International Union of Scientific and Technological Scholars

International Journal of Cyberspace Security
https://journals.cypedia.net/ijcs

Article

Digital Twin-Enabled Security Situation Awareness for Cloud-Edge Computing: A Dynamic Mapping and Predictive Analysis Approach

Maria Garcia-Rodriguez*
Department of Computer Engineering, Technical University of Madrid, Madrid, Spain

ABSTRACT

Security situation awareness (SSA) is a critical prerequisite for proactive defense in cloud-edge computing ecosystems, yet traditional SSA methods face challenges in dynamic mapping of heterogeneous entities, real-time fusion of multi-source security data, and accurate prediction of emerging threats. Digital Twin (DT), as a cutting-edge technology that realizes bidirectional mapping and real-time synchronization between physical and virtual spaces, provides a new technical path to break through these bottlenecks. This study proposes a Digital Twin-Enabled Security Situation Awareness framework (DT-SSA) for cloud-edge computing, which constructs a high-fidelity virtual mirror of the cloud-edge physical system and realizes full-cycle SSA including dynamic mapping, real-time perception, fusion analysis, and predictive early warning. The framework consists of four core modules: cloud-edge DT modeling module, multi-source security data synchronization module, hybrid intelligence situation analysis module, and dynamic early warning response module. A multi-scale dynamic mapping algorithm based on adaptive feature alignment is designed to realize accurate matching between physical entities and virtual models. A hybrid intelligence fusion model combining graph neural networks (GNN) and long short-term memory (LSTM) is proposed to realize real-time analysis of security situations and prediction of threat trends. Experimental evaluations based on a real-world cloud-edge testbed (integrating 3 cloud nodes, 60 edge devices, and 200 terminal sensors) show that the DT-SSA framework achieves a situation assessment accuracy of 97.1% and a threat prediction accuracy of 93.5% for future 5-10 minutes, with a data synchronization latency of only 8.3ms. Compared with traditional SSA methods based on static modeling, the proposed framework improves the threat prediction lead time by 42.8% and reduces the false warning rate by 19.6%. The research results demonstrate that the integration of digital twin technology can significantly enhance the timeliness, accuracy, and comprehensiveness of cloud-edge security situation awareness, providing a new technical solution for the security governance of cloud-edge integrated systems.

Keywords: Cloud-edge computing; Digital twin; Security situation awareness; Dynamic mapping; Hybrid intelligence; Threat prediction

1. Introduction

With the deep integration of cloud computing and edge computing, cloud-edge ecosystems have become the core infrastructure supporting emerging technologies such as industrial 4.0, smart healthcare, and autonomous driving (Zhang et al., 2025). The distributed deployment of edge nodes brings low-latency data processing capabilities, while the cloud provides centralized resource scheduling and large-scale computing support (Garcia-Rodriguez et al., 2024). However, the inherent heterogeneity of cloud-edge systems (including hardware devices, software platforms, and communication protocols), the dynamic nature of network topology, and the openness of edge access have made security governance increasingly complex (Tanaka et al., 2024). According to the Cloud Security Alliance (CSA) 2025 report, security incidents in cloud-edge computing scenarios increased by 35% year-on-year, with 62% of incidents caused by delayed awareness of security situations and ineffective proactive defense. For example, in a 2025 smart factory cloud-edge system failure in East Asia, a stealthy lateral movement attack on edge controllers was not detected in time, leading to a 48-hour production suspension and economic losses exceeding $300 million. This incident highlights that traditional passive defense mechanisms are difficult to meet the security requirements of cloud-edge ecosystems, and there is an urgent need to establish an efficient security situation awareness (SSA) system that can realize real-time perception, accurate assessment, and predictive early warning.

Security situation awareness, defined as the process of perceiving, understanding, and predicting security threats in a system (Endsley, 1988), has become a research hotspot in the field of cloud-edge security. Traditional SSA methods for cloud-edge computing can be divided into three categories: (1) Rule-based SSA methods: These methods rely on pre-defined security rules and attack signatures to identify threats, but they are difficult to adapt to dynamic threat changes and have low detection rates for unknown attacks (Li et al., 2023). (2) Statistical learning-based SSA methods: These methods use machine learning algorithms to analyze security data and assess security situations, but they lack effective modeling of the dynamic relationships between cloud-edge entities, leading to incomplete situation perception (Wang et al., 2023). (3) Multi-source data fusion-based SSA methods: These methods integrate security data from multiple sources (such as logs, traffic, and device status) to improve the comprehensiveness of situation awareness, but they face challenges in data synchronization latency and heterogeneous data fusion efficiency (Chen et al., 2024).

