SECURITY-AWARE UNIVERSITY RESOURCE ALLOCATION: ECC-BASED VERIFICATION FOR DYNAMIC COORDINATION

Xiaomin ZHAO [1,*]

The allocation of educational resources in higher education institutions faces challenges related to execution efficiency, coordination stability, and data security under dynamic demands and multi-stakeholder participation. This study proposes a security-aware dynamic allocation framework for university educational resources, focusing on secure verification and execution coordination rather than introducing new optimization algorithms. Elliptic curve cryptography (ECC) is employed as a lightweight cryptographic infrastructure to support secure data exchange and allocation confirmation, thereby reducing coordination overhead and execution interruptions in multi-party collaboration. A dynamic adjustment mechanism is further integrated to enable stable resource allocation under verifiable security conditions. Experimental evaluations based on historical data from a university indicate that the proposed framework achieves a resource allocation success rate of 97.2% in laboratory scenarios, compared with 82.5% for traditional static allocation schemes. Under the defined threat assumptions, no data leakage events are observed. Efficiency improvements are mainly reflected at the system execution level through reduced coordination delays and verification failures, enhancing the robustness and engineering feasibility of dynamic university resource management.

Keywords: University educational resource allocation; Elliptic Curve Cryptography; Secure coordination mechanism; Dynamic allocation framework; Multi-party resource management

1. Introduction

With the rapid development of educational informatization, the allocation of university educational resources such as laboratories, libraries, and teaching spaces has become a crucial issue due to high demand and dynamic usage patterns [1]. Traditional allocation models often adopt static and centralized approaches, lacking responsiveness to changing needs and often failing in fairness and transparency [2]. Under resource constraints, intensified interdepartmental competition and frequent incidents of data leakage and tampering highlight the need for secure and efficient allocation models.

[1] * "Xi'an Mingde" Institute of Technology, Xi'an 710124, Shaanxi, China, corresponding author, E-mail: 13919495851@163.com

Elliptic Curve Cryptography (ECC) is recognized for its high security and computational efficiency with shorter key lengths. In the context of multi-party educational resource allocation, ECC can ensure data confidentiality and enable secure verification mechanisms. While blockchain and intelligent algorithms have been explored in this domain, the integration of data security with dynamic adaptability remains limited.

This study proposes a security-aware dynamic framework for the allocation of university educational resources, with a primary emphasis on system-level coordination rather than algorithmic optimization. Instead, ECC serves as a lightweight cryptographic infrastructure that supports secure data exchange, result verification, and reliable multi-party coordination throughout the allocation process.

Existing ECC-based studies primarily focus on data transmission security, while blockchain-based allocation frameworks rely on consensus mechanisms with substantial coordination overhead. It explicitly models security verification costs and coordination latency as integral components of system-level execution efficiency. ECC-based verification is embedded into critical operational stages, such as demand submission, allocation confirmation, and dynamic adjustment. This enables stable and responsive resource allocation under fluctuating demand without altering the computational structure of conventional allocation models.

2. Literature Review

Over the years, educational resource allocation has received growing academic attention, with studies such as Yuan identifying unequal distribution in Chinese universities due to asymmetry in supply and demand information [3]. Varalakshmi and Dhanasekaran found significant satisfaction differences across departments, linked to the limitations of static allocation models [4].

Recent empirical studies using Data Envelopment Analysis (DEA) have shown that low coordination efficiency constrains effective utilization of higher education resources [5, 6]. Moreover, rigid resource allocation structures have been shown to diminish adaptability under conditions of dynamic demand [7]. Zhang et al. introduced smart contracts to enhance transparency, but high computational overhead limited scalability [8].

