Electronic Research Archive

ERA, 32(2): 1380–1405.
DOI: 10.3934/era.2024064
Received date: 17 November 2023
Revised date: 16 January 2024
Accepted date: 24 January 2024
Published date: 02 February 2024

https://www.aimspress.com/journal/ERA

Research article

Multi-cloud resource scheduling intelligent system with endogenous security

Nishui Cai* and Guofeng He

Institute of Security Technology, China Telecom Research Institute, B23, China Telecom Information Park, Shanghai 310000, China

* **Correspondence:** Email: cainishui@chinatelecom.cn; Tel: +08618918588808.

Abstract: A secure and reliable intelligent multi-cloud resource scheduling system in cyberspace is especially important in some industry applications. However, this task has become exceedingly challenging due to the intricate nature of information, the variety of knowledge representations, the compatibility of diverse knowledge reasoning engines, and the numerous security threats found in cloud networks. In this paper, we applied the endogenous security theory to the multi-cloud resource scheduling intelligent system and presented a novel model of the system. The proposed model incorporates various knowledge representations and inference engines, resulting in a multi-cloud resource scheduling intelligent system that ensures endogenous security. In addition, we have devised a scheme for an intelligent system that schedules multi-cloud resources using dual-channels and has an endogenous security mechanism, which we have named Dynamic, Heterogeneous, and Redundant (DHR). Finally, we have used the multi-cloud resource scheduling intelligent run log database to carry out numerous experiments to validate the efficiency of the dual-channel redundant reasoning system with the endogenous security mechanism's DHR property. The results of the experiment demonstrated that the multi-cloud resource intelligent scheduling system model with an endogenous security mechanism was superior to the current single-channel inference system scheme in regards to security and reliability.

Keywords: multi-cloud resource scheduling; intelligent system; endogenous security; AI algorithm; rule-based reasoning; system reliability

1. Introduction

In the existing application domain of intelligent systems for multi-cloud resource scheduling in cyberspace, academia and industry are mainly concerned with efficiently realizing information processing and knowledge reasoning. However, the number of published system vulnerabilities is increasing [1], and cyberspace system failures and disruptions caused by exploited vulnerabilities may have catastrophic consequences for those affected. Once information processing and knowledge reasoning systems are exploited by attackers due to known or unknown vulnerabilities, the effectiveness of information processing and knowledge reasoning is greatly reduced. Therefore, we need an information processing and knowledge reasoning methodology that improves the efficiency of information processing and knowledge reasoning while guarding against a variety of known and unknown risks and vulnerabilities. Nazir et al. [2] have investigated a number of tools and techniques for mining system vulnerabilities. However, there is no method to mine and discover all unknown system risks and vulnerabilities in information processing and knowledge reasoning systems.

The theory of endogenous security in cyberspace [3] may be able to solve the above problems. The root of the cyberspace security problem lies in the insufficient consideration of security requirements in architecture design, which needs to be solved by designing architectures with their own security attributes and security capabilities.

This paper is the first to apply endogenous security theory to a multi-cloud resource scheduling intelligent system. Due to the polymorphic nature of the information processed by the system, its information can be resolved into multiple knowledge representations, such as meta-knowledge, rule-knowledge, instance-knowledge, artificial intelligence (AI) model feature-knowledge, etc., which leads to the natural polymorphism of the information knowledge representations, and different forms of knowledge representations require compatible knowledge reasoning subsystems. Therefore, our first-of-its-kind multi-cloud resource intelligent scheduling system architecture should be endogenously secure due to the mechanism we call Dynamic, Heterogeneous, and Redundant (DHR). We propose an endogenously secure, multi-channel redundant approach and system for intelligent scheduling of multi-cloud resources. The system has three distinctive features (DHR): First, redundancy (R), the four parallel intelligent reasoning channels of the system have redundancy to ensure that while one reasoning channel is processing in a working state, the other is in a backup standby state; second, heterogeneity (H), each of the reasoning systems and inference machines of these four channels also have different knowledge representations, and the heterogeneity increases the difficulty of the attacker; third, dynamism (D), the system has a dynamic immune ability—when the intelligent reasoning channel in the work process encountered external threats using known or unknown system vulnerabilities to attack the failure, one of the standby reasoning channels will be timely transformed into a normal working state, while loading security components to repair the failed channel, to ensure that the system always has the ability to self-heal.

The main contributions of this work are as follows:

First, a system model of endogenous security knowledge reasoning has been designed. It provides a polymorphic knowledge representation of the information to be processed and multiple knowledge reasoning methods, which are separately compatible.

Second, we have developed a dual-channel redundant endogenous security knowledge reasoning system application plan utilizing rule-based and algorithmic reasoning techniques based on AI models to meet the needs of intelligent scheduling for multi-cloud resources.