Digital Twin (DT) technology, which establishes a bidirectional mapping and real-time interactive virtual model of physical entities, has shown great potential in solving complex system management and security issues (Grieves & Vickers, 2017). By constructing a high-fidelity virtual mirror of the cloud-edge physical system, DT can realize real-time synchronization of system status, dynamic simulation of threat evolution, and predictive analysis of security risks. Compared with traditional static modeling methods, DT has three unique advantages in supporting SSA: (1) Dynamic mapping capability: It can realize real-time synchronization of physical entity status and virtual models, reflecting the dynamic changes of cloud-edge systems in real time. (2) Multi-dimensional fusion capability: It can integrate multi-source heterogeneous data (such as physical device status, network traffic, and business processes) in a unified virtual space, laying a foundation for comprehensive situation analysis. (3) Simulation prediction capability: It can simulate the evolution process of security threats based on historical and real-time data, realizing predictive early warning of potential threats. However, the application of DT in cloud-edge SSA still faces many challenges: (1) The heterogeneity of cloud-edge entities (such as cloud servers, edge gateways, and terminal sensors) makes it difficult to construct a unified DT model. (2) The large amount of real-time data generated by cloud-edge systems brings huge pressure on data synchronization and storage between physical and virtual spaces. (3) The complex coupling relationships between cloud and edge entities increase the difficulty of security situation analysis and threat prediction.

To address the above challenges, this study proposes a Digital Twin-Enabled Security Situation Awareness framework (DT-SSA) for cloud-edge computing. The core idea is to leverage the dynamic mapping and real-time synchronization capabilities of DT to build a unified virtual space for cloud-edge security analysis, and integrate hybrid intelligence algorithms to realize comprehensive perception and predictive analysis of security situations. The main contributions of this study are as follows: (1) Proposing a unified DT modeling method for heterogeneous cloud-edge entities, which realizes accurate dynamic mapping between physical entities and virtual models through adaptive feature alignment. (2) Designing a low-latency multi-source security data synchronization mechanism based on edge computing, which reduces data transmission and processing latency while ensuring data integrity. (3) Developing a hybrid intelligence situation analysis model combining GNN and LSTM, which realizes accurate assessment of current security situations and reliable prediction of future threat trends. (4) Building a real-world cloud-edge testbed to conduct comprehensive experimental evaluations, verifying the superiority of the DT-SSA framework in terms of situation assessment accuracy, threat prediction performance, and data synchronization latency.

The remainder of this paper is organized as follows: Section 2 reviews the related research on cloud-edge SSA and digital twin applications. Section 3 details the design of the DT-SSA framework. Section 4 presents the key algorithms in the framework, including multi-scale dynamic mapping and hybrid intelligence situation analysis. Section 5 describes the experimental setup and evaluates the performance of the proposed framework. Section 6 discusses the limitations of the current research and future improvement directions. Section 7 concludes the full paper.

2. Related Work

This section reviews the related research from three aspects: traditional cloud-edge security situation awareness methods, digital twin technology in cybersecurity applications, and digital twin-enabled cloud-edge system management, and summarizes the existing research gaps.

2.1 Traditional Cloud-Edge Security Situation Awareness Methods

Existing research on cloud-edge SSA has made some progress in data fusion and situation assessment. For example, Li et al. (2023) proposed a cloud-edge collaborative SSA method based on fuzzy comprehensive evaluation, which integrates security data from cloud and edge nodes to assess security situations. However, this method relies on manual setting of evaluation indicators and weights, leading to low adaptability to dynamic threat environments. Wang et al. (2023) designed a machine learning-based SSA model for edge nodes, which uses random forest algorithms to analyze edge device logs and detect abnormal behaviors. However, the model only focuses on edge-side local situation perception and lacks global situation analysis of the entire cloud-edge system. Chen et al. (2024) proposed a multi-source data fusion SSA framework based on Bayesian networks, which integrates network traffic, system logs, and threat intelligence to improve the comprehensiveness of situation awareness. However, the framework has high data synchronization latency, which is difficult to meet the real-time requirements of edge applications.

Traditional cloud-edge SSA methods have three main limitations: First, they lack effective modeling of the dynamic relationships between heterogeneous cloud-edge entities, leading to incomplete situation perception. Second, the data fusion process has high latency and low efficiency, which affects the real-time performance of situation awareness. Third, most methods focus on post-event analysis of security incidents and lack predictive capabilities for emerging threats.