Kavin and Ganapathy proposed a lightweight ECC method to reduce encryption overhead in distributed systems, demonstrating ECC's potential for secure resource allocation [9]. Beyond data protection, recent research on ECC has increasingly focused on lightweight verification and authentication mechanisms suitable for dynamic and resource-constrained environments. Li and Hu (2024) proposed an ECC-based dynamic credential authentication and key agreement protocol, demonstrating how verification overhead can be controlled under realistic

threat models [10]. Baccouri et al. (2024) developed a lightweight ECC-based authentication scheme that explicitly accounted for execution costs and verification latency, providing evidence that ECC can support secure coordination without excessive system overhead [11].

Most existing studies have focused on optimization-based resource allocation or cryptographic security mechanisms. Few studies, however, have explicitly modeled the security-related coordination overhead inherent in dynamic resource allocation processes. Table 1 summarizes the primary distinctions between representative studies and the framework proposed in this work.

Table 1

Comparison between representative studies and this work

Study	Allocation Core	Security Mechanism	Dynamic Allocation	Coordination Overhead Modeled	Application Data
Varalakshmi & Dhanasekaran [4]	Resource allocation	ECC-based security	✓	✗	Simulation
Zhang et al. [8]	Blockchain-based	Smart contracts	✓	High (consensus)	Simulation
Kavin & Ganapathy [9]	-	ECC signatures	✗	✗	Synthetic
This study	Traditional allocation	ECC verification layer	✓	✓ (verification & latency)	Real data

3. Research Methods of the University Educational Resource Allocation Model and Efficiency Improvement

3.1 Analysis of the applicability of ECC in the educational resource allocation

The ECC algorithm attracts widespread attention due to its high security strength and low computational overhead, making it suitable for scenarios involving frequent data interaction and limited computing resources. In this study, ECC is not introduced as an optimization algorithm for educational resource allocation, but as an underlying cryptographic infrastructure. It supports secure data transmission, reliable result verification, and trusted multi-party collaboration throughout the allocation process.

In this context, ECC is employed to protect sensitive allocation-related information and to enable lightweight verification among participating entities, supporting secure multi-party coordination without altering the underlying allocation logic.

3.2 Construction of the university educational resource allocation model

To support multi-stakeholder resource allocation, a hierarchical framework is adopted, with a traditional allocation model at the upper layer and ECC providing security and coordination support at the lower layer.

Let the resource set be denoted as $R=\{r_1,r_2,\ldots,r_n\}$, where r_j represents the j-th type of educational resource; the user set is denoted as $u=\{u_1,u_2,\ldots,u_m\}$. User demand for resources is represented by the demand matrix $D\in\square^{m\times n}$, where d_{ij} denotes the relative demand weight of user u_i for resource r_j.

To ensure the authenticity and confidentiality of demand data in a multi-party environment, the demand matrix is protected by an ECC-based encryption mechanism before entering the allocation calculation, with its encrypted form expressed as: $C_{ij}=E_k(d_{ij})$. Here, E represents the ECC encryption function, and k is the public key. After the allocation is completed, authorized participants can recover the demand data through decryption: $d_{ij}=D_k(C_{ij})$. This process ensures that the input data on which the allocation model is based is not tampered with but does not alter the allocation calculation itself.

The resource allocation result is represented by the allocation matrix $A\in\square^{m\times n}$, where A_{ij} denotes the quantity of resource r_j allocated to user u_i. To evaluate allocation fairness, a fairness index F is introduced as follows:

1. $$F = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}|d_{ij}-a_{ij}|}{\sum_{i=1}^{m}\sum_{j=1}^{n}d_{ij}} \quad (1)$$

It indicates that this fairness evaluation process is irrelevant to ECC.

