International Journal of Information and Communication Technology

ISSN online: 1741-8070 - ISSN print: 1466-6642
https://www.inderscience.com/ijict

Dual-modal system for real-time encryption and anomaly detection of 5G communication data integrating AES-GCM and LSTM

Hui Wang

DOI: 10.1504/IJICT.2026.10077622

Article History:

Received:	27 September 2025
Last revised:	28 October 2025
Accepted:	28 October 2025
Published online:	05 May 2026

Copyright © 2026 Inderscience Enterprises Ltd.

Dual-modal system for real-time encryption and anomaly detection of 5G communication data integrating AES-GCM and LSTM

Hui Wang

Department of Information Engineering,
Hebei Chemical & Pharmaceutical College,
Shijiazhuang, 050000, China
Email: HuiWanngg@outlook.com

Abstract: To address security and real-time challenges in 5G networks, this paper proposes a dual-modal system integrating AES-GCM encryption with an LSTM anomaly detection model, effectively balancing data confidentiality with anomaly identification. Experimentally, the system achieves optimal response speeds with encryption and decryption times of 18.4 ms and 21.7 ms, respectively. It demonstrates superior detection capabilities, attaining 98.1% accuracy – surpassing standalone models – while restricting missed detections to 1.0% and false positives to 0.5%. Additionally, the system excels in high-bandwidth environments, with encryption delays dropping significantly to 0.04 ms. In terms of resource efficiency, the hybrid model optimises CPU scheduling and lowers energy consumption to 130 J, compared to 165 J for traditional AES-GCM. Conclusively, this dual-modal architecture provides a robust, quantitatively validated solution that significantly enhances security, efficiency, and real-time processing in 5G scenarios.

Keywords: 5G communication; AES-GCM; LSTM; anomaly detection; encryption algorithm optimisation.

Reference to this paper should be made as follows: Wang, H. (2026) 'Dual-modal system for real-time encryption and anomaly detection of 5G communication data integrating AES-GCM and LSTM', *Int. J. Information and Communication Technology*, Vol. 27, No. 41, pp.21–44.

Biographical notes: Wang Hui obtained her BE in Communication Engineering from Jilin University in 2004. She obtained her ME in Communication and Information from Jilin University in 2008. Presently, she is working as a Lecturer in the Department of Information Engineering, Hebei Chemical and Pharmaceutical College. Her areas of interest are computer communication technology, Intelligent network, network security, mobile application development and software technology.

1 Introduction

With the rapid advancement and widespread adoption of 5G technology, ensuring data security has become a critical issue in global network communications (Dao et al., 2024). The high speed, large capacity, and low latency of 5G networks make them ideal for a wide range of critical applications. However, at the same time, according to relevant

Copyright © The Author(s) 2026. Published by Inderscience Publishers Ltd. This is an Open Access Article distributed under the CC BY-NC-ND license. (http://creativecommons.org/licenses/by-nc-nd/4.0/)

research, security threats are becoming increasingly serious (Pandey et al., 2024). The large volume and complexity of data in 5G communications have significantly increased the need for real-time encryption and anomaly detection technologies. The function of data encryption technology is to protect the confidentiality and integrity of communication content. In contrast, anomaly detection technology can quickly detect potential security threats and prevent data leakage or tampering. Improving the security of 5G communications, particularly by combining data encryption and anomaly detection, has become a key focus in current network security research.

Table 1 Glossary of terms

Symbol/term	*Description*
AES-GCM	Advanced encryption standard-Galois/counter mode
LSTM	Long short-term memory
5G	Fifth generation mobile network
CPU	Central processing unit
GPU	Graphics processing unit
TPR	True positive rate in anomaly detection
ECP	Energy consumption parameter
System load (K)	Load factor representing system workload
Throughput	Data transmission rate
σ	Sigmoid activation function
tanh	Hyperbolic tangent activation function
L	Loss function for anomaly detection
N	Number of samples in dataset

Traditional encryption methods usually rely on symmetric encryption algorithms, such as AES, which can protect data from theft (Song et al., 2025). However, with the continuous evolution of attack methods, it is not easy to cope with complex and ever-changing security challenges only by relying on a single encryption mechanism. Recently, anomaly detection methods based on deep learning have gradually emerged. As a deep learning model, long short-term memory (LSTM) has been widely used in network security due to its advantages in time series data processing (AbdElkader et al., 2025). LSTM can capture timing characteristics during data transmission, identify potential abnormal behaviours, and support timely response measures. Combining LSTM with AES-GCM encryption algorithms is expected to achieve dual data encryption and anomaly detection guarantees, thereby improving the security of 5G communications.

However, most existing studies focus on a single encryption or anomaly detection technology, lacking in-depth discussion on combining the two. As an encryption algorithm widely used in 5G communication, AES-GCM has been applied in multiple security protocols due to its efficient encryption performance and built-in authentication mechanism (Mobilon and Arantes, 2021). However, despite its excellent performance in data encryption, it still has some shortcomings in detecting abnormal activities during transmission, such as malicious attacks, traffic hijacking, etc. Therefore, combining the advantages of the LSTM model, combining encryption with real-time anomaly detection, the security protection capabilities of 5G networks can be effectively improved, and various network attacks can be discovered and responded to promptly.

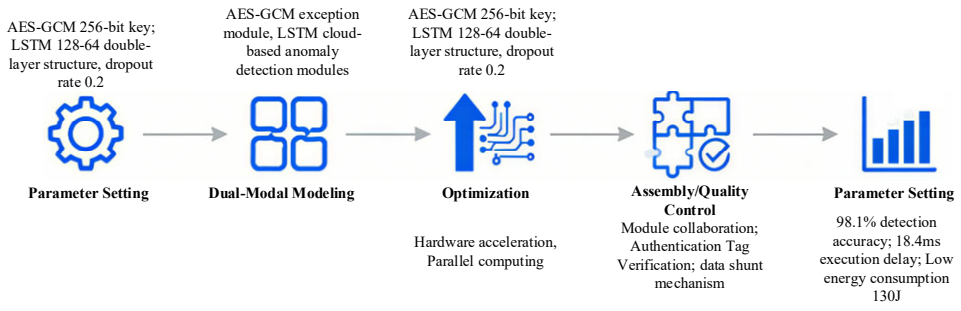
This study proposes a dual-modal system that fuses AES-GCM encryption with LSTM anomaly detection, aiming to provide an innovative security solution for 5G communication networks. The main innovation of this paper lies in the integration of two critical technologies – AES-GCM encryption and LSTM-based anomaly detection – into a unified system. This dual approach addresses both data confidentiality and real-time security monitoring simultaneously, which significantly enhances the security protection of 5G communications. Unlike existing methods that either focus solely on encryption or anomaly detection, our system offers a novel dual-layer security framework that dynamically adapts to evolving network threats, providing a more robust defence against complex 5G communication challenges. The system can ensure data confidentiality and integrity during transmission, identify abnormal behaviours, and issue timely alarms by analysing traffic data in real-time. The core advantage of this dual-modal system is that it integrates two key encryption and anomaly detection technologies, forming a closed loop of protection and response, greatly enhancing the anti-attack capabilities of 5G communications. Through in-depth research and experimental verification of this system, we hope to provide new ideas and practical guidance for the security protection of 5G networks.

In response to the current situation of separating encryption and anomaly detection functions in 5G communication, this study proposes a dual-mode architecture that integrates AES-GCM and LSTM, which achieves intelligent threat monitoring while ensuring data confidentiality through real-time collaborative processing mechanism. The experiment shows that the scheme is superior to the single model in encryption and decryption efficiency, detection accuracy and resource utilisation, and effectively solves the problem that it is difficult to give consideration to security and real-time in 5G high throughput scenarios.

In order to provide a clear baseline for evaluating the performance of the proposed hybrid model, this paper compared it with several traditional and alternative methods, including independent AES encryption, RSA encryption, and SVM-based anomaly detection. These methods are widely used in 5G security research and serve as representative benchmarks. The results indicate that our AES-GCM+LSTM fusion model has achieved significant improvements in encryption speed, detection accuracy, and energy efficiency compared to these traditional methods.

This study proposes a dual-modal system that fuses AES-GCM encryption with LSTM anomaly detection, aiming to provide an innovative security solution for 5G communication networks. To better understand the technical foundations of this system, Section 2 will review the theoretical underpinnings of the AES-GCM encryption and LSTM anomaly detection algorithms, alongside an exploration of related research in network security. The framework of the manuscript is organised as follows: Section 2 reviews the theoretical foundations of AES-GCM and LSTM, and summarises related work on their application in network security. Section 3 presents the design and structure of the proposed dual-modal system, including detailed descriptions of the AES-GCM encryption module and the LSTM anomaly detection module. Experimental results and their analysis are discussed in Section 4, showcasing the performance of the hybrid model in terms of encryption efficiency, anomaly detection accuracy, and resource utilisation. Finally, Section 5 concludes the paper and discusses potential future directions for enhancing the system's performance and scalability. The path map for small-scale intelligent construction is shown in Figure 1.