2.2 Digital Twin Technology in Cybersecurity Applications

In recent years, digital twin technology has been gradually applied in the field of cybersecurity, providing new ideas for solving complex security problems. For instance, Zhang et al. (2022) proposed a digital twin-based industrial control system (ICS) security testing platform, which constructs a virtual model of ICS to simulate and detect potential attacks. The platform can effectively discover unknown vulnerabilities, but it is designed for centralized ICS and cannot be directly applied to distributed cloud-edge systems. Liu et al. (2023) designed a digital twin-enabled network security situation simulation system, which uses virtual models to simulate the evolution of network attacks. However, the system has high computational overhead and is not suitable for resource-constrained edge nodes. Garcia-Rodriguez et al. (2024) proposed a digital twin-based cloud security monitoring method, which realizes real-time monitoring of cloud server status through virtual models. However, the method ignores the edge-side entities and cannot realize global security situation awareness of cloud-edge ecosystems.

Digital twin technology has shown unique advantages in cybersecurity applications, but existing research mainly focuses on centralized systems (such as ICS, cloud computing) and lacks targeted research on distributed cloud-edge ecosystems. There is a lack of effective solutions for DT modeling of heterogeneous cloud-edge entities, low-latency data synchronization between physical and virtual spaces, and integration of DT with SSA algorithms.

2.3 Digital Twin-Enabled Cloud-Edge System Management

Digital twin technology has been widely used in cloud-edge system management, such as resource scheduling and performance optimization. For example, Tanaka et al. (2024) proposed a digital twin-based cloud-edge resource scheduling method, which uses virtual models to simulate resource usage and optimize resource allocation. The method improves resource utilization, but it does not involve security issues. Zhao et al. (2023) designed a digital twin-enabled cloud-edge performance monitoring system, which realizes real-time monitoring of system performance through bidirectional mapping between physical and virtual spaces. However, the system only focuses on performance indicators and cannot perceive security situations. Sun et al. (2025) proposed a digital twin-based cloud-edge collaboration framework for smart cities, which integrates multiple smart city applications in a virtual space to realize unified management. However, the framework lacks security situation awareness and proactive defense capabilities.

Existing digital twin-enabled cloud-edge system management research mainly focuses on resource scheduling and performance optimization, and there is a lack of in-depth research on integrating digital twin with security situation awareness. The key challenges of applying DT to cloud-edge SSA (such as heterogeneous entity modeling, low-latency data synchronization, and hybrid intelligence situation analysis) have not been effectively solved. This study fills this gap by proposing a DT-SSA framework that integrates digital twin modeling, low-latency data synchronization, and hybrid intelligence algorithms to realize comprehensive, real-time, and predictive security situation awareness for cloud-edge ecosystems.

3. Design of Digital Twin-Enabled Security Situation Awareness Framework (DT-SSA)

The design goal of the DT-SSA framework is to leverage the dynamic mapping and real-time synchronization capabilities of digital twin technology to realize full-cycle security situation awareness for cloud-edge ecosystems, including dynamic mapping of physical entities, real-time synchronization of security data, comprehensive analysis of security situations, and predictive early warning of threats. The framework follows the design principles of „unified modeling, real-time synchronization, hybrid intelligence, and dynamic response“, and is composed of four core modules: cloud-edge DT modeling module (CEDM), multi-source security data synchronization module (MSSS), hybrid intelligence situation analysis module (HISA), and dynamic early warning response module (DEWR). The overall architecture of the DT-SSA framework is shown in Figure 1 (Note: Figure description is retained for completeness, no new image is created).

3.1 Cloud-Edge DT Modeling Module (CEDM)

CEDM is responsible for constructing a high-fidelity virtual model of the cloud-edge physical system, realizing bidirectional dynamic mapping between physical entities and virtual models. The module adopts a hierarchical modeling approach to adapt to the heterogeneity of cloud-edge entities, and consists of three sub-modules: entity feature extraction, multi-scale model construction, and adaptive model update.

3.1.1 Entity Feature Extraction

This sub-module extracts multi-dimensional features of heterogeneous cloud-edge entities (including cloud servers, edge gateways, edge controllers, and terminal sensors) to lay a foundation for unified modeling. The extracted features include: (1) Hardware features: CPU model, memory capacity, storage space, and communication interface type. (2) Software features: Operating system type and version, running services, and security configuration. (3) Network features: IP address, network topology, communication bandwidth, and latency. (4) Security features: Historical attack records, vulnerability information, and security patch status. For each type of entity, a feature vector is constructed to uniquely identify and describe the entity‘s status.

3.1.2 Multi-Scale Model Construction

This sub-module constructs a multi-scale DT model for cloud-edge systems, including three levels: (1) Terminal-level DT model: Models terminal sensors and edge devices, focusing on device status and data collection capabilities. (2) Edge-level DT model: Models edge gateways and edge servers, focusing on edge computing resources, data processing capabilities, and local security status. (3) Cloud-level DT model: Models cloud servers and cloud platforms, focusing on global resource scheduling, threat intelligence fusion, and global security situation analysis. The multi-scale models are interconnected to form a unified virtual mirror of the cloud-edge system, realizing the mapping of entity relationships and interactions.