To reflect practical allocation priorities, a resource weight calculation is defined. Assuming that the total amount of each resource is Q_j and the priority weight of the ith user is P_i, the user allocation weight W_i is as follows:

2. $$W_i = \frac{P_i}{\sum_{k=1}^{m}P_k} \quad (2)$$

The specific allocation is given in Eq. (3):

3. $$A_{ij} = W_i \cdot \frac{d_{ij}}{\sum_{k=1}^{m}d_{kj}} \cdot Q_j \quad (3)$$

Resource allocation is disturbed by external influences such as demand fluctuations and emergencies. The model modifies the resource requirement by introducing the perturbation factor $\delta_{ij}(t)$, as denoted in Eq. (4):

4. $$D'_{ij}(t) = D_{ij}(t) + \delta_{ij}(t) \quad (4)$$

$\delta_{ij}(t)$represents additional demand due to sudden changes in demand or reallocation of resources. The model dynamically optimizes the allocation scheme by adjusting the calculation rules of $\delta_{ij}(t)$ to make it still robust under emergencies.

To explicitly capture the impact of security mechanisms on allocation execution, the system-level execution time is defined as follows:

$$T_{\text{sys}} = T_{\text{alloc}} + T_{\text{ver}} + T_{\text{comm}} \tag{5}$$

Here, T_{alloc} denotes the time consumed by the resource allocation computation, T_{ver} represents the time required for ECC-based verification, and T_{comm} corresponds to the communication overhead incurred during data exchange.

Within this framework, ECC does not alter the resource allocation computation time (T_{alloc}). However, it directly affects the verification time (T_{ver}) and indirectly influences the frequency of reallocations under dynamically changing demand. By employing batch verification and incremental update strategies, verification overhead is constrained, thereby reducing unnecessary repetitions of the allocation process. Consequently, encryption functions as a system-level constraint that impacts coordination latency and execution efficiency.

3.3 Model solution process and system-level operation optimization

The model pursues two objectives: system-level allocation efficiency and fairness. The optimization goal is to maximize the overall allocation efficiency E, as represented in Eq. (6):

$$maxE = \frac{1}{T}\sum_{i=1}^{m} \sum_{j=1}^{n} A_{ij} \tag{6}$$

T is the total allocation time; A_{ij} indicates the actual allocation amount of the jth resources by user i.

In the guarantee of fairness in allocation, the allocation result needs to meet the fairness index $F \leq F_0$, which is in the specific form of Eq. (7):

$$F = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} |d_{ij} - a_{ij}|}{\sum_{i=1}^{m} \sum_{j=1}^{n} d_{ij}} \leq F_0 \tag{7}$$

F_0 refers to the fairness tolerance threshold.

At the same time, the model is subject to the following constraints. Total resource constraint: The allocation of each resource cannot exceed its total available amount Q_j, $\sum_{i=1}^{m} A_{ij} \leq Q_j, \forall j$. User demand constraint: The allocation amount cannot exceed the user demands: $A_{ij} \leq d_{ij}, \forall i, j$.

The encryption performance of ECC affects security verification and data transmission overhead, thereby influencing the system-level execution efficiency of the allocation process [13]. Optimized point multiplication and precomputation are adopted to limit cryptographic overhead. Let the elliptic curve be $E: y^2 = x^3 + ax + b \bmod p$, and the user demand data d_{ij} is transformed into the point $P(d_{ij})$ on the curve, and the encryption process can be written as Eq. (8):

$$C_{ij} = kP(d_{ij}) \tag{8}$$

k represents the randomly generated private key.

To optimize performance, common points on the curve are precomputed and stored. To reduce system-level execution overhead during the resource allocation process, the following optimization strategies are introduced. In distributed environments, allocation tasks are decomposed for parallel execution to improve efficiency. According to the real-time demand changes, the allocation weight W_i and the allocation amount A_{ij} can be dynamically adjusted, as follows:

9. $$W_i(t) = \frac{P_i(t)}{\sum_{k=1}^{m} P_k(t)}, A_{ij}(t) = W_i(t) \cdot Q_j \quad (9)$$

In high-frequency resource allocation scenarios, caching mechanisms are employed to store encrypted intermediate results, reducing redundant calculations.

