Security Mechanism Of Information Resource Management In Computer Network Environment

Huifang Xiong[1,2] and Zhiming Huang[3*]

[1] School of Information Engineering, Jiangxi Vocational and Technical College of Communications, Nanchang 330013, Jiangxi, China
[2] Key Laboratory of Traffic Incident Intelligent Monitoring of Jiangxi Education Institutes, Nanchang 330013, Jiangxi, China
[3] School of Design and Art, Jiangxi University of Finance and Economics, Nanchang 330013, Jiangxi, China
[*] Corresponding author. E-mail: hzhiming501@163.com

Received Aug. 24, 2026; accepted Sep. 26, 2026

Research on management of information resources in network conditions reveals important issues. One of the main problems is the risk of possible data leakage or alteration during transmission. Besides, basic authentication methods offer low protection. To eliminate the above difficulties, the author suggests a secure enhanced management system and suggests that ECC-AES hybrid encryption technology be adopted. In the ECC-AES encryption strategy, Elliptic Curve Cryptography is utilized to obtain public keys for quick key generation with ECC while Advanced Encryption Standard is used for high-speed symmetric encryption and thus ensures data safety both during transmission and storage. Experimental results demonstrate that, when encrypting 10 MB of data, this algorithm achieves a data leakage rate of 2.24% with an encryption time of 176 ms. This mechanism effectively mitigates common network threats and provides a reliable security safeguard for information resource management.

Keywords: Computer Network Environment, Information Resource Management, Security Mechanism, Elliptic Curve Cryptography, Advanced Encryption Standard, Hybrid Encryption

© The Author('s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are cited.

http://dx.doi.org/10.6180/jase.202701_36.042

1. Introduction

The advancement of technologies in the field of information spread has made computer networks an effective and helpful tool for distributing and sharing information, but has also made information resources management vulnerable to severe security threats. Cases of data leakage, data tampering and unauthorized access are increasingly apparent in all fields. Traditional management practices are not able to tackle modern threats due to outdated technology and limited functionality [1]. This paper presents an analysis of the current widely-used technologies aimed at ensuring information resources safety with the help of advanced encryption approaches and improved multi-authentication techniques.

The combination of ECC and AES has created a hybrid encryption system, where ECC is used for proper key generation and distribution while AES is used for quick symmetrical data encryption. In addition, it also entails Huffman coding, which is a method for compression and data transmission efficiency improvement. Furthermore, this paper proposes a dynamic role-based access control policy based on trust values and a two-step multi-factor authentication mechanism to mitigate the risks of privilege abuse and identity spoofing. The core objectives of this approach are confidentiality and integrity, with availability as the secondary objective and access controllability as a supporting objective; ECC-AES ensures confidentiality and integrity, MFA and RBAC guarantee access controllability, and redundancy and compression strategies are employed

to balance availability.

2. Related work

The information resource management security mechanism safeguards information against tampering and leakage across its collection, processing and storage lifecycle.Zhang Peiying proposed a virtual network embedding algorithm with computing, storage and security constraints to ensure secure and rational resource allocation in ICPSs [2]. Hashemi Soheil analyzed IoT architecture from the subject abstraction layer, systematically sorting out security vulnerabilities and prerequisites in IoT resource management amid rising user privacy risks [3].

In computer network environments, information encryption and authentication form the core of information security mechanisms, jointly protecting information resources throughout transmission, storage and usage. Chen Longbing focused on the practical application of digital encryption technology in computer network information security [4]. Guangxu Yu proposed a machine learning-based feature selection method to address the insufficient protection capability of traditional network security technologies amid rapid Internet development [5].

3. Materials and methods

3.1. Encryption Algorithm Selection and Implementation

In the computer network environment, the security of information resource management has received increasing attention. Faced with ever-evolving cyber attacks, ensuring the confidentiality of information during data transmission and storage has become a core challenge in current information resource management. Encryption technologies can actively protect the security of information resources [6]. System security and performance must be considered when selecting an encryption algorithm. This paper constructs a hybrid encryption method that combines ECC and AES.

This work selects Huffman coding as the compression scheme. It statistically analyzes the occurrence frequency of each symbol in information resources, assigns shorter codes to high-frequency symbols to reduce overall coded data length [7]. Huffman encoding performs lossless compression on the plaintext before encryption, which reduces the data volume and improves the efficiency of ECC-AES; however, it may alter the statistical distribution and introduce length-side-channel risks. Therefore, fixed-length block padding is employed to mitigate the risks associated with length leakage and bypass analysis.The approach effectively reduces the data volume to be encrypted, further improves the operating efficiency of the ECC-AES hybrid encryption algorithm, and notably enhances the real-time performance of information transmission.

$$QD = Q_1 * D_1 + Q_2 * D_2 + \cdots + Q_m * D_m \tag{1}$$

Q represents the weight parameter of each information node in the Huffman tree. D represents the distance parameter between each information node.