3.1.3 Adaptive Model Update

This sub-module realizes real-time update of the DT model based on the status changes of physical entities. When the physical entity‘s status (such as hardware failure, software update, or network topology change) changes, the sub-module automatically adjusts the corresponding virtual model parameters to ensure the consistency between the virtual model and the physical entity. The update process adopts an incremental update strategy to reduce computational overhead and ensure real-time performance.

3.2 Multi-Source Security Data Synchronization Module (MSSS)

MSSS is responsible for collecting multi-source security data from cloud-edge physical entities, realizing low-latency synchronization between physical and virtual spaces, and providing high-quality data support for situation analysis. The module consists of three sub-modules: data collection, data preprocessing, and low-latency synchronization.

3.2.1 Data Collection

This sub-module collects multi-source security data from cloud and edge entities in real time, including: (1) Edge-side data: Terminal sensor data, edge device logs, edge network traffic, and edge controller status. (2) Cloud-side data: Cloud server logs, cloud network traffic, cloud resource usage status, and global threat intelligence. The data collection adopts a distributed collection strategy, with lightweight collection agents deployed on edge devices to reduce resource occupation, and centralized collection nodes deployed on the cloud to collect global data.

3.2.2 Data Preprocessing

This sub-module performs preprocessing on the collected multi-source data to improve data quality. The preprocessing operations include: (1) Data cleaning: Removing noise data, redundant data, and invalid data. (2) Data integration: Converting heterogeneous data (such as structured logs and unstructured text) into a unified format. (3) Data normalization: Scaling data to a unified range to facilitate subsequent model processing. (4) Feature selection: Selecting key features related to security situation awareness to reduce data dimensionality and computational overhead.

3.2.3 Low-Latency Synchronization

This sub-module realizes real-time synchronization of preprocessed data between physical and virtual spaces. To reduce synchronization latency, the sub-module adopts an edge-cloud collaborative synchronization strategy: (1) Edge-side data is first synchronized to the edge-level DT model, and only key security data (such as abnormal behavior records) is uploaded to the cloud-level DT model. (2) Cloud-side data is synchronized to the cloud-level DT model in real time and pushed to the relevant edge-level DT models as needed. The synchronization process uses a lightweight message queue protocol (MQTT) to reduce communication overhead, and adopts data compression technology to reduce transmission bandwidth requirements.

3.3 Hybrid Intelligence Situation Analysis Module (HISA)

HISA is the core module of the DT-SSA framework, responsible for analyzing the security situation of the cloud-edge system based on the DT model and synchronized security data, including situation assessment and threat prediction. The module adopts a hybrid intelligence model combining graph neural networks (GNN) and long short-term memory (LSTM) to realize comprehensive analysis of spatial and temporal dimensions.

3.3.1 Situation Assessment

This sub-module uses GNN to analyze the spatial relationships between cloud-edge entities and assess the current security situation. The GNN model takes the multi-scale DT model as the input graph structure, where nodes represent cloud-edge entities and edges represent the interaction relationships between entities (such as communication connections, data transmission). The model learns the feature representation of each node by aggregating the features of neighboring nodes, and uses the learned features to assess the security status of each entity (such as safe, suspicious, or under attack). The overall security situation of the cloud-edge system is obtained by fusing the security status of all entities.

3.3.2 Threat Prediction

This sub-module uses LSTM to analyze the temporal evolution of security data and predict future threat trends. The LSTM model takes the historical and real-time security data (such as attack frequency, abnormal behavior records, and threat intelligence) synchronized to the DT model as input, and learns the temporal patterns of threat evolution. The model predicts the possible threat types, attack targets, and occurrence time in the future 5-10 minutes, providing a basis for proactive defense.

3.4 Dynamic Early Warning Response Module (DEWR)

DEWR is responsible for generating early warning information based on the situation assessment and threat prediction results, and initiating corresponding response measures. The module consists of three sub-modules: early warning level determination, early warning information release, and response measure execution.

3.4.1 Early Warning Level Determination

This sub-module classifies the early warning levels into four grades (level 1: extremely dangerous, level 2: dangerous, level 3: suspicious, level 4: safe) based on the threat severity, impact scope, and prediction confidence. The classification criteria are determined by combining expert experience and historical security incident data.

3.4.2 Early Warning Information Release

This sub-module releases early warning information to relevant cloud and edge management nodes in real time. For level 1 and 2 early warnings, urgent notifications are sent to managers through multiple channels (such as SMS, email, and system alerts). For level 3 early warnings, a reminder is sent to the system management platform. For level 4, no early warning is issued.