Finally, we carried out experiments on the DHR characteristics of the multi-cloud resource intelligent scheduling system that we have designed. The findings indicate that the endogenous security DHR characterization implemented in our application scheme is effective and significantly enhances system reliability.

The paper is structured as follows: Section 2 presents an overview of related research and Section 3 introduces a knowledge reasoning system model with endogenous secure DHR features featuring multiple channels and a methodology for assessing system reliability. Then, Section 4 systematically outlines the practical design of application scenarios for an intelligent scheduling system in multi-cloud resource management with endogenous security. Section 5 details the research methodology and analysis while interpreting the results. Finally, Section 6 summarizes the findings of the paper.

2. Related work

2.1. Multi-cloud resource scheduling intelligent system

In the area of multi-cloud resource scheduling, a range of scheduling approaches and techniques has emerged. Yang et al. presented a multi-population competition-cooperation-based scheduling of field service resources in cloud manufacturing [4]. Meanwhile, Sun et al. put forth an efficient, cost-effective and energy-saving multiple workflow scheduling in hybrid clouds [5]. Zhou et al. introduced a scalable genetic algorithm based on heuristic local search for multidimensional resource scheduling in cloud computing [6]. Agarwal et al. analyzed the scheduling of multiprocessor tasks in fog cloud computing using a multi-objective hybrid genetic algorithm [7]. Zhang et al. utilized an extended multi-factor evolutionary algorithm to propose personalized demand-driven multi-task scheduling in cloud manufacturing [8]. Xiong et al. presented a successful adaptive adjustment model for scheduling tasks and allocating resources in cloud manufacturing that is based on the interests of various stakeholders [9]. Zhang et al. examined scheduling of multiple tasks in cloud remanufacturing systems that incorporate reuse, reprocessing, and replacement while factoring in quality uncertainty [10]. Wang et al. proposed decomposition-based multi-objective evolutionary algorithms for the joint scheduling of virtual machines and tasks in cloud computing within the data space [11].

A key technology for intelligent scheduling of multi-cloud resources is the knowledge reasoning system, and its associated techniques and methods are continually undergoing innovation. Wu et al. proposed a neural symbol inference method employing dynamic knowledge partitioning technology [12], while Wang et al. suggested a set method for the diagnosis of mechanical faults under unbalanced conditions using DenseNet and evidence reasoning rules [13]. Gao et al. conducted an analysis of a method for managing the health of mechanical equipment. The method is based on improved intuitive fuzzy entropy and case-based reasoning technology [14]. Fard et al. introduced a hybrid method of geographic information systems and evidence reasoning for selecting sustainable waste power plant sites [15]. Xu et al. proposed a new online optimization method for boiler combustion systems based on data-driven technology and case-based reasoning principles [16]. Kalhori et al. introduced a novel fuzzy inference method of interval 2 type for classification systems. This method is grounded on the normal form of possibility-based fuzzy metrics [17]. Wang et al. proposed a task recommendation technique that integrates multi-perspective social relationship learning and reasoning in mobile crowd perception systems [18]. Xu et al. evaluated a new approach to online combustion optimization for boilers. The technique combines dynamic modeling, multi-objective optimization, and improved case-based reasoning [19]. Yadav et al. presented a hybrid method using behavioral reasoning theory [20]. Zhang et al. proposed a warning method based on fuzzy evidence reasoning, which takes into account heterogeneous information [21]. Zhao et al. have introduced a method of spatial case-based reasoning for the assessment of regional landslide risk. In a similar vein, Long et al. have proposed a parameterized extended case-based reasoning approach based on functional foundations to enable automatic experiential reasoning in mechanical product design [22,23]. Finally, Chen et al. have analyzed a decision-making method using logical reasoning to handle qualitative knowledge [24]. Wang and Gao proposed a method for evidence localization in digital forensics, utilizing a case-based variable scale reasoning approach [25]. Cercone et al. highlighted the advantages of a hybrid architecture incorporating rule induction and case-based reasoning [26]. Sottara et al. introduced a configurable Rete-OO engine able to infer various types of incomplete information [27]. Cao et al. conducted an analysis of the interpretability of expert systems employing belief rules [28]. Guo et al. formulated a multi-layer case-based reasoning approach for intricate product systems [29].

In brief, the prevailing method for knowledge reasoning is the expert system. It utilizes a set of rules to quantify the information obtained from expert interviews. The logical reasoning mechanism then processes this rule set, generating prompts, predictions or advice as appropriate. Several approaches exist to logical reasoning mechanisms, including fuzzy logic. The technique providing the most apt response to data is termed case-based reasoning. It is a learning and reasoning strategy that stores events and compares them.

