International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Survey on Encryption Technology for Computer Network Data Security Protection

Mr Pradeep Nayak[1], Suhas S[2], Sujal Shyam Bandekar[3], Tejaswini A S[4], Thulasi[5]

Faculty, Department of Information Science And Engineering[1]

Students, Department of Information Science And Engineering[2,3,4,5]

Alva's Institute of Engineering and Technology,Mijar,Manglore,Karnataka,India
Email:thulasipoojary2005@gmail.com

Abstract

Data encryption technology has emerged as the mainstay of the defence system in the context of the coexistence of network security threats and digital transformation. In order to address the inherent flaws in key management, anti-attack capability, and computational efficiency of conventional symmetric and asymmetric encryption algorithms, this study suggests a hybrid encryption algorithm model based on the fusion of symmetric encryption techniques with asymmetric encryption methods. It builds an encryption framework that considers cryptographic strength, real-time performance, and cross-platform compatibility in addition to achieving precise feature vector extraction and noise filtering of network data. Experiments demonstrate that the hybrid algorithm outperforms the single encryption protocol in key space size, attack index, and limit encryption constant value. This validates the hybrid algorithm's technical advantages in fending off sophisticated threats like man-in-the-middle attacks and brute force cracking, and it offers theoretical support for the development of intelligent network security protection systems.

1. Introduction

With the repetitive upgrading of information technology and the faster penetration of digital process, computer network security has become the essential element supporting the digital transformation of society. The Internet of everything's global network ecosystem presents significant obstacles for data asset security and protection: In February 2024, the "2023 Data Breach Investigation Report" produced by Verizon, a communications operator, showed that 83% of network attacks were explicitly targeted at data theft, of which system weaknesses in vital industries such as banking and medical care commonly lead to chain security problems. In this context, as the basic architecture of the network security defence system, the application value of data encryption technology has been extended beyond the traditional information confidentiality to the dimension of active risk defence. The global network ecosystem of the Internet of everything poses serious challenges to the security and protection of data assets: The communications company Verizon's "2023 Data Breach Investigation Report" from February 2024 revealed that 83% of network attacks specifically targeted data theft, with system flaws in critical sectors like banking and healthcare frequently resulting in chain security issues. In this context, as the underlying architecture of the network security defence system, the application value of data encryption technology has been extended beyond the traditional information confidentiality to the dimension of active risk defence.

2. Literature review

In terms of data encryption technology classification and algorithm optimisation, Li Shengqin [1] (2025) suggested in Data Encryption Technology-Based Computer Network Security Management that dynamic keys.Dissemination technique is the primary strategy to increase the security of standard symmetric encryption. The author points out that although AES algorithm has good efficiency, static key is vulnerable to man-in-the-middle attack. By Using time stamp and random integer to generate dynamic key, AES method can successfully deal with the risk of critical leakage. In

addition, the paper also analyses the viability of quantum key distribution (QKD) technology in financial data transfer, stating that its physical non-cloning properties can greatly strenWu Yongfeng [2] (2024) sliced into the Internet of Things scenario and provided the optimisation direction of lightweight encryption technique. According to the research, elliptic curve encryption (ECC) is more appropriate for smart home and industrial sensor networks due to its shorter key length under the same security strength, whereas the traditional RSA algorithm is difficult to adapt to low-power devices due to the large consumption of computing resources. The author empirically confirmed that the hybrid encryption protocol based on ECC may lower the latency of iot communication by 32%.Then payment systems' defences against attacks. Song Yanjing [3] (2025) conducted a comprehensive analysis of the end-to-end encryption (E2EE) implementation process as part of research on differential deployment techniques for data encryption application scenarios. It is discovered that service providers may still receive unencrypted data via intermediary servers even if the TLS protocol can guarantee transport layer security. In order to create a "zero-trust" payment environment, the author suggests a dual ratchet algorithm that combines the Signal protocol to enable dynamic session key updates and uses zero-knowledge proof technology to confirm server behaviour compliance. Zhang Yuanyuan [4] (2024) focusses on the application bottleneck of homomorphic encryption technology.His group created a partial lattice- based homomorphic encryption technique that provides a limited amount of statistical evaluations of encrypted electronic medical records, while reducing the computational overhead to less than 60% of traditional schemes. The scheme has been successfully utilised in the cross-institutional patient data sharing scenario at a number of trial institutions. Sun Qianxiang et al. [5] (2024) concentrated on the government system's usage of hybrid encryption technology and presented a strategy of "layered encryption -centralised decryption". The model employs AES-GCM to accomplish effective encryption at the data transmission layer, uses the state secret SM9 technique