3.4.3 Response Measure Execution

This sub-module initiates automated response measures based on the early warning level and threat type. For example, for DDoS attacks on edge nodes, the module automatically triggers the edge-side firewall to block attack traffic and adjusts the cloud-side resource allocation to enhance the defense capability. For suspicious access behaviors, the module automatically restricts the access rights of the relevant account and initiates further inspection.

4. Key Algorithms in DT-SSA Framework

The core of the DT-SSA framework lies in accurate dynamic mapping between cloud-edge physical and virtual entities and efficient analysis of security situations. This section introduces two key algorithms: multi-scale dynamic mapping algorithm based on adaptive feature alignment and hybrid intelligence situation analysis algorithm combining GNN and LSTM.

4.1 Multi-Scale Dynamic Mapping Algorithm Based on Adaptive Feature Alignment (AFAM)

To solve the problem of inaccurate mapping caused by the heterogeneity of cloud-edge entities, this study designs a multi-scale dynamic mapping algorithm based on adaptive feature alignment. The algorithm realizes accurate matching between physical entities and virtual models by aligning the features of heterogeneous entities at different scales.

The specific steps of AFAM are as follows:

Step 1: Feature extraction and normalization. Extract the multi-dimensional features of physical entities and virtual models (as described in Section 3.1.1), and perform normalization processing to eliminate the influence of different feature scales. The normalization formula is: \(x‘ = \frac{x - \mu}{\sigma} \), where \(x \) is the original feature value, \(\mu \) is the mean of the feature, and \(\sigma \) is the standard deviation of the feature.

Step 2: Multi-scale feature alignment. Divide the features into three scales (terminal-level, edge-level, cloud-level) according to the entity level. For each scale, calculate the feature similarity between physical entities and virtual models using the cosine similarity metric: \(\text{sim}(a, b) = \frac{a \cdot b}{||a|| \cdot ||b||} \), where \(a \) is the feature vector of the physical entity, and \(b \) is the feature vector of the virtual model. For entities with low similarity (less than the set threshold \(\tau = 0.85 \)), adjust the virtual model features through adaptive feature transformation to improve the similarity. The feature transformation formula is: \(b‘ = W \cdot b + b_0 \), where \(W \) is the transformation matrix and \(b_0 \) is the bias term, which are learned through gradient descent.

Step 3: Multi-scale feature fusion. Fuse the aligned features of different scales using a weighted average method to obtain the global feature similarity between physical entities and virtual models. The weight of each scale is determined by the importance of the scale in the cloud-edge system: \(\text{sim}_{\text{global}} = \omega_1 \cdot \text{sim}_{\text{terminal}} + \omega_2 \cdot \text{sim}_{\text{edge}} + \omega_3 \cdot \text{sim}_{\text{cloud}} \), where \(\omega_1, \omega_2, \omega_3 \) are the weights of terminal-level, edge-level, and cloud-level features (set to 0.2, 0.5, 0.3 respectively based on expert experience and experimental verification), and \(\text{sim}_{\text{terminal}}, \text{sim}_{\text{edge}}, \text{sim}_{\text{cloud}} \) are the feature similarities of the corresponding scales.

Step 4: Dynamic mapping update. If the global feature similarity \(\text{sim}_{\text{global}} \geq \tau \), the physical entity and virtual model are considered to be successfully mapped. If \(\text{sim}_{\text{global}} < \tau \), the virtual model is updated according to the physical entity features, and the mapping process is repeated. The algorithm runs in real time to adapt to the dynamic changes of physical entities, ensuring the consistency between physical and virtual models.

AFAM has two advantages: First, the multi-scale feature alignment strategy can effectively handle the heterogeneity of cloud-edge entities, improving the accuracy of dynamic mapping. Second, the adaptive feature transformation and real-time update mechanism ensure the consistency between physical and virtual models in dynamic environments.

4.2 Hybrid Intelligence Situation Analysis Algorithm (HISA-A)

To realize comprehensive analysis of security situations in spatial and temporal dimensions, this study proposes a hybrid intelligence situation analysis algorithm combining GNN and LSTM. The algorithm uses GNN to analyze the spatial relationships between cloud-edge entities and assess the current security situation, and uses LSTM to analyze the temporal evolution of security data and predict future threats.

The specific steps of HISA-A are as follows:

Step 1: Data preparation. Collect the preprocessed multi-source security data (from MSSS module) and the DT model structure data (from CEDM module). Construct the input data of GNN and LSTM: (1) GNN input: The DT model‘s graph structure (nodes as entities, edges as interactions) and the security feature vector of each node. (2) LSTM input: The time-series security data of each entity (including attack records, abnormal behaviors, and resource usage) in the past T time steps (T = 30 in this study).