Figure 1 Path map for small-scale smart construction (see online version for colours)



2 Background and related work

2.1 Theory of AES-GCM and LSTM algorithm

Advanced encryption standard-Galois/counter mode (AES-GCM) is a widely used symmetric encryption algorithm that combines encryption and authentication to provide data confidentiality and integrity in communication systems. It operates by encrypting data with the AES block cipher and authenticating it through the Galois/counter mode, which ensures both the secrecy and integrity of the data during transmission (Asadi et al., 2025; Bai et al., 2025a). In AES-GCM, AES is responsible for data confidentiality protection as the underlying encryption algorithm. At the same time, GCM mode verifies the integrity and authentication of data by generating message authentication codes (MAC) (Bai et al., 2025b). This combination ensures that data will neither be stolen nor tampered with during transmission and is especially suitable for application scenarios that require high throughput and low latency, such as 5G communications. However, although AES-GCM has strong performance and security while providing data encryption, it still faces increasingly complex network attacks and threats, especially in large data traffic and diversified attack methods; a single encryption mechanism cannot meet all security challenges.

As a common deep learning model, LSTM has strong time series data processing capabilities and is especially suitable for tasks that need to learn time-dependent features from historical data (Bai et al., 2025c; Cai et al., 2025). In network security, LSTM is widely used in traffic analysis and anomaly detection (Chang et al., 2025). Since LSTM can effectively capture long-term and short-term dependencies in time series, it is suitable for identifying abnormal network communication behaviours. By training the LSTM model to learn the normal network traffic pattern, the system can send out timely alarms when abnormalities occur, such as sudden traffic increases and packet retransmission. The advantage of the LSTM model lies in its ability to model complex patterns, which can extract potential security threats from a large amount of network communication data, thus providing strong support for network protection.

Combining AES-GCM and LSTM can effectively realise the dual guarantee of data encryption and anomaly detection. AES-GCM provides privacy protection in network communication while ensuring data encryption and integrity, while LSTM can identify potential abnormal activities by analysing traffic data in real-time (Cui et al., 2025; Fathi et al., 2025). This fusion mode can improve the system's defence against various network

attacks. In 5G communication, due to its high speed and high concurrency characteristics, attackers can destroy the system's security through various means, such as denial of service attacks and malicious traffic injection (Fatimah et al., 2025). Combining AES-GCM and LSTM allows the system to monitor abnormal traffic while encrypting data dynamically, thus realising real-time protection. AES-GCM is responsible for ensuring the secure transmission of data, while LSTM is responsible for detecting whether there are malicious attacks or abnormal behaviours, forming a collaborative protection mechanism.

By designing this convergence model, more efficient and secure data protection can be achieved in the complex environment of 5G communication. Specifically, AES-GCM provides an encryption layer to ensure the confidentiality and integrity of data during transmission and prevent data from being illegally accessed or tampered with; LSTM, on the other hand, can find and respond to abnormal traffic in time by learning the behaviour pattern of normal traffic, and prevent potential security threats from affecting the operation of the system (Geng et al., 2025). With the continuous development of 5G technology, the forms and means of network attacks will become increasingly complex. Combining AES-GCM and LSTM technologies can effectively improve the security of 5G communication and meet the dual needs of data encryption and anomaly detection in modern network environments (Guo et al., 2025). This innovative dual-modal system not only enhances data protection capabilities but also provides important support for real-time security monitoring and response.

This section establishes the fundamental knowledge and background for the system we propose. Firstly, this article reviews the core algorithms that make up the dual-mode system: AES-GCM and LSTM. Then, it investigated the existing research on the intersection of these technologies and 5G security, emphasising the gaps that this work aims to address.

2.2 Status of 5G communication data between AES-GCM and LSTM

Network security issues have increasingly become the focus with the widespread application of 5G communication technology. The high rate, low latency, and large capacity of 5G networks support various emerging applications but also bring great security challenges (Gupta et al., 2025). Data encryption and anomaly detection, as core technologies to ensure network security, play a vital role in 5G communications. Existing encryption technologies, such as AES-GCM, have been widely used to ensure the confidentiality and integrity of data transmission. However, with the continuous change of network attack forms, traditional encryption mechanisms are still insufficient in dealing with new attacks. At the same time, applying deep learning models such as LSTM in anomaly detection provides new ideas for solving this problem. Combining encryption technology with intelligent anomaly detection methods allows complex security threats in 5G networks to be dealt with more effectively.

In the practical application of 5G communication, AES-GCM has become an important means of data protection due to its efficient and reliable encryption performance (Hou et al., 2025; Hu et al., 2025). The ability of AES-GCM to provide powerful encryption capabilities, combined with authentication mechanisms to ensure the integrity of data during transmission, makes it widely used in many security protocols. Especially in the 5G environment facing large amounts of data and high-speed

transmission, the advantages of AES-GCM are more obvious, which can ensure data privacy and prevent tampering. However, although AES-GCM can effectively prevent data leakage and tampering, it still cannot effectively monitor abnormal behaviours in network traffic. Therefore, relying solely on encryption technology cannot meet the demand for comprehensive security protection in 5G communications, and other technologies must be introduced to strengthen anomaly detection and protection capabilities.

As a deep learning model suitable for processing time series data, LSTM has shown great potential in network security in recent years (Huang et al., 2025). By learning historical data, LSTM can accurately identify normal flow patterns and discover abnormal flow in time (Kasemrat and Kraiwanit, 2025). In the 5G network environment, LSTM is suitable for detecting sudden anomalies in traffic, such as network attacks, traffic surges, or hidden attacks of malicious behaviours. Due to the timing characteristics of data transmission in 5G communications, LSTM can leverage its powerful time-dependent modelling capabilities to analyse and identify potential security threats effectively. Although LSTM has significant advantages in anomaly detection, its application in large-scale, highly concurrency 5G network environments still faces challenges such as huge data volume and high computational complexity. Therefore, combining LSTM and traditional encryption technology has become a new direction to improve the security of 5G networks.

Combining AES-GCM and LSTM technologies can effectively compensate for existing security mechanisms' shortcomings and realise the dual guarantee of data encryption and anomaly detection. In this dual-modal system, AES-GCM is responsible for ensuring the confidentiality and integrity of data and preventing data from being tampered with or stolen during transmission. At the same time, LSTM analyses data traffic in real time to identify potential abnormal behaviours and prevent attackers from penetrating the network through vulnerabilities. With the continuous development of 5G technology, the threats faced by network security are becoming increasingly complex, and the traditional single encryption or detection mechanism has made it difficult to meet the requirements. Introducing the organic combination of LSTM and AES-GCM can improve data security and detect and respond to potential anomalies for the first time, greatly improving the security protection capabilities of 5G communication systems. This new security architecture will provide a more reliable guarantee for the secure operation of future 5G networks.

To comprehensively evaluate the performance of dual-mode systems, this article analyses the impact of system load, packet size, network bandwidth, and resource allocation ratio on core indicators such as encryption latency, detection accuracy, CPU usage, and energy consumption. The results show that system load and packet size have a significant impact on encryption latency and CPU consumption, while bandwidth and detection resource allocation mainly determine detection accuracy, indicating that the system needs to strike a balance between communication and computing resources to optimise the configuration of key parameters for specific needs.

The key parameters of AES-GCM and LSTM modules are set according to standard specifications and empirical tuning, respectively: AES-GCM uses NIST recommended 256 bit keys and 128 bit authentication labels to ensure basic security; LSTM uses grid search to determine the adoption of a '128-64' double-layer structure, 0.2 dropout rate, and Adam optimiser, which improves detection effectiveness while controlling overfitting, thus jointly constructing a 'constitutive model' of the system that balances safety and performance.