For data encryption, the ECC-AES hybrid algorithm uses ECC to generate an efficient key pair, then performs AES symmetric encryption on fixed-size plaintext blocks through multiple rounds of operations to output ciphertext. Compared with standalone AES, it delivers more secure and flexible key distribution, effectively resisting data theft, tampering and forgery, and notably enhances the security and reliability of network information resource management:

$$E_{ij} = x_c + X_{IJ}^I \tag{2}$$

x_c represents the split data point, and X_{IJ}^I represents the time window length.The ECC private key is stored in a TEE or HSM; session keys are updated periodically and distributed via a secure channel; upon user logout or in the event of a key compromise, the old key is immediately revoked and destroyed, thereby enabling comprehensive key lifecycle management.

3.2. Access Control Strategy Design

This paper applies the trust value as an essential reference for adjusting role levels to continuously improve the security of information resource management in a dynamically changing computer network environment. According to the user's trust value, his position in the role tree is flexibly adjusted, and his role level changes. The role level ranges from 1 to n, representing different permission levels from the lowest to the highest. When a user shows a larger trust value, their level of role is increased, leading to additional privileges for that user. This will allow the user to access any resources only to the extent corresponding to their level of trust, which means that the abuse of entitlements and misuse of privileges will be minimized. The user's level of trust is calculated as a weighted mean of the usage frequency, probability of compliance with historical transactions, and the number of attempts to access the resources inappropriately; the level of trust starts at 0.5 and gets updated after each session; besides, the trust level of old users will be decreased at an appropriate rate according to the time factor.The user's role level $R(x)$ is adjusted according to the value of $trust(x)$, using Formula (3):

$$R(x) = \max\left(1, \left[\frac{trust(x)}{T_{threshold}}\right] + 1\right) \tag{3}$$

$R(x)$ represents the current role level of user x. $trust(x)$ represents the trust value of user x. The higher the trust value, the higher the role level.The Role Tree is based on the principle of least privilege: the root is the system administrator, intermediate levels are departmental roles, and the final nodes are particular positions. The hierarchy's level of detail (n) depends on the structure of the organization. At the time of migration of users, the process begins with revoking the previous permissions and granting new ones, with anomaly detection services taking place at the same time to record any unauthorized attempts to access data or perform actions, thus lowering the trust score in real time and triggering the process of permission demotion.

3.3. Identity Authentication Mechanism

In this study, the MFA approach is used to secure management of information assets through proper verification of identity and permission of the users. A two-stage MFA procedure has been applied to elevate security beyond conventional passwords. Firstly, the user's credentials through a username and password are established (knowledge facet). Simply using passwords is insecure because they can be stolen or automated by hackers. Therefore, a second step is added: a one-time code that is sent to the user's mobile phone (possession factor). The dynamic code should be entered by the user. This code is generated separately for each session. This layered mechanism protects the user from getting hacked since even if the password is stolen by the attacker, they still won't manage to authenticate unless they physically possess the user's device.

Assuming the hash value of the password is $H(E)$, the verification formula is:

$$H(E) \stackrel{?}{=} H(E_s) \tag{4}$$

Among them, E is the password entered by the user. E_s is the hash value of the correct password stored in the system database.If $H(E) = H(E_s)$, the verification of the password is successful; otherwise, the password is incorrect and the verification fails. Even though the dual verification of the knowledge factor and the possession factor increases security, there are still some possible security loopholes.Upon successful authentication, an ECC ephemeral key pair is used to negotiate and generate a shared key, which is then derived into a session AES key via HKDF; an ECC key pair is regenerated for each session, enabling protocol-level integration between the identity authentication and encryption modules.

4. Results and discussion

The experimental environment consists of an Intel Core i7-12700 CPU, 16 GB of RAM, and the Windows 11 operating system; the implementation is written in Python 3.10 using the PyCryptodome library, with the AES cipher mode set to GCM, a 256-bit key length, and the ECC algorithm utilizing the secp256r1 curve.

In a computer network environment, information resources are encrypted using the ECC-AES algorithm to form a security mechanism to prevent data leakage. The ECC-AES algorithm can encrypt various network information resource data very well. Different amounts of information resource data are selected for encryption to study the speed of the algorithm encryption time. The encryption time obtained is compared with the encryption time required by ECC, AES, RSA (Rivest-Shamir-Adleman), and DES (Data Encryption Standard). Figure 1 presents the specific comparison results.

Figure 1 when processing 1MB to 10MB of information resource data, the encryption time of ECC-AES is significantly shorter than that of ECC, RSA, and DES algorithms. Even compared with the AES algorithm, ECC-AES shows substantial advantages. The larger the amount of data, the more significant the performance advantage of ECC-AES. When processing 10MB of data, ECC-AES encryption takes only 176 milliseconds, which is much lower than ECC's 861 milliseconds, RSA's 986 milliseconds, and DES's 894 milliseconds. Its encryption time is also better than AES's 438 milliseconds.