The primary complexity of ECC comes from the encryption and decryption processes. Encryption complexity: $O(\log n)$, significantly reducing computation time by utilizing fast point multiplication. Allocate computational complexity: $O(m \cdot n)$, where m and n refer to the number of users and resources, respectively. After distributed optimization, the complexity is approximately reduced to $O((m \cdot n)/p)$, where p is the number of parallel processing units.

3.4 Design of experiment

Historical allocation data from a university resource management system, including library, laboratory, and course records, are used for offline evaluation to reflect real operational scenarios.

In the experiment, key model parameters include the total available resources $Q = \{Q_1, Q_2, \ldots, Q_n\}$ and user priority weights $P = \{P_1, P_2, \ldots, P_m\}$, which are determined based on historical allocation statistics to reflect realistic resource scales and priority differences.

For the security layer, ECC is implemented using the curve $y^2 = x^3 + ax + b \pmod p$ where p is a prime number and the parameters satisfy $4a^3 + 27b^2 \neq 0$. A 256-bit key length is adopted to balance security and computational overhead under practical deployment conditions. Public keys are centrally distributed by the allocation management unit. Historical allocation data from a university resource management system, including library, laboratory, and course records, are used for offline evaluation to reflect real operational scenarios.

The model's applicability is evaluated in experimental scenarios ranging from small-scale (50 users, 5 resources) to large-scale (500 users, 25 resources) with varying demand intensity.

To comprehensively assess the model's performance, this study employs three categories of indices: security, allocation efficiency, and resource utilization. Security is mainly evaluated based on the confidentiality, integrity, and anti-attack capabilities of the allocation data. Specific indices introduced in the experiment

include data leakage rate, encryption verification time, and data tampering rate. Security evaluation focuses on minimizing leakage and tampering while controlling verification overhead. The allocation efficiency index measures the model's ability to complete resource allocation within a unit of time, covering allocation time and allocation completion rate.

The resource utilization index measures the matching degree between the actual use of resources and the total amount, as expressed in Eq. (10):

10. $$U_j = \frac{\sum_{i=1}^{m} A_{ij}}{Q_j}, U_j \in [0,1] \tag{10}$$

The average resource utilization rate represents the overall resource utilization efficiency, as indicated in Eq. (11):

11. $$U_{avg} = \frac{1}{n}\sum_{j=1}^{n} U_j \tag{11}$$

The resource vacancy rate represents the proportion of unallocated resources to the total amount of resources: I_j=1-U_j.

All evaluation metrics are derived from repeated experiments conducted under predefined experimental assumptions. The allocation success rate is defined as the ratio of successfully fulfilled allocation requests after adjustment to the total number of requests. The fairness index is calculated using Equation (6) under identical demand conditions across different methods.

The data leakage rate is assessed by monitoring unauthorized access and integrity violations during data transmission and storage under predefined threat assumptions. A reported leakage rate of 0% indicates that no data breaches or tampering incidents were observed during the experiments; however, this does not imply absolute or unconditional security.

To ensure rigor and transparency in the security evaluation, this study defines a threat model that explicitly delineates the scope of the security assumptions considered. The adversary is assumed to perform passive eavesdropping, active tampering, replay attacks, and limited unauthorized access, while denial-of-service attacks and full system compromise are excluded.

Based on this threat model, a data leakage event is defined as any successful unauthorized access to plaintext allocation data during transmission or storage. A tampering event is defined as a failure in integrity verification caused by message modification or replay. The measurement of security metrics involves monitoring system logs, counting the number of integrity check failures, and recording replay attempts that were blocked during the experimental runs. Under the defined threat model, no leakage or tampering events were observed, which does not imply absolute security.

4. Result Analysis of the University Educational Resource Allocation Model and Efficiency Improvement

4.1 Verification result of models

To verify the practical effectiveness of the proposed framework, experimental evaluations are conducted and compared with alternative allocation methods. In typical scenarios, such as laboratory resource allocation, the configurations for different numbers of users and types of resources are summarized, and the results are presented in Fig. 1. Data leakage rate is evaluated under predefined experimental threat assumptions.