for identity binding at the data storage layer, and realises multi-tenant isolation of the government cloud platform through the key management mechanism, which effectively solves the problem of permission conflict in cross-department data collaboration. In terms of network security system construction and risk management research, Li Jinqiu
[6] (2025) offered a "three-level protection" structure of hybrid encryption system from the standpoint of enterprise-level network security architecture: The first stage utilises SM4 method to encrypt internal communication data for entire traffic.The second stage realises the physical separated storage of key through hardware security module (HSM). The third stage introduces blockchain technology to record key operation logs, ensuring that the key life cycle can be traced. In an energy company deployment, the framework decreased data breaches by 78%.The foundation of Gan Jianfang's [7] (2024) dynamic defence approach for LAN security is the integration of intrusion detection systems (IDS) with encryption technology.

3. Research method

3.1 Classification of data encryption technologies

According to the encryption method, data encryption technology can be divided into symmetric encryption and asymmetric encryption. (1) Symmetric encryption technology Symmetric encryption technology is mainly based on the operation of a single key mechanism, using a single key to complete the whole process of data encryption and decryption(algorithm principle is shown in Figure 1).

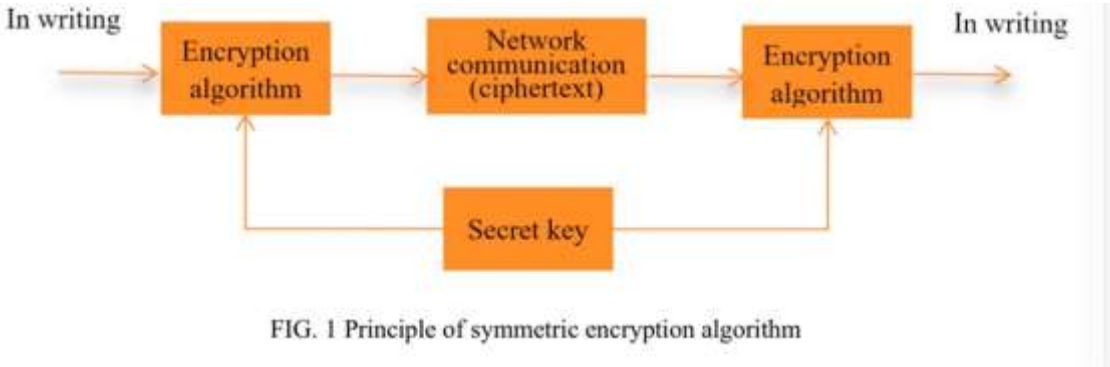

FIG. 1 Principle of symmetric encryption algorithm

This technology system's primary characteristic is that it operates much more efficiently than the asymmetric system, and it is especially ideal for the real-time analysis of sea volume data [8]. In the usual algorithm evolution path, the DES algorithm is gradually replaced due to the brute force cracking risk of 64-bit key length, whereas the AES technique employing 128/192/256-bit variable key has become the mainstream encryption strategy for current iot devices and databases due to its versatility and anti-differential attack capability. Furthermore, the possible leakage risk of key distribution is still the major constraint inhibiting the large-scale use of this technology. The differences between the two encryption techniques are indicated in Table 1.

Table 1 Differences between DES algorithm and AES algorithm

Encryption algorithm	Key length	Algorithmic operation	Insufficient
DES	64-bit	Initial permutation, 16 iterations, inverse permutation	The key length is short, which may cause brute force cracking
AES	128/192/256-bit	Each data can be applied in multiple rounds	The operation process of algorithm encryption is complex

(2) Asymmetric encryption technology

Asymmetric encryption technique realises encryption and decryption separation by generating public and private key pairs by mathematical functions, in which the public key is openly released to the whole network, and the private key is maintained independently by the user (Figure 2). This approach makes it more resistant to attack in an open network setting by ensuring that backward derivation is not possible with one- way trap functions (such as elliptic curve discrete logarithm and huge prime decomposition) [9]. The security of RSA algorithm, as a classical asymmetric representation, is dependent on the complexity of integer decomposition at the thousand bit level.By using elliptic curve geometry, the ECC technique can achieve the same level of security as RSA 1024 bit with a key length of 160 bits while using far less computational power. The technology has been heavily integrated into security infrastructures such as digital certificates and SSL/TLS protocols.