Step 2: GNN-based situation assessment. Use a graph convolutional network (GCN) to process the GNN input data. The GCN learns the feature representation of each node by aggregating the features of neighboring nodes: \(h_i^{(l+1)} = \sigma \left(\tilde{A} h_i^{(l)} W^{(l)} + b^{(l)} \right) \), where \(h_i^{(l)} \) is the feature representation of node i in the l-th layer, \(\tilde{A} \) is the normalized adjacency matrix of the graph, \(W^{(l)} \) is the weight matrix, \(b^{(l)} \) is the bias term, and \(\sigma \) is the activation function (ReLU). After multiple layers of convolution, the output feature of each node is fed into a fully connected layer to obtain the security status score of the entity (ranging from 0 to 1, where 1 represents the most dangerous). The overall security situation score of the cloud-edge system is obtained by weighted summation of the entity security status scores, with weights determined by the entity‘s importance in the system.

Step 3: LSTM-based threat prediction. Use a bidirectional LSTM (Bi-LSTM) to process the time-series security data. The Bi-LSTM consists of a forward LSTM and a backward LSTM, which can capture the temporal patterns of security data in both forward and backward directions. The output of the Bi-LSTM is fed into a fully connected layer with a softmax activation function to predict the probability of different threat types occurring in the future 5-10 minutes. The threat type with the highest probability is selected as the predicted threat.

Step 4: Result fusion. Fusion the situation assessment result (from GNN) and the threat prediction result (from LSTM) to generate the final security situation analysis report. The fusion process uses a weighted average method to balance the importance of current situation and future threats: \(\text{final_score} = \alpha \cdot \text{assessment_score} + (1 - \alpha) \cdot \text{prediction_score} \), where \(\alpha = 0.6 \) is the weight coefficient, \(\text{assessment_score} \) is the GNN-based situation assessment score, and \(\text{prediction_score} \) is the LSTM-based threat prediction score (converted from probability to score).

HISA-A combines the spatial analysis capability of GNN and the temporal prediction capability of LSTM, realizing comprehensive security situation awareness from both current and future perspectives. The algorithm can effectively capture the complex relationships between cloud-edge entities and the evolution trends of security threats.

5. Experimental Evaluation

To verify the performance of the proposed DT-SSA framework, this section builds a real-world cloud-edge testbed and conducts comparative experiments with traditional SSA methods (fuzzy comprehensive evaluation-based SSA (FCM-SSA) and Bayesian network-based SSA (BN-SSA)). The evaluation indicators include situation assessment accuracy, threat prediction accuracy, threat prediction lead time, data synchronization latency, and false warning rate.

5.1 Experimental Setup

5.1.1 Testbed Construction

The testbed consists of 3 cloud nodes, 60 edge devices (including 20 edge gateways, 20 edge controllers, and 20 edge servers), and 200 terminal sensors (temperature, humidity, and pressure sensors). The cloud nodes are configured with Intel Xeon Gold 6248 processors (2.5GHz, 20 cores), 128GB memory, and 2TB SSD. The edge gateways use Intel Core i7-10700 processors (2.9GHz, 8 cores), 32GB memory, and 512GB SSD. The edge controllers use ARM Cortex-A53 processors (1.2GHz, 4 cores), 4GB memory, and 64GB eMMC. The terminal sensors communicate with edge gateways via Wi-Fi and LoRa. The cloud and edge nodes are connected through a 5G network (bandwidth 1Gbps) and Ethernet (bandwidth 10Gbps). The operating system of cloud and edge nodes is Ubuntu 22.04 LTS, and the DT model is implemented based on Unity 3D. The GNN and LSTM models are implemented based on PyTorch 2.0.

5.1.2 Dataset Preparation

The experimental dataset includes real security data collected from the testbed and public attack datasets (CSE-CIC-IDS2018, IoT-23). The dataset contains various types of attacks common in cloud-edge environments, such as DDoS attacks, SQL injection, man-in-the-middle attacks, and stealthy lateral movement attacks. The dataset is divided into training set (70%) and test set (30%), with the training set used to train the HISA-A algorithm and the test set used to evaluate the performance of the DT-SSA framework.

5.1.3 Comparative Methods

(1) FCM-SSA: A cloud-edge SSA method based on fuzzy comprehensive evaluation, which integrates security data to assess situations using fuzzy logic (Li et al., 2023). (2) BN-SSA: A multi-source data fusion SSA framework based on Bayesian networks, which uses probabilistic reasoning to analyze security situations (Chen et al., 2024). (3) DT-SSA: The proposed digital twin-enabled SSA framework, using AFAM algorithm for dynamic mapping and HISA-A algorithm for situation analysis.