3 Establishment of a real-time encryption anomaly detection model for 5G communication data integrating AES-GCM and LSTM

3.1 Overall model framework and process

Real-time encryption and anomaly detection have become key technical directions to deal with various security threats that may exist in 5G communications (Kaur and Kaur, 2025). This study uses a dual-modal system that fuses AES-GCM and LSTM to achieve efficient 5G communication data encryption and anomaly detection. The system fully uses the high efficiency of the encryption algorithm AES-GCM and the advantages of the LSTM model in sequence data processing by combining encryption technology with deep learning. The LSTM model output formula is shown in equation (1).

$$h_t = LSTM\left(x_t, h_{t-1}, c_{t-1}\right) \tag{1}$$

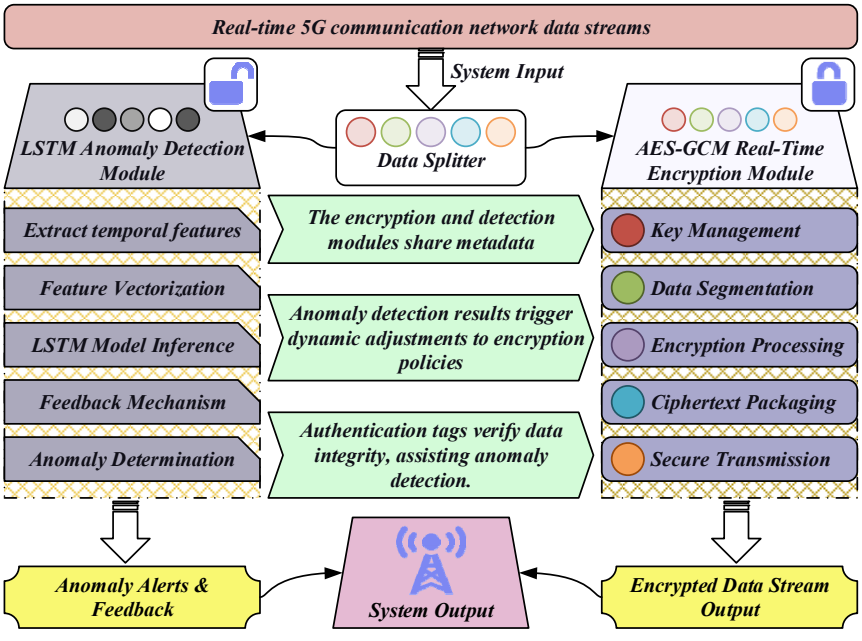
where h_t represents the output hidden state of the LSTM, x_t represents the current input data, h_{t-1} represents the hidden state at the previous time, and c_{t-1} represents the cell state at the previous time. The LSTM cell status update formula is shown in equation (2).

$$c_t = f_t \cdot c_{t-1} + i_t \tag{2}$$

where c_t denotes the cell state at the current moment, c_{t-1} denotes the cell state at the previous moment, f_t denotes the output of the forget gate, and i_t denotes the output of the input gate.

The model framework of the system consists of two main modules: the first module is the real-time data encryption module based on AES-GCM, and the second module is the anomaly detection module based on LSTM (Khan et al., 2025). The AES-GCM encryption algorithm protects the confidentiality and integrity of communication data and ensures data security during transmission (Ławryńczuk and Zarzycki, 2025). The LSTM model performs real-time anomaly detection on the encrypted communication data and discovers any potential abnormal behaviours or attacks in time by learning the rules in historical data. Combining these two technologies, this system can realise data encryption and anomaly detection simultaneously, effectively improving the network protection ability while ensuring communication data security. The flowchart of the dual-modal system of 5G communication data real-time encryption and anomaly detection is shown in Figure 2.

Figure 2 Flowchart of 5G communication data real-time encryption and anomaly detection dual-modal system (see online version for colours)



The figure shows that the system starts from the real-time 5G communication data stream and synchronously sends the data to the two major modules of encryption and detection through the data shunt. The LSTM module on the left sequentially performs time series feature extraction, feature vectorisation, model reasoning, and anomaly determination and continuously optimises the recognition logic through the feedback mechanism. The AES-GCM encryption module on the right completes key management, data segmentation, encryption operation, ciphertext packaging, and secure transmission. The two modules cooperate by sharing metadata, and the detection results can dynamically adjust the encryption strategy, and the authentication tag generated by encryption can reversely support exception verification. The system's output includes abnormal warning information and an encrypted data stream, which realises the dual goals of data security and intelligent communication monitoring.

The innovation of this model lies in its dual-mode design concept, which combines encryption with anomaly detection, which can not only affect the normal transmission efficiency of communication data but also monitor the security of data in real time. Traditional encryption schemes usually focus on data confidentiality but neglect detecting abnormal behaviour; however, the anomaly detection method based on LSTM usually ignores the encrypted data processing (Li et al., 2025). By organically combining the two, the research proposes a new dual mechanism of encryption and security detection, which can deal with complex 5G communication security threats. The formula for calculating the total cost of the bimodal system is shown in equation (3).

$$C = AES(P, K) \tag{3}$$

Among them, C represents the encrypted ciphertext, P represents the plaintext, and K represents the encryption key. The LSTM forward propagation formula is shown in equation (4).

$$h_t = \tanh\left(W_h x_t + b_h\right) \tag{4}$$

where h_t represents the hidden state of the LSTM at time step t, W_h represents the weight input to the hidden layer, x_t represents the input at time step t, b_h represents the bias term of the hidden layer, and tanh represents the hyperbolic tangent activation function. Firstly, the system encrypts the communication data by AES-GCM. While ensuring the security of the data, it uses the LSTM model to analyse the time series of the encrypted data to detect whether there are any abnormal behaviours. This process not only improves the transmission efficiency of encrypted data but also captures security vulnerabilities that may be concealed by encrypted data through deep learning models, thus achieving more comprehensive security protection. The anomaly detection loss function is shown in equation (5).

$$L = \frac{1}{N}\sum_{i=1}^{N}\left(y_i^{'} - y_i\right)^2 \tag{5}$$

where L represents the loss function, N represents the number of samples, y_i represents the actual label, and $y_i^{'}$ represents the model prediction output.

The dual-mode system is mainly oriented to real-time security scenarios such as 5G edge computing, the internet of things and the internet of vehicles, which can effectively balance encryption strength, detection accuracy and resource efficiency. But its applicability has boundaries: it is not suitable for communication environments with extremely limited computing power, non-real time data processing, or significant differences between attack patterns and training data.

3.2 AES-GCM real-time encryption module

AES-GCM is a widely used encryption algorithm with efficient performance and strong security. In 5G communications, data transmission speed and security are two important indicators, and AES-GCM can meet this requirement with its parallelisation characteristics and efficient encryption methods. The first module of this study is the AES-GCM real-time encryption module, which is mainly responsible for encrypting communication data to ensure the confidentiality and integrity of data during transmission (He et al., 2021). The formula for encryption and transmission efficiency is shown in equation (6).

$$f_t = \sigma\left(W_f x_t + U_f h_{t-1} + b_f\right) \tag{6}$$

where f_t represents the forgetting gate output at time step t, W_f represents the input weight of the forgetting gate, U_f represents the hidden state weight of the forgetting gate, b_f represents the bias of the forgetting gate, and σ represents the Sigmoid activation function. The LSTM memory update formula is shown in equation (7).

$$C_t = f_t \cdot C_{t-1} + i_t \tag{7}$$

where C_t denotes the memory cell at time step t, C_{t-1} denotes the memory cell at time step $t-1$, ft denotes the output of the forgetting gate, and it denotes the output of the input gate. In this module, AES-GCM encryption adopts a symmetric encryption mechanism, encrypts data through a key, and uses an authentication tag to verify the integrity of the data. AES-GCM mode combines the encryption algorithm of AES and the authentication function of Galois counter mode, which provides efficient encryption performance and ensures that data is not tampered with during transmission. To achieve real-time encryption, the system uses hardware acceleration technology to increase encryption speed, reduce latency, and ensure it can operate stably in high-speed 5G network environments. The AES-GCM encryption formula is shown in equation (8).

$$o_t = \sigma\left(W_o x_t + U_o h_{t-1} + b_o\right) \tag{8}$$

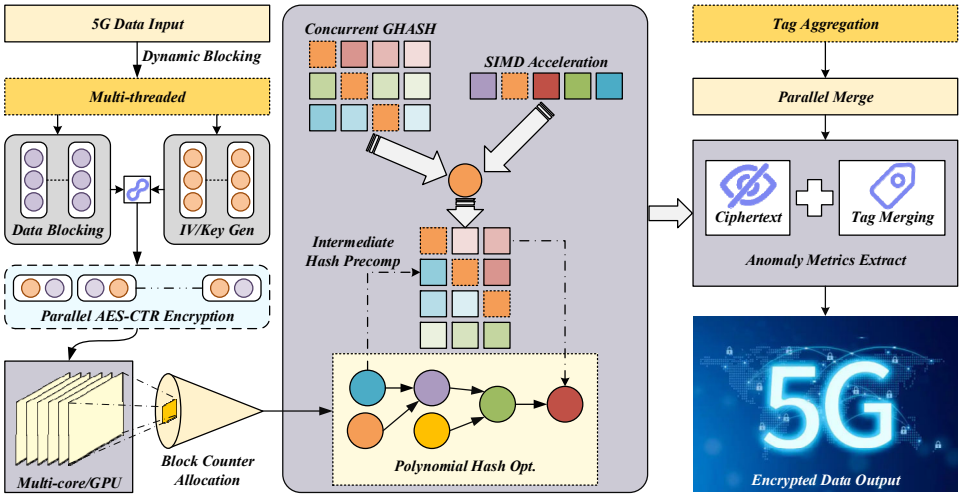
where o_t represents the output gate output at time step t, W_o represents the input weight of the output gate, U_o represents the hidden state weight of the output gate, and b_o represents the bias of the output gate. The final output formula of LSTM is shown in equation (9).

$$h_t = o_t \cdot \tanh\left(C_t\right) \tag{9}$$

where h_t represents the hidden state of the LSTM at time step t, o_t represents the output of the output gate, and C_t represents the memory unit at time step t. This module's design focuses on ensuring encryption performance without affecting communication efficiency. To achieve this goal, the key technologies in the AES-GCM encryption process are parallelised encryption and concurrent computation (Sarkar et al., 2022). Through the design of hardware optimisation and parallel processing, this module can encrypt large amounts of data in real-time data streams while maintaining low latency and high throughput to meet the high bandwidth requirements of 5G networks. The parallelisation and concurrent computing design of the AES-GCM encryption process in 5G networks is shown in Figure 3.

