service quality. In this context, many lightweight encryption algorithms have been proposed, mainly to achieve more efficient security performance with less memory and time overhead. Literature [34] proposes a lightweight encryption algorithm Secure IoT (SIT), which aims to reduce the encryption cost of data in secure transmission. The experiment shows that only a few rounds of encryption can achieve excellent security performance. Besides, literature [35] proposes a hybrid lightweight encryption algorithm, and two different encryption algorithms are adopted simultaneously. The asymmetric encryption algorithm is used to improve the security of data transmission, and the symmetric encryption technology is used to ensure the security of private ciphers. The experimental results show that the hybrid lightweight encryption algorithm has low computational overhead and effectively improves the security of data transmission in the network.

(2) **Machine learning.** In recent years, machine learning technology has been widely used to solve various practical problems, such as image recognition and traffic prediction. To protect data transmission security and prevent malicious attacks, literature [36] adopts machine learning to process and analyze the data set of intrusion traffic, and then detects the traffic of malicious attacks according to the deep learning network model. Similarly, literature [37] employs convolution neural network model to identify and classify traffic, and prevents malicious attacks by detecting the traffic transmitted by the network to ensure data communication security. The experimental results show that the accuracy of this model in detecting malicious traffic can reach 99%. Therefore, it can detect malicious attacks more accurately, thus ensuring the security and privacy of the entire network.

(3) **Other technologies.** In addition to the above research work, it also combines with other technologies to strengthen security under the multi-tenant context by the advantages of other technologies. Security issues for multi-tenant access, literature [38] proposes an access control method based on

environmental factors and security labels, which enables tenants to access cloud data more flexibly and finely, and effectively prevents illegal and unauthorized access. Meanwhile, literature [39] proposes implementing blockchain technology in a multi-tenant environment. In the multi-tenant mode, it establishes a private virtual account for each tenant to guarantee their data security and personal privacy. In addition, literature [40] proposes a hybrid encryption algorithm by combining encryption algorithm with evolutionary computation. Moth Swarm Algorithm (MSA), is used to find the optimal elliptic curve value and calculate the optimal cipher of the elliptic curve encryption algorithm ECC, aiming to improve the calculation efficiency and security performance of ECC. According to the experimental results, we can see that the hybrid encryption algorithm has higher security performance, more minor ciphers and less resource consumption than before. The throughput and transmission efficiency of the whole network is improved.

6 Conclusion

Tenant data privacy and transmission security are major concerns in multi-tenant data centers. However, it is challenging to meet the needs of all traffic transmissions with just one security processing approach due to the various data center features and heavy traffic. Consequently, this paper suggests a fine-grained security enhancement method (SEM) for heterogeneous traffic, primarily consisting of two improvements: (i) To handle the secure transmission of short flows in DCN, choose the lightweight encryption method GIFT, which greatly satisfies the demands of short flows with low latency and high response while resolving the issue of the standard technique's lengthy encryption time. (ii) The asymmetric elliptic curve encryption technique ECC, which is used to transmit Intra-DCN long flows and Inter-DCN traffic, has a high-security factor and increases the security of traffic transmission. According to the experimental findings, SEM considerably reduces the FCT of short flows by 70% and significantly enhances the security of traffic transmission in cloud environments. In addition, compared with other encryption technologies, SEM performs better in high-load and large-scale scenarios.

However, SEM still consumes too much computing resources and memory space. Future work will focus on finding ways to use memory and processing resources as sparingly as feasible, for as by considering the hash storage strategy.

Funding Statement: This work is supported by the National Natural Science Foundation of China (62102046, 62072056), the Natural Science Foundation of Hunan Province (2022JJ30618, 2020JJ2029), and the Scientific Research Fund of Hunan Provincial Education Department (22B0300).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] V. Narasayya and S. Chaudhur, "Cloud data services: Workloads, achitectures and multi-tenancy," *Foundations and Trends in Databases*, vol. 10, no. 1, pp. 1–107, 2021.

[2] G. Dessouky, A. -R. Sadeghi and S. Zeitouni, "SoK: Secure FPGA multi-tenancy in the cloud: Challenges and opportunities," in *2021 IEEE European Symp. on Security and Privacy*, Vienna, Austria, pp. 487–506, 2021.

[3] J. Wang, Y. Gao, W. Liu, W. Wu and S. J. Lim, “An asynchronous clustering and mobile data gathering schema based on timer mechanism in wireless sensor networks,” *Computers, Materials & Continua*, vol. 58, no. 3, pp. 711–725, 2019.