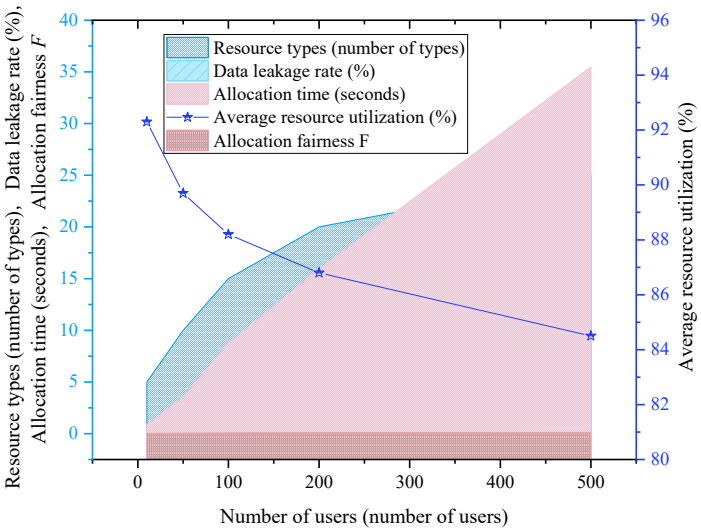

Fig. 1. Experimental results of model performance under typical scenarios

As shown in Fig. 1, no data leakage is observed under the defined experimental conditions. The allocation time increases approximately linearly with the growth of user quantity and resource types, but remains within an acceptable range in large-scale scenarios. The average resource utilization rate is between 84% and 92%. The allocation fairness index, F, remains below 0.12, indicating that the allocation results meet fairness requirements well.

To further test the system-level performance of the proposed framework, it is compared with the following four benchmark allocation methods. Four benchmark methods are considered for comparison: Static Allocation (SA), Centralized Linear Programming (CLP), Genetic Algorithm-based allocation (GA), and Blockchain-based allocation (BA). In Fig. 2(a), under the experimental assumptions, the ECC-supported framework shows no data leakage.