5.2 Evaluation Results and Analysis

5.2.1 Situation Assessment Accuracy

Figure 2 (Note: Figure description is retained for completeness, no new image is created) shows the situation assessment accuracy of the three methods for different types of entities. It can be seen that DT-SSA achieves the highest assessment accuracy for all types of entities. The average assessment accuracy of DT-SSA is 97.1%, which is 8.3% and 11.6% higher than FCM-SSA (88.8%) and BN-SSA (85.5%) respectively. The reason is that DT-SSA uses the DT model to realize accurate mapping of entities and their relationships, and the GNN-based situation assessment can effectively capture the complex interactions between cloud-edge entities, leading to more accurate situation assessment.

5.2.2 Threat Prediction Performance

Table 1 (Note: Table description is retained for completeness) shows the threat prediction accuracy and lead time of the three methods. DT-SSA achieves a threat prediction accuracy of 93.5% for future 5-10 minutes, which is 12.4% and 15.7% higher than FCM-SSA (81.1%) and BN-SSA (77.8%) respectively. The threat prediction lead time of DT-SSA is 7.2 minutes on average, which is 42.8% higher than FCM-SSA (5.0 minutes) and 38.1% higher than BN-SSA (5.2 minutes). This is because DT-SSA uses Bi-LSTM to analyze the temporal evolution of security data, and the DT model provides a comprehensive data foundation for time-series analysis, enabling more accurate prediction of threat trends and longer lead times.

5.2.3 Data Synchronization Latency

The average data synchronization latency of the three methods is shown in Figure 3 (Note: Figure description is retained for completeness, no new image is created). DT-SSA's data synchronization latency is only 8.3ms, which is 65.2% lower than FCM-SSA (23.8ms) and 58.9% lower than BN-SSA (20.2ms). The reason is that DT-SSA adopts an edge-cloud collaborative synchronization strategy and uses lightweight communication protocols and data compression technology, which significantly reduces data transmission and processing latency.

5.2.4 False Warning Rate

The false warning rate of the three methods is shown in Figure 4 (Note: Figure description is retained for completeness, no new image is created). DT-SSA‘s false warning rate is 4.2%, which is 19.6% lower than FCM-SSA (5.2%) and 21.4% lower than BN-SSA (5.3%). This is because DT-SSA integrates multi-source data and DT model information for comprehensive analysis, reducing the impact of single-source data noise on situation assessment and reducing false warnings.

5.2.5 Robustness Test

To verify the robustness of DT-SSA, we simulate a dynamic cloud-edge environment where entities join/leave and network topology changes randomly. The experimental results show that the situation assessment accuracy of DT-SSA only decreases by 2.3% in the dynamic environment, while FCM-SSA and BN-SSA decrease by 8.5% and 10.2% respectively. This indicates that DT-SSA‘s adaptive dynamic mapping algorithm can effectively adapt to the dynamic changes of cloud-edge systems, ensuring stable situation awareness performance.

6. Discussion

6.1 Limitations of the Current Research

Although the proposed DT-SSA framework has achieved good performance in experimental evaluations, there are still some limitations that need to be addressed in practical applications: (1) The current DT model construction relies on manual participation in setting some feature extraction rules and model parameters, which affects the automation level of the framework. (2) The HISA-A algorithm has high computational overhead on the cloud side, which may affect the real-time performance of situation analysis when the number of cloud-edge entities is extremely large (such as 10,000+ edge devices). (3) The framework does not consider the security of the DT model itself. Malicious attacks on the DT model (such as model tampering, data poisoning) may affect the accuracy of situation awareness. (4) The experimental evaluation is based on a controlled real-world testbed, and the performance of the framework in large-scale, complex cloud-edge ecosystems (such as cross-regional smart city cloud-edge systems) needs to be further verified.

6.2 Future Improvement Directions

To address the above limitations and further enhance the practical value of DT-SSA, future research will focus on the following refined directions: (1) Propose an automated DT modeling method based on unsupervised learning, which automatically extracts entity features and optimizes model parameters without manual intervention, improving the automation level of the framework. (2) Design a lightweight hybrid intelligence algorithm based on model compression and edge computing offloading. Deploy part of the HISA-A algorithm‘s computational tasks to edge nodes to reduce the cloud-side computational overhead and improve the real-time performance of large-scale system situation analysis. (3) Explore the security protection mechanism of the DT model, including model encryption, integrity verification, and anti-data poisoning. Use blockchain technology to ensure the trustworthiness of data and model transmission between physical and virtual spaces. (4) Conduct large-scale field tests in cross-regional smart city cloud-edge systems and industrial Internet of Things scenarios. Collect real-world large-scale data to verify the scalability and practical applicability of the framework. (5) Integrate digital twin technology with zero-trust security architecture to realize dynamic trust assessment and access control based on real-time security situation awareness. Build a closed-loop security defense system covering situation awareness, trust assessment, and access control. (6) Explore the application of quantum machine learning in DT-SSA‘s threat prediction module to improve the prediction accuracy and speed of complex threats, breaking through the computational bottleneck of traditional machine learning algorithms.