[4] J. Kumar, M. Kumar, D. K. Pandey and R. Raj, “Encryption and authentication of data using the IPSEC protocol,” in *Proc. of the Fourth Int. Conf. on Microelectronics, Computing and Communication Systems*, vol. 673, Singapore, Springer, pp. 855–862, 2021.

[5] H. Wang, H. Zheng, B. Hu and H. Tang, “Improved lightweight encryption algorithm based on optimized S-box,” in *2013 Int. Conf. on Computational and Information Sciences*, Shiyang, China, pp. 734–737, 2013.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann *et al.,* “PRESENT: An ultra-lightweight block cipher,” in *Cryptographic Hardware and Embedded Systems—CHES 2007*, vol. 4727, Berlin Heidelberg: Springer, pp. 450–466, 2007.

[7] S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. M. Sim *et al.,* “GIFT: A small present,” in *Cryptographic Hardware and Embedded Systems—CHES 2017*, vol. 10529, Cham: Springer, pp. 321–345, 2017.

[8] D. A. Shafiq, N. Z. Jhanjhi, A. Abdullah and M. A. Alzain, “A load balancing algorithm for the data centers to optimize cloud computing applications,” *IEEE Access*, vol. 9, pp. 41731–41744, 2021.

[9] Z. Awada, K. Boulos, M. El-Helou, K. Khawam and S. Lahoud, “Distributed multi-tenant RAN slicing in 5G networks,” *Wireless Networks*, vol. 28, pp. 3185–3198, 2022.

[10] J. Hu, J. Huang, W. Lv, Y. Zhou, J. Wang *et al.,* “CAPS: Coding-based adaptive packet spraying to reduce flow completion time in datacenter,” *IEEE/ACM Transactions on Networking*, vol. 27, no. 6, pp. 2338–2353, 2019.

[11] A. Pekar, J. Mocnej, W. K. G. Seah and I. Zolotova, “Application domain-based overview of IoT network traffic characteristics,” *ACM Computing Surveys*, vol. 53, no. 87, pp. 1–33, 2021.

[12] J. Wang, C. Jin, Q. Tang, N. N. Xiong and G. Srivastava, “Intelligent ubiquitous network accessibility for wireless-powered MEC in UAV-assisted B5G,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2801–2813, 2021.

[13] J. Hu, J. Huang, Z. Li, Y. Li, W. Jiang *et al.,* “RPO: Receiver-driven transport protocol using opportunistic transmission in data center,” in *2021 IEEE 29th Int. Conf. on Network Protocols (ICNP)*, Dallas, TX, USA, pp. 1–11, 2021.

[14] C. A. Lara-Nino, A. Diaz-Perez and M. Morales-Sandoval, “Lightweight elliptic curve cryptography accelerator for internet of things applications,” *Ad Hoc Networks*, vol. 103, pp. 102159, 2020.

[15] R. Nazir, A. A. laghari, K. Kumar, S. David and M. Ali, “Survey on wireless network security,” *Archives of Computational Methods in Engineering*, vol. 29, no. 3, pp. 1591–1610, 2022.

[16] M. K. Hasan, S. Islam, R. Sulaiman, S. Khan, A. A. Hashim *et al.,* “Lightweight encryption technique to enhance medical image security on internet of medical things applications,” *IEEE Access*, vol. 9, pp. 47731–47742, 2021.

[17] K. Tamilarasi and A. Jawahar, “Medical data security for healthcare applications using hybrid lightweight encryption and swarm optimization algorithm,” *Wireless Personal Communications*, vol. 114, pp. 1865–1886, 2020.

[18] J. Wang, H. Han, H. Li, S. He, P. Kumar Sharma *et al.,* “Multiple strategies differential privacy on sparse tensor factorization for network traffic analysis in 5G,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1939–1948, 2022.

[19] P. Sun, “Security and privacy protection in cloud computing: Discussions and challenges,” *Journal of Network and Computer Applications*, vol. 160, pp. 102642, 2020.

[20] D. A. Osvik, A. Shamir and E. Tromer, “Cache attacks and countermeasures: The case of AES,” in *Cryptographers’ Track at the RSA Conf. CT-RSA 2006: Topics in Cryptology*, vol. 3860, Berlin, Heidelberg: Springer, pp. 1–20, 2006.

[21] N. T. Raja and K. M. Singh, “Secure and efficient text encryption using elliptic curve cryptography,” *Evolution in Computational Intelligence*, vol. 267, pp. 521–529, 2022.

[22] F. M. Cardoso, C. Gracia-Lázaro, F. Moisan, S. Goyal, Á. Sánchez *et al.,* “Effect of network topology and node centrality on trading,” *Sci. Rep.*, vol. 10, no. 1, pp. 11113, 2020.