An alternative knowledge reasoning methodology lies in machine learning, deep learning, and reinforcement learning applied to various types of neural networks. Ouache et al. have introduced a framework founded on evidence reasoning and machine learning for assessing and forecasting human-caused fire accidents [30]. Kierner et al. presented a classification system for hybrid architectures, which integrate rule-based reasoning and machine learning in clinical decision-making systems [31]. Bride et al. examined the fundamentals of high-performance machine learning for logical reasoning and verification [32]. Chen et al. introduced recursive inference based on training time for machine learning [33]. Bellomarini et al. proposed a knowledge graph with machine learning and reasoning capabilities [34]. Namvar et al. introduced a method for integrating intelligent reasoning into machine learning development [35]. Krüger et al. put forth an interpretable machine learning method for predicting student dropout rates [36], while Gao et al. presented a deep learning method based on evidence reasoning rules [37]. Liu and Qian have conducted an investigation of knowledge graph inference through reinforcement learning in the context of aluminum alloy applications [38]. Meanwhile, Muslim et al. have introduced a reinforcement learning-based framework for offloading computing services in both edge and core cloud environments [39].

2.2. Endogenous security issues and theory

Endogeneity means that one or more explanatory variables in the system model are correlated with the random perturbation term. If all the explanatory variables are X_i and the random perturbation u_i, endogeneity can be expressed as: $cov(u_i, X_i) \neq 0$.

Endogenous problems prevail in the field of cyberspace security [3]. Endogenous security (ES) issues of multi-cloud resource scheduling and reasoning systems include functional security issues and information security issues. Functional security concerns pertain to any impairment of a system's expected function (EF), while information security concerns include incidents of information leakage, tampering, and similar occurrences. In addition to knowledge reasoning EFs, knowledge reasoning systems have associated visible side effect functions (VSEFs) or invisible dark functions (IDFs). When a VSEF is detected, a security patch is used. However, security patches themselves can have new security problems. In summary, whenever a knowledge-based reasoning EF is performed, there must be a VSEF or an IDF.

Ahmad et al. conducted an overview of the security challenges and solutions in 5G [40], while Hu et al. presented a meticulously designed framework for network security defense [41]. Nevertheless, the inherent security issue of intelligently scheduling multi-cloud resources remains unresolved.

The proposed theoretical model by Wu for endogenous security assurance in cyberspace not only provides protection from identified security risks, but also shields against unknown threats and attacks [3]. The essence of endogenous security lies in the DHR mechanism, which selects groups of actuators dynamically from heterogeneous and redundant ones. This not only fulfils the expected system functions, but also adds uncertainty for adversaries. The system's structure and operation mechanism guarantee its reliability and make it more difficult for attackers to carry out effective attacks.

The knowledge reasoning system program's evaluation method can draw reference from both the system reliability theory and engineering applications' practical experience [3]. The varied forms of information knowledge representation, including meta-knowledge, rule knowledge, case knowledge, and artificial intelligence model knowledge, combined with the diverse knowledge reasoning methods and redundancy of parallel reasoning architecture design, constitute the fundamental characteristics of multi-channel knowledge reasoning systems with endogenous safety. These features form the basis for calculating system reliability.

To address the endogenous security issue of the decision-making system used in scheduling multi-cloud resources, the intelligent reasoning system architecture for multi-cloud resource scheduling has been designed with the application of endogenous security theory.

3. Endogenous security model and reliability of reasoning systems in multi-cloud resource scheduling

3.1. Causes of endogenous security issues of reasoning systems in multi-cloud resource scheduling

The EF of a multi-cloud resource scheduling intelligent system is to safely and reliably process and transmit cloud network resource scheduling information and cloud network data streams to realize the knowledge reasoning function. However, as shown in Figure 1, there are different VSEFs in addition to the existence of IDFs. Due to the existence of meta-knowledge, rule-knowledge, instance-knowledge, AI model-knowledge, etc., natural polymorphic knowledge reasoning represented by information knowledge is characterized by time-varying, heterogeneity, and redundancy in cloud network resource scheduling intelligence. At the same time, the knowledge polymorphism of reasoning system intelligent resource scheduling in cloud network data stream security and network transmission of cloud network resource scheduling information also leads to predictable VSEFs such as difficulty in knowledge representation of complex information data, inappropriate matching of knowledge representation with inference engine type, and abnormal results when inference engine handles unknown boundary conditions.