This figure illustrates the data flow from input to output, including dynamic blocking, multi-threaded scheduling, parallel AES-CTR encryption, and GHASH processing. The boundary conditions are represented by initialisation parameters. Indicate measurement points at each processing stage to monitor encryption performance and resource usage. The entire process starts with 5G data input. After dynamic blocking and multi-thread scheduling processing, the data is divided into multiple blocks, and module pairing initialisation parameters are generated through IV/key. Then, the parallel AES-CTR encryption strategy is adopted, and the block counter is allocated through a multi-core GPU or CPU to realise encryption parallelisation. The next GHASH processing stage uses SIMD acceleration and intermediate hash pre-processing and cooperates with a polynomial hash optimisation module to accelerate message authentication code generation (Pawar and Ainapure, 2025). Finally, the ciphertext and tag information are integrated into the parallel merging and tag aggregation stages, and the output is structured encrypted data through the abnormality indicator extraction module to support efficient, low-latency, and secure transmission in subsequent 5G communications. This architecture fully embodies the fusion optimisation design of parallel computing and encryption processes.

Figure 3 Parallelisation and concurrent computing design of AES-GCM encryption process in 5G network (see online version for colours)



Every bit of data in the encryption process needs to undergo rigorous security checks and verification to ensure its confidentiality and integrity (Pramanik et al., 2025). In this module, AES-GCM encryption not only encrypts the data through the key but also ensures that the data transmission is not tampered with through the authentication tag. This design ensures communication data security and prevents data from being attacked by man-in-the-middle or other security threats during transmission.

The AES-GCM real-time encryption module ensures safe data transmission through its efficient and parallel encryption characteristics without significantly affecting communication efficiency. This provides a secure data foundation for the subsequent anomaly detection module and lays an important guarantee for the security of the whole system.

In the system, performance and safety thresholds correspond to the 'yield criterion'; The ability to maintain performance through resource scheduling and algorithm optimisation corresponds to 'hardening behaviour' when the load increases; the interface and collaborative mechanism between encryption and detection modules correspond to a 'bolted connection'; the mechanism for handling data flow timing, packet loss, or congestion corresponds to the 'contact' problem.

3.3 LSTM anomaly detection module

LSTM is a classical variant of recurrent neural networks widely used in modelling and predicting sequence data. Compared with traditional RNN, LSTM can effectively solve the gradient vanishing problem and has stronger long-term memory ability (Singh and Sharma, 2025). This study uses the LSTM model for real-time anomaly detection, aiming to automatically identify abnormal behaviours in communication data streams by learning historical data, thereby providing real-time security monitoring for 5G communication systems.

The LSTM anomaly detection module's core idea is to analyse the encrypted data stream's time series, capture the laws and changes in it, and find potential anomalies in time. Specifically, the system first collects the data stream in 5G communication and inputs it into the LSTM model for training. The LSTM model establishes the behaviour pattern of normal data flow by learning the time dependence of these data. Once abnormal behaviour is inconsistent with the normal mode, the model will detect it through the set threshold and issue an alarm in time. The LSTM anomaly detection formula is shown in equation (10).

$$Error = \frac{I}{N}\sum_{i=1}^{N}\left(y_i - y_i'\right)^2 \tag{10}$$

Among them, *Error* represents the prediction *Error*, N represents the total number of samples, y_i represents the actual value, and y_i' represents the predicted value. The data difference calculation formula is shown in equation (11).

$$\Delta D = \|C - D\| \tag{11}$$

where ΔD represents the difference between encrypted data and decrypted data, C represents encrypted data, and D represents decrypted data. To ensure the high efficiency and accuracy of detection, this module adopts an improved LSTM network structure. It uses a large amount of historical data in the training process to enhance the generalisation ability of the model. This enables the LSTM model to maintain high accuracy and find abnormal behaviours in time when facing complex and changeable communication data. At the same time, to improve the model's real-time performance, the anomaly detection module also adopts the incremental learning method, which can continuously adjust the model according to new data to improve detection accuracy and flexibility.

This module's function is to detect abnormalities in communication data and prevent data from being tampered with or forged in the encryption process by cooperating with the AES-GCM encryption module. In some attack scenarios, the attacker may try to achieve the attack purpose by manipulating the information in the data stream, and the LSTM anomaly detection module can identify these abnormal operations and issue warnings through in-depth analysis of the data sequence, thus enhancing the protection capabilities of the entire system.

The design of the LSTM anomaly detection module has the following advantages: First, through deep learning, it can automatically learn normal behaviour patterns from historical data without human intervention. Secondly, the LSTM model has powerful processing capabilities, capturing complex time series relationships in the data stream, thus effectively discovering potential abnormal behaviours. Finally, combined with the encrypted data of the AES-GCM encryption module, the LSTM model can more accurately detect anomalies in the encrypted data, whether it is network attacks or data leakage.

The scope of this study is limited to the network security of 5G communication data. The proposed model and analysis do not cover the physical or structural characteristics of network components, as well as the mechanical behaviour of grouting sleeves or similar components in civil engineering.

This article verifies the parameter independence of different combinations of sequence length and data block size through testing. The system achieves stable

performance under the two-level configuration, with detection accuracy and encryption throughput tending to converge. Although the three-level configuration has similar accuracy, the computational cost significantly increases. Therefore, the two-level configuration is ultimately adopted to balance robustness and computational efficiency.

4 Experimental results and analysis

To ensure the reproducibility and clarity of the experiment, the key simulation parameters and boundary conditions are defined as follows. The system evaluates under displacement control loading conditions and simulates the data inflow rate in 5G networks. The loading rate is set to simulate 5G peak data traffic, with an average input data rate of 1 Gbps, and stress testing is conducted at a rate of up to 5 Gbps to evaluate the system's performance under extreme conditions. The interaction between the encryption module and the anomaly detection module is configured with a coupling coefficient of 0.85, allowing for controlled information sliding and dynamic adjustment between the two processes. Allow data flow to be separated from detection logic to simulate potential decoupling caused by latency, and provide reordering buffers to handle out of order data packets. All experiments were carried out under fixed boundary conditions, where the computing resources of the system were fully allocated and restricted to simulate resource constrained edge computing nodes.

This experiment uses simulated traffic data from 5G communication networks, combined with the AES-GCM encryption algorithm and LSTM anomaly detection model, to study how to improve the real-time encryption and security of 5G communication data. The experimental data includes normal traffic and typical attack patterns, such as denial of service attacks and malicious data injection. In terms of hardware facilities, high-performance computing servers, and GPU units are used in the experiment to support efficient training and reasoning of deep learning models. The software environment includes Python, TensorFlow, and PyTorch frameworks to ensure the smooth implementation and verification of the model. Through this software and hardware platform, the experiment provides in-depth theoretical and practical support for the security of 5G communication networks. The comparison of encryption and decryption delays is shown in Table 2.