[23] P. Yu, Y. Shi, L. Wang, S. Ke and M. Yin, *A Method for Optimizing Communication Network Topology Based on Genetic Algorithm*. vol. 307, Singapore: Springer Nature Singapore, pp. 30–40, 2021.

[24] O. N. Akande, O. C. Abikoye, A. A. Kayode, O. T. Aro and O. R. Ogundokun, "A dynamic round triple data encryption standard cryptographic technique for data security," vol. 12254, Cham: Springer International Publishing, pp. 487–499, 2020.

[25] C. Cid, S. Murphy and M. J. B. Robshaw, "Small scale variants of the AES," vol. 3557, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 145–162, 2005.

[26] D. J. Wheeler and R. M. Needham, "TEA, a tiny encryption algorithm," in *Fast Software Encryption. LNCS*, vol. 1008, Heidelberg: Springer, pp. 363–366, 1995.

[27] L. Chen, K. Chen, W. Bai and M. Alizadeh, "Scheduling mix-flows in commodity datacenters with karuna," in *Proc. ACM SIGCOMM, Association for Computing Machinery*, New York, NY, USA, pp. 174–187, 2016.

[28] T. Benson, A. Akella and D. A. Maltz, "Network traffic characteristics of data centers in the wild," in *Proc. IMC*, New York, NY, USA, pp. 267–280, 2010.

[29] Ç. K. Koç, F. Özdemir and Z. Ö. Özger, "Rivest-shamir-adleman algorithm," in *Partially Homomorphic Encryption*, Cham: Springer, pp. 37–61, 2021.

[30] J. Hu, J. Huang, W. Lv, W. Li, Z. Li *et al.,* "Adjusting switching granularity of load balancing for heterogeneous datacenter traffic," *IEEE/ACM Transactions on Networking*, vol. 29, no. 5, pp. 2367–2384, 2021.

[31] J. Liu, J. Huang, W. Lv and J. Wang, "APS: Adaptive packet spraying to isolate mix-flows in datacenter network," *IEEE Transactions on Cloud Computing*, vol. 10, no. 2, pp. 1038–1051, 2022.

[32] D. Liu, G. Chuai and W. Gao, "Dynamic adaptive marking strategy based on DCTCP in datacenter networks," in *2022 IEEE 2nd Int. Conf. on Power, Electronics and Computer Applications (ICPECA)*, Shenyang, China, pp. 387–392, 2022.

[33] L. Hiryanto, S. Soh, K. -W. Chin, D. -S. Pham and M. Lazarescu, "Green multi-stage upgrade for bundled-links SDN/OSPF-ECMP networks," in *ICC 2021-IEEE Int. Conf. on Communications*, Montreal, QC, Canada, pp. 1–7, 2021.

[34] M. Usman, I. Ahmed, M. I. Aslam, S. Khan and U. A. Shah, "SIT: A lightweight encryption algorithm for secure internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 1, 2017.

[35] M. A. Habib, M. Ahmad, S. Jabbar, S. H. Ahmed and J. J. P. C. Rodrigues, "Speeding up the internet of things: LEAIoT: A lightweight encryption algorithm toward low-latency communication for the internet of things," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 31–37, 2018.

[36] R. Abdulhammed, M. Faezipour, A. Abuzneid and A. AbuMallouh, "Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic," *IEEE Sensors Letters*, vol. 3, no. 1, pp. 1–4, 2019.

[37] B. Tang, W. Jiang and Y. Ke, "Research on CNN-based malicious traffic identification method," in *2021 7th Int. Conf. on Computing and Artificial Intelligence (ICCAI 2021)*, New York, NY, USA, Association for Computing Machinery, pp. 257–265, 2021.

[38] Y. Duan, X. Deng and H. Yang, "A multi-tenant access control method based on environmental attributes and security labels," in *2021 3rd Int. Conf. on Information Technology and Computer Communications (ITCC 2021)*, New York, NY, USA, Association for Computing Machinery, pp. 41–46, 2021.

[39] E. A. Adeniyi, R. O. Ogundokun, S. Misra, J. B. Awotunde and K. M. Abiodun, "Enhanced security and privacy issue in multi-tenant environment of green computing using blockchain technology," in *Blockchain Applications in the Smart Era*, Hong Kong, China: EAI/Springer Innovations in Communication and Computing, pp. 65–83, 2022.

[40] P. Kumar and A. K. Bhatt, "Enhancing multi-tenancy security in the cloud computing using hybrid ECC-based data encryption approach," *IET Communications*, vol. 14, no. 18, pp. 3212–3222, 2020.