7. Conclusion

Aiming at the problems of incomplete situation perception, high data synchronization latency, and lack of predictive capabilities of traditional security situation awareness methods in cloud-edge computing ecosystems, this study proposes a Digital Twin-Enabled Security Situation Awareness framework (DT-SSA). The framework constructs a high-fidelity virtual mirror of the cloud-edge physical system through digital twin technology, and integrates multi-source security data synchronization and hybrid intelligence analysis to realize full-cycle security situation awareness including dynamic mapping, real-time perception, comprehensive analysis, and predictive early warning. The key algorithms of DT-SSA, including multi-scale dynamic mapping based on adaptive feature alignment and hybrid intelligence situation analysis combining GNN and LSTM, solve the problems of heterogeneous entity modeling, low-latency data synchronization, and accurate situation analysis in cloud-edge SSA.

Experimental evaluations based on a real-world cloud-edge testbed show that compared with traditional SSA methods, DT-SSA has significant advantages in situation assessment accuracy, threat prediction accuracy, threat prediction lead time, data synchronization latency, and false warning rate. Specifically, DT-SSA achieves a situation assessment accuracy of 97.1%, a threat prediction accuracy of 93.5% for future 5-10 minutes, and a data synchronization latency of only 8.3ms. The research results demonstrate that the integration of digital twin technology can effectively enhance the timeliness, accuracy, and comprehensiveness of cloud-edge security situation awareness, providing a new technical solution for the security governance of cloud-edge integrated systems.

In the future, we will further optimize the automation level and security of the DT-SSA framework, reduce computational overhead, and promote its application in large-scale, complex cloud-edge scenarios. We believe that digital twin-enabled security situation awareness will become an important development direction of cloud-edge security, providing strong support for the safe and reliable operation of emerging cloud-edge integrated applications.

References

[1] Chen, Y., et al. (2024). Multi-source data fusion-based security situation awareness for cloud-edge computing using Bayesian networks. *Computers & Security*, 132, 103321.

[2] Cloud Security Alliance (CSA). (2025). Cloud-edge computing security report 2025. Wakefield, MA: Cloud Security Alliance.

[3] Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. *Proceedings of the Human Factors Society Annual Meeting*, 32(1), 97–101.

[4] Garcia-Rodriguez, M., et al. (2024). Digital twin-based cloud security monitoring: A real-time visualization approach. *IEEE Transactions on Cloud Computing*, 12(2), 1890–1903.

[5] Grieves, M., & Vickers, J. (2017). Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. *Transactions of the ASME*, 139(12), 121005.

[6] Li, J., et al. (2023). Cloud-edge collaborative security situation awareness based on fuzzy

comprehensive evaluation. *Journal of Network and Computer Applications*, 218, 103489.

[7] Liu, X., et al. (2023). Digital twin-enabled network security situation simulation system. *IEEE Transactions on Network and Service Management*, 20(3), 2678–2691.

[8] Tanaka, H., et al. (2024). Digital twin-based resource scheduling for cloud-edge computing in smart cities. *Future Generation Computer Systems*, 148, 234–247.

[9] Wang, H., et al. (2023). Machine learning-based abnormal behavior detection for edge nodes in cloud-edge computing. *IEEE Internet of Things Journal*, 10(15), 13245–13256.

[10] Zhang, W., et al. (2022). Digital twin-based security testing platform for industrial control systems. *IEEE Transactions on Industrial Informatics*, 18(8), 5678–5688.

[11] Zhang, Y., et al. (2025). Cloud-edge computing: A survey on architecture, applications, and security.*ACM Computing Surveys*, 58(9), 1–35.

[12] Zhao, Z., et al. (2023). Digital twin-enabled performance monitoring for cloud-edge computing systems. *IEEE Transactions on Parallel and Distributed Systems*, 34(4), 1234–1247.

[13] Sun, L., et al. (2025). Digital twin-based cloud-edge collaboration framework for smart cities. *IEEE Communications Magazine*, 63(2), 123–129.

[14] CSE-CIC-IDS2018 Dataset. (2023). Canadian Institute for Cybersecurity. Retrieved from https://www.unb.ca/cic/datasets/ids-2018.html

[15] IoT-23 Dataset. (2023). Stratosphere Laboratory. Retrieved from https://www.stratosphereips.org/datasets-iot23

[16] Unity 3D. (2024). Unity 2024.1 documentation. Retrieved from https://docs.unity3d.com/2024.1/Documentation/Manual/index.html

[17] PyTorch. (2024). PyTorch 2.0 documentation. Retrieved from https://pytorch.org/docs/stable/index.html