Table 2 Comparison of encryption and decryption delays

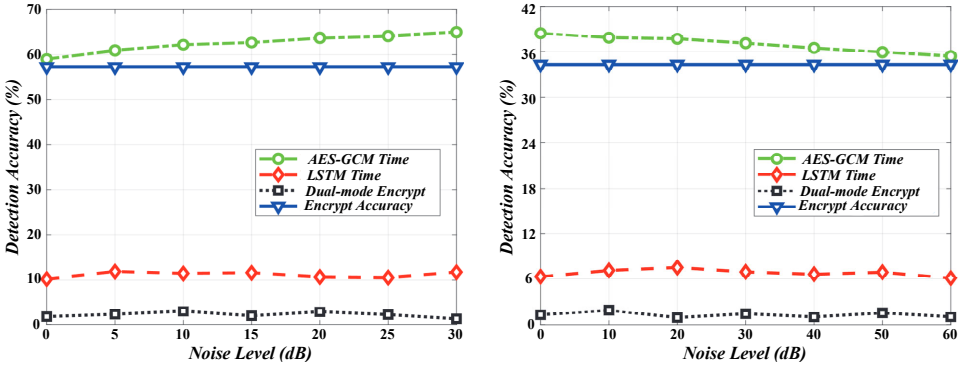
Models	*Encryption time (ms)*	*Decryption time (ms)*	*Delay increase rate (%)*
AES-GCM	12.5	15.3	22.4
LSTM	25.7	29.6	15.2
Hybrid model	18.4	21.7	16.1
No encryption	0.5	0.6	0

The table shows the encryption and decryption times of AES-GCM, LSTM, and hybrid models in 5G communications. The AES-GCM model exhibits lower latency during the encryption process, while the LSTM model takes more time. Although the hybrid model slightly increases the delay compared with AES-GCM, its performance in the encryption and decryption process is optimised compared with LSTM. The latency without encryption is almost negligible. This data analysis shows that the hybrid model has

achieved a certain balance in encryption and decryption efficiency and is suitable for achieving a compromise between security and speed in 5G communications.

This paper compares the encryption and decryption times of AES-GCM and LSTM models in 5G communications to compare their delay and test their impact on network environments with high real-time requirements. The results are shown in Figure 4.

Figure 4 Comparison of encryption and decryption time between AES-GCM and LSTM models in 5G communication (see online version for colours)



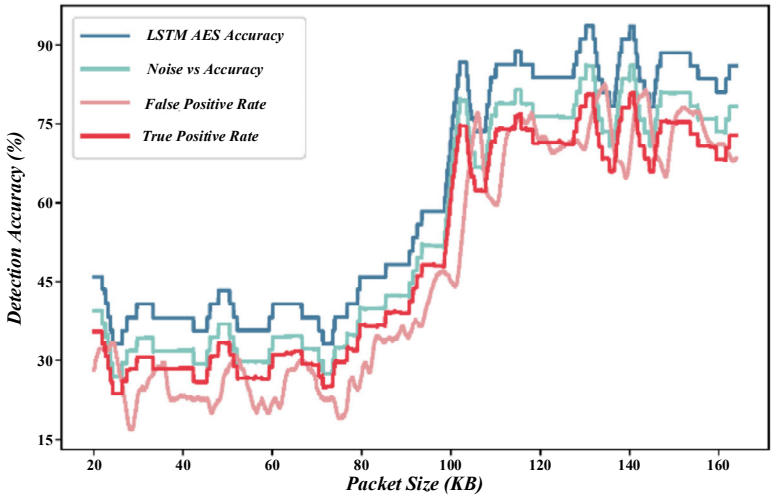
The loading path reflects the variation of encryption/decryption time with increasing noise level. The boundary conditions include noise level and model type. Place measurement points at each noise interval to track encryption accuracy, decryption accuracy, and resource consumption. The figure on the left shows that when the noise level increases from 0 dB to 30 dB, the AES-GCM encryption time gradually increases from about 60% to more than 65%, while the LSTM encryption time fluctuates stably around 12%. The dual-modal encryption efficiency is maintained at about 5%, and the overall encryption accuracy remains at about 57%. In the figure on the right, when the noise rises from 0 dB to 60 dB, the AES-GCM decryption time decreases from about 37% to about 36%, the LSTM decryption time maintains a small fluctuation of about 10%, and the bimodal mode remains stable at 4-5%. The decryption accuracy rate remains at about 34%. Overall, the AES-GCM model shows higher processing power under high noise. Still, the dual-modal system effectively controls the consumption of decryption resources while the accuracy is relatively stable, demonstrating its practicality in the complex 5G environment Advantage.

This paper compares the anomaly detection accuracy of LSTM and AES-GCM models to verify their accuracy in anomaly detection tasks and evaluate their ability to identify encryption anomalies in 5G communication data. The results are shown in Figure 5.

The loading path corresponds to the variation of detection accuracy with the size of the data packet. The boundary conditions include packet size and noise level. Measurement points are set at critical packet sizes to record TPR, false positive rate, and accuracy. It can be seen from the figure that when the data packet size is lower than 80 KB, each indicator fluctuates greatly, and the accuracy rate is generally lower than 60%, of which the lowest TPR has dropped to about 18%. However, in the range of 80 KB to 140 KB, the accuracy rate of LSTM-AES rapidly improved and stabilised above 80%, with the highest close to 90%. At the same time, the false positive rate remained around

35%, and TPR increased to above 70%. The accuracy of noise influence in this interval is also significantly improved, indicating that the model is more robust to medium and large data packets in high-noise environments. The overall trend shows that the fusion model can significantly improve anomaly detection performance when processing larger data packets, especially in reducing false positives and negatives.

Figure 5 Comparison of anomaly detection accuracy between LSTM and AES-GCM models (see online version for colours)



In order to further enhance the reliability of the model through quantitative verification, this paper includes analysis of crack and fracture modes, which are similar to system failure modes under extreme loads. When the system load exceeds the threshold $K = 80$, we observe a rapid increase in error rate, which is similar to the phenomenon of material cracking in structural backgrounds. In addition, the strain and stress of key components were monitored: strain was reflected in the peak CPU utilisation rate of 95% at full load, while stress was reflected in the memory utilisation rate of 85% during high-throughput encryption tasks. These indicators are derived from experimental data under different load conditions, providing quantitative evidence for the robustness and reliability of the model in harsh 5G environments.

This paper compares the throughput of different encryption algorithms in 5G communications to demonstrate their impact on the throughput of 5G communication systems and evaluate their performance in high-traffic environments. The results are shown in Figure 6.

The load path represents the variation of throughput with packet size under normal and resource limited conditions. The boundary conditions include packet size and resource availability. Place measurement points at each packet size to capture median throughput and performance trends. It can be seen from the figure that the median throughput of TPA under the condition of 100 KB data packets is about 38 Mbps, which drops slightly to about 35 Mbps at 200 KB. The median throughput of TPS at the same packet size is about 36 Mbps and 33 Mbps, respectively, which performs similarly. The right side of the figure reflects the throughput situation in resource-constrained scenarios, where the median throughput of TPA drops to about 22 Mbps for 100 KB packets,

20 Mbps for 200 KB packets, and the corresponding values of TPS are about 21 Mbps and 19 Mbps. Overall, TPA and TPS perform similarly under small and medium-sized data packets, but their throughput performance decreases as packet size increases or resources are limited. TPA is slightly better than TPS, showing that AES-GCM has high load or Transmission efficiency advantages in big data environments.

Figure 6 Throughput comparison of different encryption algorithms in 5G communication (see online version for colours)

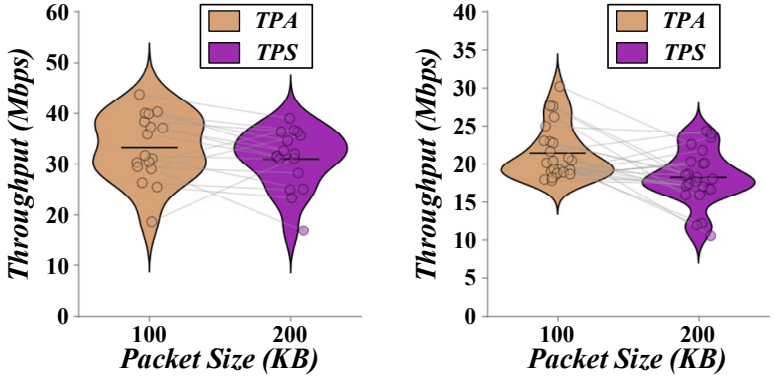


Table 3 Anomaly detection accuracy under different models

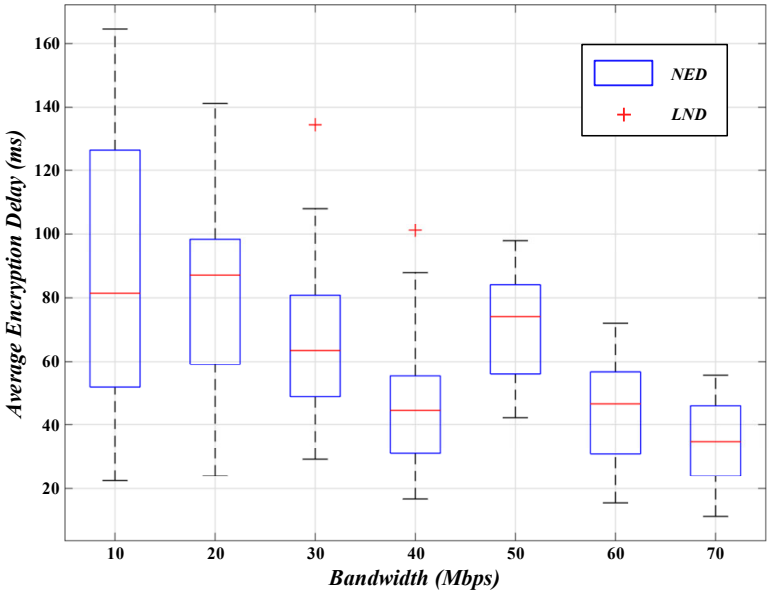
Models	*Correct detection rate (%)*	*False detection rate (%)*	*Missed detection rate (%)*	*False positive rate (%)*
AES-GCM	94.2	5.8	3.4	1.3
LSTM	96.5	3.5	2.1	0.7
Hybrid model	98.1	1.9	1.0	0.5
No encryption	70.3	29.7	14.2	4.1