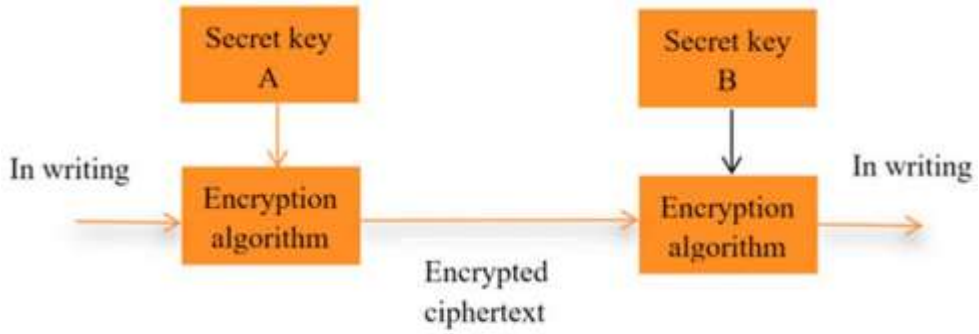

FIG. 2 Principle of asymmetric encryption algorithm

As can be observed from the previous statement, both symmetric encryption and asymmetric encryption schemes have certain faults. In order to further improve the availability of encryption algorithms and the level of network security protection, this paper proposes a hybrid encryption method based on symmetric encryption algorithm (AES) and asymmetric encryption algorithm (ECC) on the basis of comprehensive advantages and disadvantages of symmetric encryption algorithm and asymmetric encryption algorithm (ECC).

4. Experiment and result

This section compares the conventional single protocol encryption algorithm with the hybrid encryption algorithm in this paper using the experimental comparison method in order to confirm the efficacy and viability of the hybrid algorithm of symmetric encryption and asymmetric encryption proposed in this paper in data encryption processing. The comparison index comprises the algorithm key length, key space size, limit encryption constant value, double precision

coefficient, and coverage length.

4.1 Preparation for experiment

In order to evaluate the adaptability of encryption schemes in real network environment, a multi-dimensional.A framework for verification is created.

(1) Simulation environment construction:

Deploy distributed system design based on VMware Workstation virtualisation technology, build eight heterogeneous compute nodes to model network connectivity situations at the company level and set up differentiated hardware parameters (CPU 2-8 core /RAM 4-16GB) for each node to replicate the performance gradient of physical devices.

(2) Data collaboration architecture:

The Hadoop YARN framework is used to build virtual clusters, and dynamic resource scheduling policies are used to achieve adaptive load balancing of cross-node encryption jobs, guaranteeing that experimental data throughput reaches TB level.

(3) Intelligent partitioning of encryption domain:

The communication link is split into six logically isolated encryption subdomains based on data sensitivity and transmission frequency using the hybrid encryption algorithm presented in this paper and the community discovery algorithm in graph theory. Each subdomain is set up with a separate security policy controller.

(4) Quantification of transmission efficiency

The encryption distance evaluation model is developed, which computes the physical span of key distribution path, ciphertext encapsulation time delay and anti-man-in-the- middle attack strength (quantified by fuzzy test coverage), and generates a three- dimensional performance evaluation matrix. The encryption system based on the hybrid encryption algorithm is built in turn, and the corresponding values of five parameters— key length, key space size, limit encryption constant value, double precision coefficient, and coverage length—are set in advance, as indicated in Table 2. The real coverage length of the key base instruction of the hybrid algorithm can be obtained through the multidimensional verification processing of the aforementioned process.

Table 2 Data encryption protocol parameters

Basic encryption protocol items	Single protocol encryption algorithm	Hybrid encryption algorithm
Key Length (bit)	156	164
Key Space Size (bit)	0.9×10^{13}	1.4×10^{13}
Limit encryption constant	13.69	17.08
Double precision coefficient	0.42	0.71
Coverage length (bit)	82	96

According to the corresponding values of the five parameter dimensions given in the above table, the computer network data security encryption environment is constructed, and the operation state is stable under the condition of specific parameter values is verified by comparative analysis of experiments.