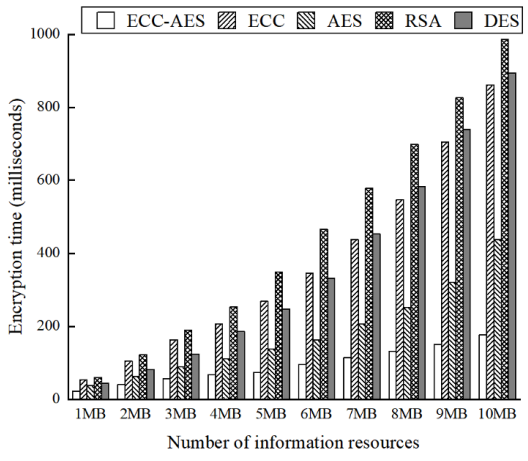


Fig. 1. Comparison of encryption time for information resource data using different encryption algorithms

The ECC-AES algorithm is used to encrypt information resources to form a management security mechanism to

prevent data from being leaked. Its experimental results are compared with ECC, AES, RSA, and DES algorithms. Figure 2 compares the specific data leakage rate results.

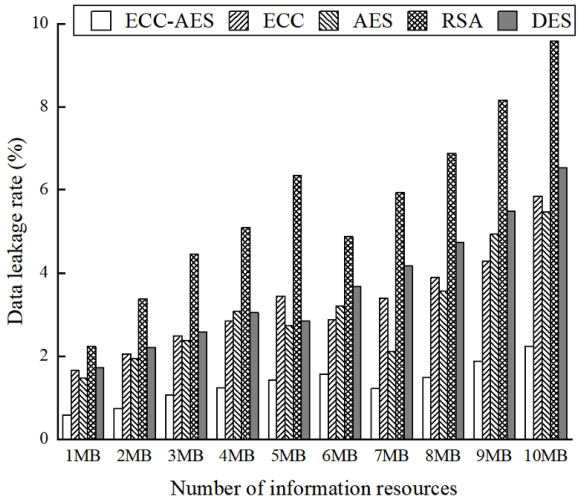


Fig. 2. Comparison of data leakage rates for information resource management using different encryption algorithms

In Figure 2, when processing 1MB to 10MB of data, the data leakage rate of ECC-AES remains low. When processing 10MB of data, the data leakage rate of ECC-AES is 2.24%, which is much lower than 5.84% of ECC, 5.47% of AES, 9.58% of RSA, and 6.53% of DES.

To address risks such as SIM card hijacking, SS7 vulnerabilities, and malicious software interception of SMS messages, this framework prioritizes the use of TOTP-based authentication applications or hardware tokens, and enables binding verification and abnormal login alerting for the SMS channel to reduce the likelihood of one-time passwords being bypassed or intercepted.

5. Conclusion

This research paper analyses the security measures for management of information resources in computer networks in the light of emerging cybersecurity challenges. The role of the ECC-AES hybrid encryption algorithm in secure information transmission and storage is emphasized in the research, given the capability of this encryption technology to combine the features of ECC and AES to encrypt data and manage keys efficiently. In addition to that, the report examines the function of Role-Based Access Control (RBAC) in information system security, explaining how role definition and access control can stop the theft of information.This paper makes use of middleware deployment that works with common databases, file servers, and web applications without needing any changes in business logic; however, it has costs related to key management, operations and support of MFA, renewing certificates, and monitoring of authentication. The research has certain limitations: the size of datasets is from 1 MB to 10 MB only, which does not allow evaluating high-concurrency cases or real attacks; the security assessment is focused on leakage rate analysis only and lacks the analysis of side-channel attacks and management of key lifecycle; moreover, access control and MFA systems do not receive any support from formal verification and users' experiments.

References

[1] M. Ghobaei-Arani, A. Souri, and A. A. Rahmanian, (2019) *"Resource Management Approaches in Fog Computing: A Comprehensive Review"* **Journal of Grid Computing *18***(1): 1–42. DOI: 10.1007/s10723-019-09491-1.

[2] P. Zhang, C. Wang, C. Jiang, N. Kumar, and Q. Lu, (2022) *"Resource Management and Security Scheme of ICPSs and IoT Based on VNE Algorithm"* **IEEE Internet of Things Journal *9***(22): 22071–22080. DOI: 10.1109/JIOT.2021.3068158.

[3] S. Hashemi and M. Zarei, (2020) *"Internet of Things Backdoors: Resource Management Issues, Security Challenges, and Detection Methods"* **Transactions on Emerging Telecommunications Technologies *32***(2): e4142. DOI: 10.1002/ett.4142.

[4] L. Chen, (2022) *"Research on Data Encryption Technology in Computer Network Information Security"* **Engineering Science Research and Application *3***(4): 97–99. DOI: 10.37155/2717-5316-0304-35.

[5] G. Yu, (2020) *"Research on Computer Network Information Security Based on Improved Machine Learning"* **Journal of Intelligent & Fuzzy Systems *40***(4): 6889–6900. DOI: 10.3233/JIFS-189520.

[6] M. Du, (2020) *"Application of Information Communication Network Security Management and Control Based on Big Data Technology"* **International Journal of Communication Systems *35***(5): e4643. DOI: 10.1002/dac.4643.

[7] I. De et al., (2024) *"Implementing Multi-Factor Authentication (MFA) for Robust Network Access Security"* **Journal of Discrete Mathematical Sciences and Cryptography *27***(2-B): 821–832. DOI: 10.47974/JDMSC-1958.