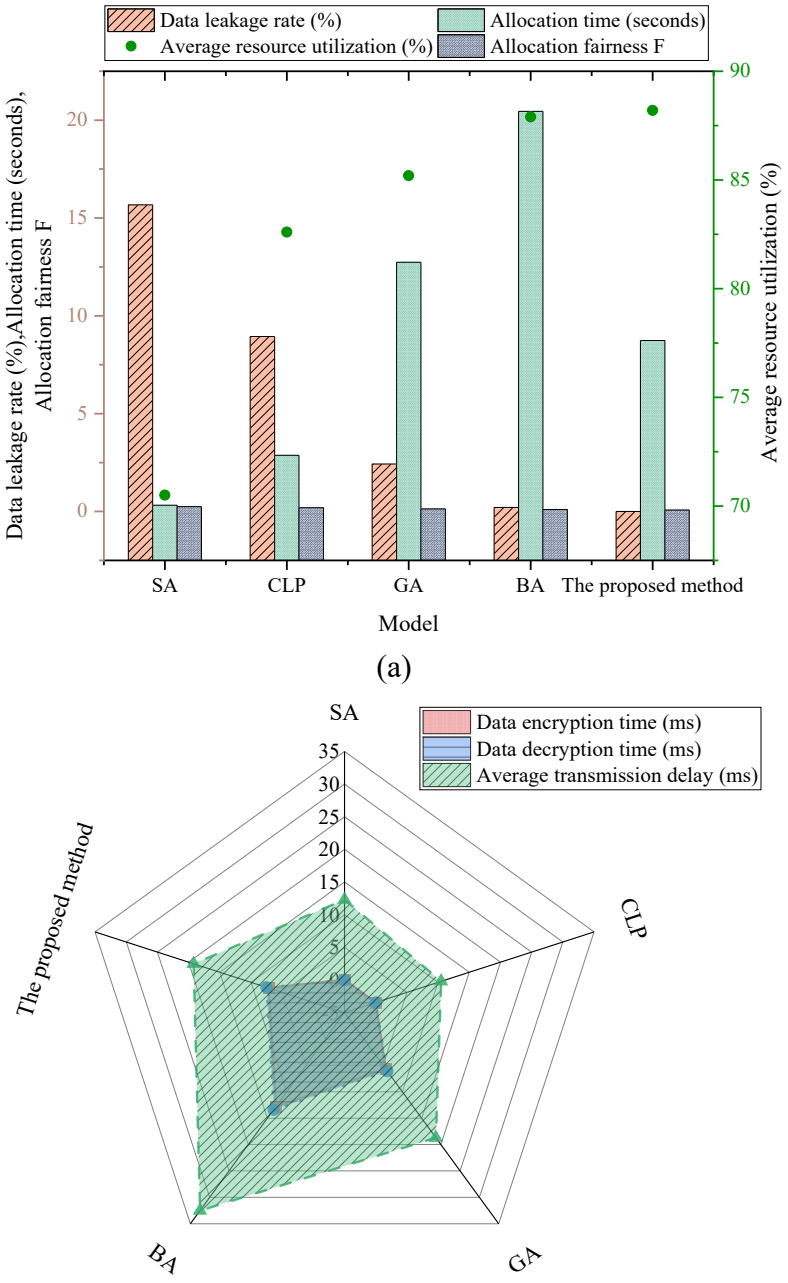

Fig. 2. System-level performance comparison with communication and verification overheads (a) System-level performance comparison; (b) Communication and verification overhead comparison

In Fig. 2(a), under the experimental assumptions, the ECC-supported framework shows no data leakage. In terms of allocation time, the proposed

framework achieves shorter execution time than GA-based and BA-based methods under secure conditions, while maintaining performance comparable to CLP-based methods. Although the BA model shows slightly higher resource utilization (87.9%) in some cases, the proposed framework maintains a relatively high utilization level (88.2%) while providing additional security guarantees. In terms of allocation fairness, the proposed framework achieves a lower fairness index (F=0.07) compared with other methods, indicating that the allocation results are more balanced under secure coordination. These improvements are not due to optimization by ECC, but to enhanced execution stability enabled by secure coordination. Secure and verifiable coordination reduces conflicts, verification failures, and rollbacks under dynamic demand, leading to more consistent execution and higher utilization.

In Fig. 2(b), the average encryption and decryption time of the proposed framework is 7.4 ms, which is lower than that of the BA-based method and comparable to that of the GA-based method. Through optimized encryption operations and lightweight key design, the proposed framework limits the additional communication latency to 19.2 ms, indicating that security mechanisms can be integrated without introducing excessive system-level transmission overhead.

4.2 Robustness of the model

The following experiment is designed to verify the stability of the model under demand fluctuations. Demand fluctuation frequencies are set to 5, 10, and 20 adjustments per hour. The model's allocation success rate and fairness index *F* are recorded. The experimental results are demonstrated in Fig. 3.

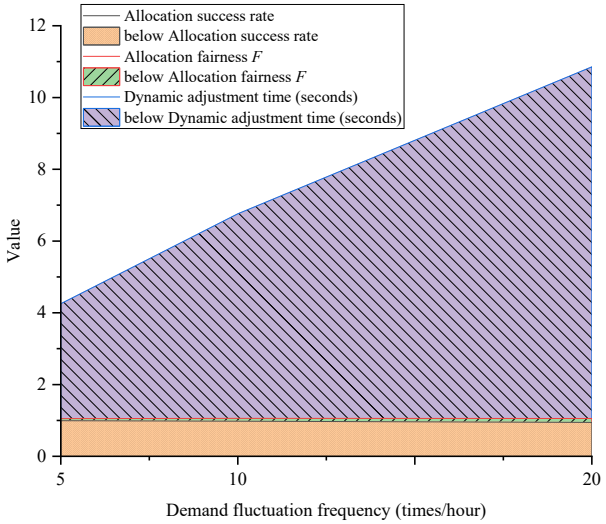

Fig. 3. Results of allocation stability under different demand fluctuation frequencies