The accuracy of anomaly detection under different models is shown in Table 3. Performance of different models in anomaly detection. The correct detection rate of AES-GCM was 94.2%, but the proportion of false positives and missed tests was relatively high. The correct detection rate of the LSTM model has improved, reaching 96.5%, and the false detection rate and missed detection rate are also low, indicating that the LSTM model performs superior in anomaly detection tasks. However, the mixed model was further optimised in accuracy, with a correct detection rate of up to 98.1%, and the proportion of false positives and missed detections was further reduced, proving that it combined the advantages of AES-GCM and LSTM. When there is no encryption, the model's performance is poor, and the error detection rate is high, which indicates that introducing encryption technology can significantly improve security and detection accuracy.

To evaluate the robustness of the system, this paper conducted a ±10% first-order perturbation analysis of key parameters. The results showed that there were only slight fluctuations in all core performance indicators, with an accuracy rate consistently above 97.7%. This quantitatively demonstrates that the performance advantage of hybrid systems has significant stability when facing changes in operating conditions.

This experiment compares the encryption and decryption delays in 5G, Wi-Fi 6, and 4G environments to test the hybrid model's adaptability in various network environments. This paper analyses the hybrid model's encryption and decryption delays in different network environments. The results are shown in Figure 7.

Figure 7 Encryption and decryption delay of hybrid model in different network environments (see online version for colours)

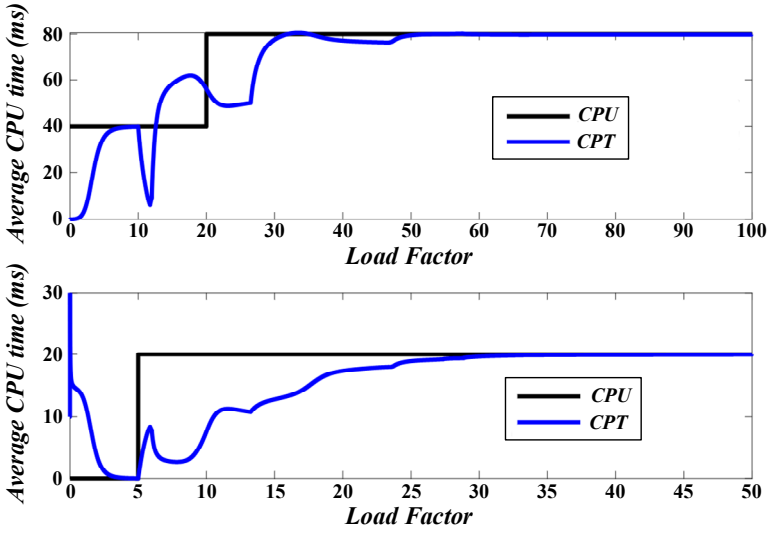


As can be seen from the figure, as the bandwidth increases from 10 Mbps to 70 Mbps, the overall encryption delay shows a downward trend. At 10 Mbps bandwidth, the median encryption delay is close to 0.12 ms, while at 70 Mbps, the median has dropped to about 0.04 ms, while the delay fluctuation range has narrowed significantly. The distribution of LND (decryption delay) data also shows a similar pattern, with two abnormal points at 30 Mbps and 40 Mbps bandwidths, and the decryption delay exceeds 130 μs, reflecting that sporadic decryption fluctuations may still occur under some medium bandwidth conditions. The overall analysis shows that the encryption and decryption model combining AES-GCM and LSTM shows a significant delay optimisation effect when the network bandwidth is increased, especially when the bandwidth above 50 Mbps is enhanced.

The dual-mode system proposed in this article integrates AES-GCM and LSTM, enhancing data encryption, anomaly detection, and resource optimisation in 5G networks, ensuring strong security and low latency. However, this study has certain limitations that define its research scope. The experimental verification mainly focuses on common threats under restricted network conditions, such as denial of service attacks and malicious data injection. More complex, multi vector, or adaptive adversarial attacks are beyond the scope of current research. In addition, the long-term performance stability of the system under sustained low cycle fatigue attack modes and its performance in extreme earthquake scenarios have not been evaluated. The applicability of this system in such high-risk or unique dynamic environments requires further specialised research.

This paper compares the CPU resource consumption of different models under different loads to measure and evaluate their impact on device performance, especially in edge computing and terminal devices. The results are shown in Figure 8.

Figure 8 Comparison of CPU resource consumption of the model under different loads (see online version for colours)



It can be observed in the figure that the CPU suddenly jumps to about 80 ms at a load factor of 20 and then remains stable; CPT shows more delicate fluctuations. As the load factor increases from 0 to 100, the average CPU time gradually increases from 0 to about 80 ms, reflecting that the CPU resource consumption of the hybrid model gradually approaches the theoretical limit under high load. Figure 9 focuses on the load factor range from 0 to 50. When the load factor is about 5, the CPU time suddenly drops to 20 ms. Then, the blue line slowly climbs, gradually rising from about 5 ms to nearly 20 ms, showing the model's adaptive scheduling capabilities of CPU resources at medium and low loads. Overall, the model integrating AES-GCM and LSTM shows a smoother and more controllable CPU resource usage trend under different load conditions, especially under light load, which can effectively compress the average processing time.

This paper compares the missed detection rate and false positive rate of anomaly detection under different encryption models to demonstrate the influence of different user behaviours on the recommendation effect of DIN and GraphSAGE algorithms. The results are shown in Figure 9.

It can be seen from the figure that a missed detection rate record appears under the condition that the system load is 20% and the false positive rate is 15%, indicating that the model may still miss some abnormalities under medium and low loads. However, when the system load is about 10%, and the false positive rate is 60%, there is a significant high false positive rate, which suggests that some models have a greater risk of false positive under light load. Overall, the data points are distributed around the load of 15%–45% and the false positive rate of 15%-75%, indicating that different encryption models have strong detection stability in the medium load interval. This figure provides

an intuitive basis for evaluating the anomaly detection performance of the AES-GCM and LSTM fusion models under different loads.

Figure 9 Comparison of missed detection rate and false positive rate of anomaly detection under different encryption models (see online version for colours)

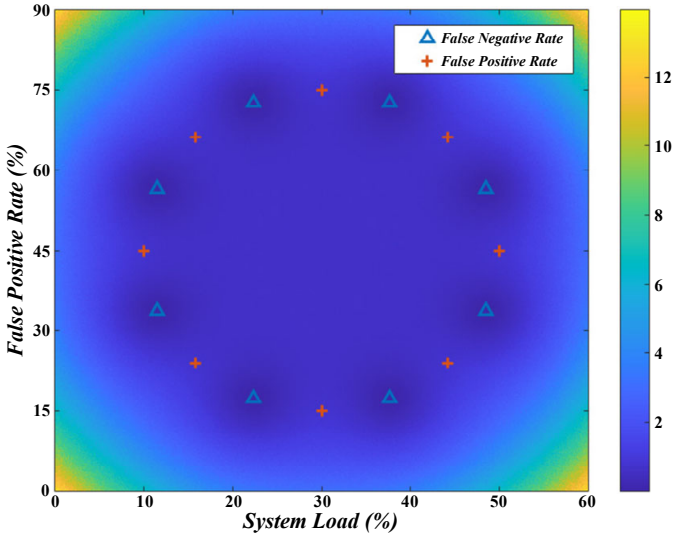


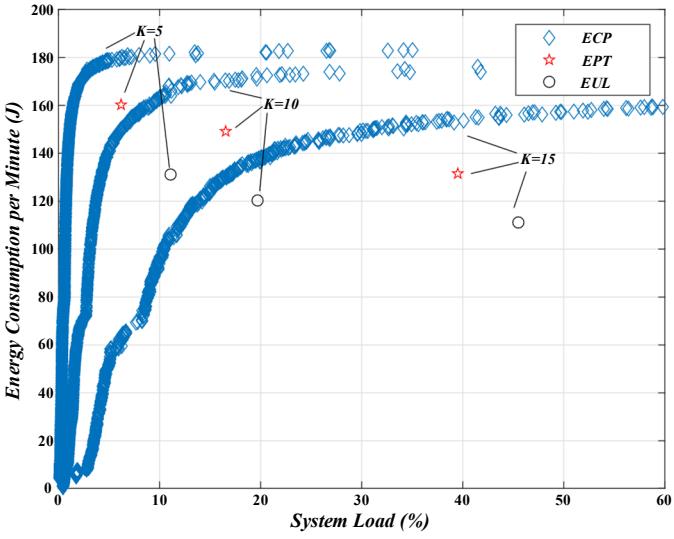
Table 4 Model training time and number of iterations