4.2 Analysis of experimental results

Experimental comparison indices should be specified in advance before the experiment. This experiment must compare and analyse the encryption security of computer network data under different algorithms, and the attack index must be used to gauge encryption security under various algorithms. The less severe the assault index of data encryption, the better the encryption security. The computation procedure is provided in (5).

$$\eta = \frac{M_0 \times N_s}{\theta} \quad (5)$$

In the preceding formula, M0is the number of nodes in the computer network environment; Ns denotes the number of network communication data's encrypted nodes. θ is a collection of communication linkages between all nodes of a computer network.

On this basis, in order to avoid the uniformity of the experimental results, this paper conducts a comparative analysis according to the two algorithms in Table 2, so as to test the attack situation of network data under the two encryption algorithms. Through experiments, it is found that the attack index of network data encrypted by a single protocol encryption algorithm is maintained between 0.4-0.7, while the attack index of network data encrypted by the hybrid algorithm proposed in this paper is maintained within 0.1, and the encryption effect is more obvious. At the same time, it also shows that the energy characteristics of computer network nodes will directly affect the attack index after data encryption processing, and the hybrid encryption algorithm proposed in this paper has a good effect on improving the security of network data.

5. Conclusion

From the theoretical perspective of algorithm fusion and protocol optimisation, this study systematically demonstrates the paradigm innovation value of hybrid encryption technology in network security defence. Firstly, through the cooperation mechanism of AES and ECC, the efficiency of symmetric encryption and the security strength of asymmetric encryption are successfully harmonised. Secondly, based on the multi- scale analysis framework of network data feature vectors, a quantitative design technique of encryption constraints is proposed to provide universal criteria for the adaptive configuration of encryption algorithms in varied contexts. Ultimately, intelligent partitioning of the encryption area and quantisation model of transmission efficiency indicate the theoretical benefits of hybrid encryption in lowering attack surface and enhancing protocol robustness. The research results show that the core theoretical contribution of hybrid encryption technology is to break through the linear defense logic of traditional encryption algorithms, and realise the nonlinear cooperative optimisation of security and computing efficiency through algorithm coupling and protocol layering.

Reference

[1] Li Shengqin. Computer Network Security Management Based on Data Encryption Technology [J]. Network security Technology and application, 2025, (03): 34-36.

[2] WuYongfeng. Application Research of Data Encryption Technology in Computer Network security [J]. Electronic Products World, 2024, 31 (12): 9-11+23.

[3] SongYanjing. Application Research of Data Encryption Technology in Computer Network Security [J]. Digital Communication World, 2025, (01): 124-126.

[4] ZhangYuanyuan. Application Research of Data encryption Technology in the field of Computer Network security [J]. China Management Information Technology, 2024, 27
(24): 175-177.

[5] Sun Qianxiang, Liu Xianghuan. Research on application of Hybrid data encryption technology for Computer network information Security [J]. China Broadband, 2024, 20
(11): 55-57.

[6] LI Jinqiu. Construction Strategy of Data Encryption Technology in Computer Network Security System [J]. Information and Computer, 2025, 37 (04): 71-73.

[7] Gan Jianfang. Practical Application of Data encryption Technology in Computer Network Security System [J].

Computer Knowledge and Technology, 2024, 20 (36): 79-82.

[8] Sang Jiacun. Application Research of Data Encryption Technology in Computer Network security [J]. Digital Communications World, 2024, (11): 150-152.

[9] Chen Hua, Cao Ruicheng. Application of data encryption technology in Computer network security [J]. Science and Technology Information, 2024, 22 (20): 51-53. (in Chinese).

[10] Dong Hongmeng. Application and Protection Strategy of data Encryption Technology in Computer Network Information Security [J]. Paper Equipment C Materials, 2024, 53 (10): 130-132.

[11] Lu Huawei. Research on data encryption technology based on Computer network information security [J]. Information Systems Engineering, 2024, (08): 132-135.

[12] Zhao Weili. Application analysis of data encryption technology in Computer network security system [J]. Information and Computer (Theoretical Edition), 2024, 36 (14): 142-
144.