In Fig. 3, the allocation success rate represents the percentage of the model that satisfies the user's needs after demand adjustments. Under high-frequency demand fluctuations (20 times/hour), the allocation success rate remains at 94.3%, indicating that the model can effectively adapt to frequent dynamic adjustments. The secure verification and incremental update mechanisms limit unnecessary reallocations caused by inconsistent or unverified demand updates, thereby enabling the system to operate stably under varying load conditions. Scalability results are based on offline evaluations using a single university dataset and should be interpreted as controlled evidence rather than generalizable guarantees. Future work will involve further validation using datasets from multiple universities or in online deployment scenarios.

5. Conclusion

This study develops a systematic solution integrating lightweight cryptographic mechanisms into educational resource allocation. By explicitly defining the role boundaries and implementation approach of encryption, the study clarifies how security mechanisms support dynamic, multi-party resource management without interfering with allocation computations. The study offers a novel reference for balancing security, scalability, and engineering feasibility in university resource management systems. However, the current evaluation is based solely on offline data from a single institution; future work will focus on extending the framework to multi-institutional settings and online deployment scenarios.

REFERENCES

[1] Ren, Z. (2023). Optimization of Innovative Education Resource Allocation in Colleges and Universities Based on Cloud Computing and User Privacy Security. Wireless Personal Communications, 2023, 1-15.

[2] Dai, B., & An, X. (2023). Higher educational information resource sharing model based on blockchain. International Journal of Emerging Technologies in Learning (Online), 18(7), 72.

[3] Yuan, L. (2022). Construction of a multimedia education resource security model based on multistage integration. Mathematical Problems in Engineering, 2022(1), 3624360.

[4] Varalakshmi, J., & Dhanasekaran, S. (2024). A dual hashing-based authentication and secure data transmission scheme for vehicular cloud environment using MECC with optimal resource allocation mechanism. Soft Computing, 2024, 1-15.

[5] Chen, B., Chen, Y., Sun, Y., Tong, Y., & Liu, L. (2024). The measurement, level, and influence of resource allocation efficiency in universities: empirical evidence from 13 “double first class” universities in China. Humanities and Social Sciences Communications, 11(1), 1-16.

[6] Ye, Z., Khanal, R., & Cao, Z. (2025). Studying on the efficiency of higher education resource allocation and its influencing factors in the western China using DEA-Malmquist and Tobit models. PLoS One, 20(10), e0334090.

[7] Zhong, Q. A. (2025). Allocation Efficiency of Higher Education Resources in China: A Three-Stage DEA Model-Based Calculation. Frontiers in Economics and Management, 6(8), 51-67.

[8] Zhang, L., Zou, Y., Wang, W., Jin, Z., Su, Y., & Chen, H. (2021). Resource allocation and trust computing for blockchain-enabled edge computing system. Computers & Security, 105, 102249.
[9] Kavin, B. P., & Ganapathy, S. (2021). A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves. Int. Arab J. Inf. Technol., 18(2), 180-190.
[10] Li, M., & Hu, S. (2024). A lightweight ECC-based authentication and key agreement protocol for IoT with dynamic authentication credentials. Sensors, 24(24), 7967.
[11] Baccouri, S., Farhat, H., Azzabi, T., & Attia, R. (2024). Lightweight authentication scheme based on elliptic curve el gamal. Journal of Information and Telecommunication, 8(2), 231-261.
[12] Asamoah, K. O., Darko, A. P., Antwi, C. O., Sey, C., Osei, A. H., Ma, X., & Zhu, J. (2024). A probabilistic reliable linguistic model for blockchain-based student information management system assessment. Applied Soft Computing, 159, 111645.