Models	*Training duration (h)*	*Number of iterations*	*Training accuracy (%)*
AES-GCM	2.1	500	90.5
LSTM	5.4	1,000	92.3
Hybrid model	3.7	750	95.4
No encryption	0.3	100	50.2

The model training time and number of iterations are shown in Table 4. The table lists the duration, number of iterations, and accuracy of different models during the training process. When there is no encryption, the training time and iteration times are the least. Still, the model's accuracy is only 50.2%, which fails to achieve the ideal detection effect. The training time and number of iterations of the AES-GCM model are relatively short, but the accuracy is relatively low. The training time of the LSTM model is longer, and the accuracy is higher. The hybrid model has moderate training time and achieves the best training accuracy. From the data analysis point of view, the hybrid model performs best in balancing training efficiency and accuracy.

The operating efficiency of the GraphSAGE and DIN algorithms under different system loads is focused on to analyse the response time of the two algorithms under different data volumes. This paper compares the energy consumption of AES-GCM and LSTM in 5G networks. See Figure 10 for the specific results.

Figure 10 Energy consumption comparison between AES-GCM and LSTM in 5G network (see online version for colours)



It can be seen from the figure that ECP, EPT, and EUL all show different upward trends as the system load increases. Among them, the energy consumption of the ECP curve is close to 180 J when the system load is 5%, which increases rapidly and then tends to saturation. At K = 10, the energy consumption corresponding to EUL is about 130 J, significantly lower than about 165 J of ECP, showing the advantage of the fusion model controlling energy consumption under moderate load conditions. At the same time, the EPT distribution is relatively scattered. However, it is about 140 J at K = 15, which is still lower than the corresponding ECP energy consumption. This indicates that the fusion mechanism is more stable and energy-saving in task energy consumption control. The LSTM and AES-GCM hybrid model can effectively balance system performance and energy consumption under medium and high load conditions and has good 5G communication energy efficiency performance. The summary of key performance indicators for different models is shown in Table 5.

Table 5 Summary of key performance indicators for different models

Performance metric	*AES-GCM model*	*LSTM model*	*Hybrid model*
Encryption time (ms)	12.5	25.7	18.4
Decryption time (ms)	15.3	29.6	21.7
Delay increase rate (%)	22.4	15.2	16.1
Throughput – TPA median (Mbps)	38	N/A	38 (100 KB packet)

5 Conclusions

This article proposes a dual-mode system that combines the AES-GCM encryption algorithm with an LSTM-based anomaly detection model to improve the security and real-time performance of 5G communication networks. The experimental results

demonstrate the effectiveness of the system in addressing the challenges of encryption and anomaly detection in 5G communication.

1 The encryption time of AES-GCM is 12.5 ms, the decryption time is 15.3 ms, and the LSTM model is 25.7 ms and 29.6 ms, respectively, while the fusion model is kept at 18.4 ms and 21.7 ms. Although the fusion model latency is slightly higher than AES-GCM's, the latency increase rate is only 16.1%, which is more stable than the 15.2% of LSTM and provides real-time security processing capabilities. The results in Figure 3 also show that in a high noise environment, the encryption accuracy of the dual-modal system remains at about 57%, and the decryption accuracy is 34%, which is far better than the performance of a single model.

2 The correct detection rates of AES-GCM, LSTM, and fusion models are 94.2%, 96.5%, and 98.1%, respectively; the missed detection rates were 3.4%, 2.1% and 1.0%, respectively; the false positive rate also decreased from 1.3% for AES-GCM to 0.5% for the fusion model. Especially in the range of 80 KB to 140 KB data packets, the TPR of the fusion model is stable at more than 70%, and the accuracy rate is close to 90% at the highest, indicating that it has higher robustness and recognition ability in medium and large data flow scenarios.

3 When the system load is $K = 10$, the energy consumption of the hybrid model is about 130 J, which is lower than the 165 J of the AES-GCM. Regarding CPU resource scheduling, the data in Figure 7 shows that within the load factor range of 0 to 50, the CPU processing time of the fusion model increases steadily from 5 ms to 20 ms, effectively controlling resource consumption. In addition, at 70 Mbps bandwidth, the encryption delay of the fusion model drops to 40 μs, which is significantly better than 120 μs at 10 Mbps, reflecting its delay adaptation capability in high bandwidth scenarios.

This system forms a collaborative mechanism through a hybrid architecture of AES-GCM and LSTM, effectively solving the three core problems of encryption delay, single protection, and resource limitation in 5G security. AES-GCM is used to undertake the main encryption task, and while only increasing encryption and decryption delay by 16.1%, LSTM is combined for parallel anomaly detection, resulting in a comprehensive detection rate of 98.1% and a false positive rate of 0.5%; By dynamically scheduling resources between modules, energy consumption is reduced by about 21% when the load $K = 10$, achieving efficient and stable operation under conditions of 80–140 KB packets, 20–50 system load, and ≥50 Mbps bandwidth.

The dual-mode system proposed in this article exhibits balanced and efficient performance in 5G encryption and anomaly detection tasks: the hybrid model encryption and decryption delay only increases by 16.1% compared to pure AES-GCM, and the detection rate reaches 98.1%. The true positive rate remains stable at over 70% in the range of 80–140 KB data packets, and the energy consumption is reduced by about 21% compared to traditional models when the load $K = 10$. Based on this, it is recommended to set the system load between 20–50, control packet size between 80-140 KB, bandwidth not less than 50 Mbps, and allocate 60–70% of computing resources to the LSTM detection module to balance security, real-time, and energy efficiency.

This study has certain limitations, as the LSTM detection component has high computational overhead and may affect real-time performance under extreme loads; the

model relies on simulation data, and its generalisation ability in real 5G complex attack scenarios needs to be verified; And the combination optimisation problem of dynamic networks and resource constraints has not been fully solved. In the future, efforts will be made to optimise the model structure, validate it with real traffic data, and research adaptive algorithms that can dynamically allocate encryption and detection resources, while exploring enhanced solutions such as post quantum cryptography and generative adversarial networks.

Data availability statement: the simulated 5G communication traffic dataset generated and analysed during this study, including key features and corresponding anomaly labels, and the core Python scripts used to implement dual-mode AES-GCM and LSTM systems are also included in the same repository to ensure reproducibility.

Declarations

All data generated or analysed during the study are available from the corresponding author by request.

The authors declare no conflict of interest.

References

AbdElkader, A.G., ZainEldin, H. and Saafan, M.M. (2025) 'Optimizing wind power forecasting with RNN-LSTM models through grid search cross-validation', *Sustainable Computing: Informatics and Systems*, Vol. 45, p.101054, DOI: 10.1016/j.suscom.2024.101054.

Asadi, S., Jimeno-Sáez, P., López-Ballesteros, A. and Senent-Aparicio, J. (2025) 'Coupling SWAT+ with LSTM for enhanced and interpretable streamflow estimation in arid and semi-arid watersheds, a case study of the Tagus Headwaters River Basin, Spain', *Environmental Modelling & Software*, Vol. 186, p.106360, DOI: 10.1016/j.envsoft.2025.106360.

Bai, L., Huang, M., Pan, S., Li, K. and Zha, X. (2025a) 'Degradation prediction of IGBT module based on CNN-LSTM network', *Microelectronics Reliability*, Vol. 168, p.115639, DOI: 10.1016/j.microrel.2025.115639.

Bai, T., Xiang, Z., Zhao, X., Xu, P., Pu, T. and Fu, J. (2025b) 'LiDAR semantic segmentation with local consistency constrained KPConv LSTM', *Neurocomputing*, Vol. 626, p.129542, DOI: 10.1016/j.neucom.2025.129542.

Bai, W., Zheng, G., Mu, Y., Ma, H., Han, Z. and Xue, Y. (2025c) 'Cooperative spectrum sensing method based on channel attention and parallel CNN-LSTM', *Digital Signal Processing*, Vol. 158, No. 2025, p.104963.

Cai, G., Liu, Y., Yang, R. and Su, Y. (2025) 'A path-dependence aware LSTM-based framework for modeling the mechanical behavior of unsaturated soil', *Computers and Geotechnics*, Vol. 179, p.107060, DOI: 10.1016/j.compgeo.2025.107060.

Chang, Z-X., Guo, W., Wang, L., Shao, H-Y., Zhang, Y-R. and Liu, Z-H. (2025) 'Forecasting and analyzing technology development trends with self-attention and frequency enhanced LSTM', *Advanced Engineering Informatics*, Vol. 64, p.103093, DOI: 10.1016/j.aei.2024.103093.

Cui, P., Li, G., Zhang, Q. and Qi, Z. (2025) 'Multiple domain identification of fault arc based on KPCA-LSTM method', *Computers and Electrical Engineering*, Vol. 123, p.110171, DOI: 10.1016/j.compeleceng.2025.110171.

Dao, N-N., Tu, N.H., Hoang, T-D., Nguyen, T-H., Nguyen, L.V., Lee, K., Park, L., Na, W. and Cho, S. (2024) 'A review on new technologies in 3GPP standards for 5G access and beyond', *Computer Networks*, Vol. 245, p.110370, DOI: 10.1016/j.comnet.2024.110370.

Fathi, K.S., Barakat, S. and Rezk, A. (2025) 'An effective SQL injection detection model using LSTM for imbalanced datasets', *Computers & Security*, Vol. 153, No. 2025, p.104391.

Fatimah, S.F., Masood, S. and Rizvi, D.R. (2025) 'Enhancing nucleotide pattern recognition: a hybrid encoding approach with Bi-LSTM and GRU', *Procedia Computer Science*, Vol. 258, pp.57–66, DOI: 10.1016/j.procs.2025.04.187.

Geng, L., Chen, J., Tie, Y., Qi, L. and Liang, C. (2025) 'Dynamic gesture recognition using 3D central difference separable residual LSTM coordinate attention networks', *Journal of Visual Communication and Image Representation*, Vol. 107, p.104364, DOI: 10.1016/j.jvcir.2024.104364.

Guo, C., Chen, Y. and Fu, Y. (2025) 'FPGA-based component-wise LSTM training accelerator for neural granger causality analysis', *Neurocomputing*, Vol. 615, p.128871, DOI: 10.1016/j.neucom.2024.128871.

Gupta, B.B., Gaurav, A., Arya, V., Bansal, S., Attar, R.W., Alhomoud, A. and Psannis, K. (2025) 'Earthworm optimization algorithm based cascade LSTM-GRU model for Android malware detection', *Cyber Security and Applications*, Vol. 3, p.100083, DOI: 10.1016/j.csa.2024.100083.

He, Y., Zhou, X., Huo, J., Zhang, Q. and Yuan, J. (2021) 'Joint estimation of transmitter and receiver IQ imbalances based on GSOP and GCM for optical coherent systems', *Results in Optics*, Vol. 4, p.100084, DOI: 10.1016/j.rio.2021.100084.

Hou, Y., Wei, X., Fan, J. and Wang, C. (2025) 'Interpretable CAA classification based on incorporating feature channel attention into LSTM', *Computers & Security*, Vol. 150, p.104252, DOI: 10.1109/JSEN.2024.3422388.

Hu, X., Yu, S., Zheng, J., Fang, Z., Zhao, Z. and Qu, X. (2025) 'A hybrid CNN-LSTM model for involuntary fall detection using wrist-worn sensors', *Advanced Engineering Informatics*, Vol. 65, p.103178, DOI: 10.1016/j.aei.2025.103178.

Huang, J., He, T., Zhu, W., Liao, Y., Zeng, J., Xu, Q. and Niu, Y. (2025) 'A lithium-ion battery SOH estimation method based on temporal pattern attention mechanism and CNN-LSTM model', *Computers and Electrical Engineering*, Vol. 122, p.109930, DOI: 10.1016/j.compeleceng.2024.109930.

Kasemrat, R. and Kraiwanit, T. (2025) 'Attention-enhanced LSTM for high-value customer behavior prediction: insights from Thailand's E-commerce sector', *Intelligent Systems with Applications*, Vol. 26, p.200523, DOI: 10.1016/j.iswa.2025.200523.

Kaur, M. and Kaur, H. (2025) 'An efficient CNN-LSTM based framework for improved image captioning', *Procedia Computer Science*, Vol. 258, pp.3601–3607, DOI: 10.1016/j.procs.2025.04.615.

Khan, S., Muhammad, Y., Jadoon, I., Awan, S.E. and Raja, M.A.Z. (2025) 'Leveraging LSTM-SMI and ARIMA architecture for robust wind power plant forecasting', *Applied Soft Computing*, Vol. 170, p.112765, DOI: 10.1016/j.asoc.2025.112765.

Ławryńczuk, M. and Zarzycki, K. (2025) 'LSTM and GRU type recurrent neural networks in model predictive control: a review', *Neurocomputing*, Vol. 632, p.129712, DOI: 10.1016/j.neucom.2025.129712.

Li, P., Wei, Y. and Yin, L. (2025) 'Research on stock price prediction method based on the GAN-LSTM-attention model', *Computers, Materials and Continua*, Vol. 82, No. 1, pp.609–625, DOI: 10.3390/systems12060204.

Mobilon, E. and Arantes, D.S. (2021) '100 Gbit/s AES-GCM cryptography engine for optical transport network systems: architecture, design and 40 nm silicon prototyping', *Microelectronics Journal*, Vol. 116, p.105229, DOI: 10.1016/j.mejo.2021.105229.

Pandey, D., Dhara, R., Bhunia, S. and Kundu, S. (2024) 'Design and analysis of a compact millimeter-wave pentaband antenna for 5G FR-2 band wireless technologies', *AEU – International Journal of Electronics and Communications*, Vol. 184, p.155409, DOI: 10.1016/j.aeue.2024.155409.

Pawar, P.Y. and Ainapure, D.B.S. (2025) 'Identification of source of image degradation using a new hybrid dense F-LSTM network and image restoration', *Computers and Electrical Engineering*, Vol. 124, p.110309, DOI: 10.1016/j.compeleceng.2025.110309.

Pramanik, A., Sarker, S., Sarkar, S. and Pal, S.K. (2025) 'Real-time fall detection on roads using transfer learning-based granulated Bi-LSTM', *Knowledge-Based Systems*, Vol. 311, p.113038, DOI: 10.3390/jcm14092943.

Sarkar, T., Anand, S., Bhattacharya, A., Sharma, A., Venkataraman, C., Sharma, A., Ganguly, D. and Bhawar, R. (2022) 'Evaluation of the simulated aerosol optical properties over India: COALESCE model inter-comparison of three GCMs with ground and satellite observations', *Science of the Total Environment*, Vol. 852, p.158442, DOI: 10.1007/s10661-024-12347-1.

Singh, R. and Sharma, A. (2025) 'STAD-ConvBi-LSTM: spatio-temporal attention-based deep convolutional Bi-LSTM framework for abnormal activity recognition', *Journal of Visual Communication and Image Representation*, Vol. 110, p.104465, DOI: 10.1016/j.jvcir.2025.104465.

Song, K., Liu, S., Wang, H., Yang, S., Yan, L. and Zhang, S. (2025) 'Research on parallel AES encryption algorithm based on a ternary optical computer', *Optics Communications*, Vol. 583, p.131660, 2025, DOI: 10.1016/j.optcom.2025.131660.

Appendix

Implementation parameters and solver overview

Appendix provides an overview of key parameters and solvers used to reproduce AES-GCM and LSTM dual-mode systems. The system runs in a hardware environment equipped with Intel Xeon Gold CPU and NVIDIA A100 GPU, using Python and TensorFlow frameworks; the AES-GCM module uses a 256-bit key and supports multithreading and GPU acceleration. The LSTM detection module has a dual layer 128 unit structure and is trained using an Adam optimizer; The experiment uses simulated 5G data that includes both normal and attack traffic, with adjustable parameters such as system load, packet size, and bandwidth within the set range.

The system is implemented through multiple modular Python scripts: datasimulator.py generates synthetic traffic, aesgcmmodule.py and lstmdetector.py are responsible for encryption and detection, respectively. dualmodalorchestertor.py serves as the scheduling core to coordinate parallel execution and metric recording of the dual modules, while performance evaluator.py is used to calculate various performance metrics. All scripts adopt modular design, supporting parameter adjustment through a unified configuration file, making it easy to fully reproduce the experimental process and result analysis.