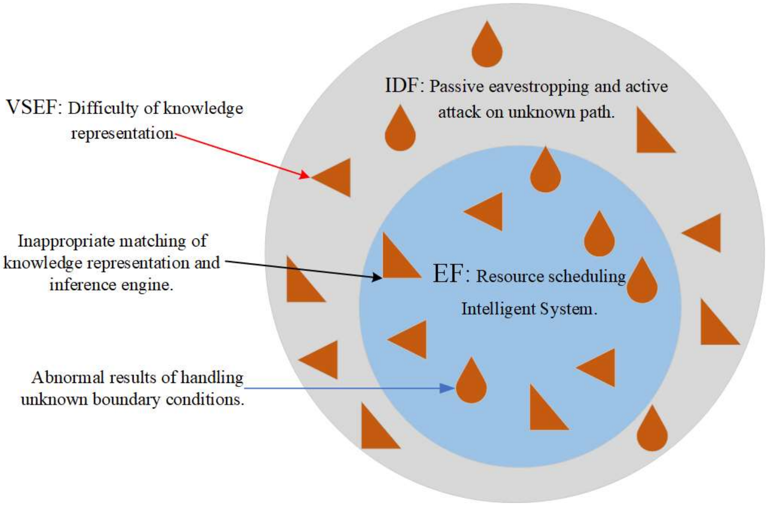
IDF: Passive eavestropping and active attack on unknown path.
VSEF: Difficulty of knowledge representation.
Inappropriate matching of knowledge representation and inference engine.
EF: Resource scheduling Intelligent System.
Abnormal results of handling unknown boundary conditions.

Figure 1. Causes of reasoning system ES issues.

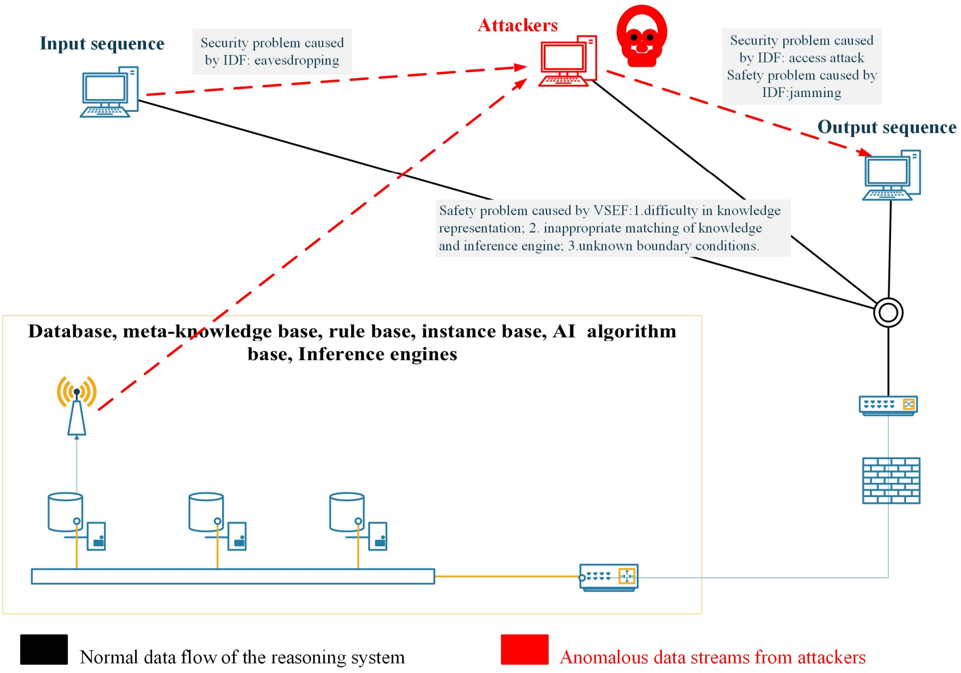
Input sequence
Security problem caused by IDF: eavesdropping
Attackers
Security problem caused by IDF: access attack Safety problem caused by IDF:jamming
Output sequence
Safety problem caused by VSEF:1.difficulty in knowledge representation; 2. inappropriate matching of knowledge and inference engine; 3.unknown boundary conditions.
Database, meta-knowledge base, rule base, instance base, AI algorithm base, Inference engines
■ Normal data flow of the reasoning system
🟥 Anomalous data streams from attackers

Figure 2. The ES issues of a reasoning system in multi-cloud resource scheduling.

There are two reasons for the endogenous security problem of reasoning systems in data flow security, as shown in Figure 2. On one hand, it refers to the polymorphism, naturalness and human interference in the knowledge representation of the information data to be processed. Since the multi-path effect of intelligent scheduling of cloud network resources starts from the knowledge representation of scheduling information, it will reach different knowledge inference systems through many different paths such as meta-knowledge, rule-based knowledge, case-based knowledge, and AI model-based knowledge. We expect to build a multi-level inference system where the raw information data to be processed will converge in a more accurate and reasonable way in the multi-level inference system through a number of accessible paths. However, the information processing paths with different accessibility are different, and the knowledge representation of the information data to be processed may be uncertain. Therefore, this VSEF can also be called the predictable side effect function of path selection. On the other hand, an attacker who receives a signal from an unknown path eavesdrops on it or launches an attack. This is an artificial security attack on the IDF in the integrated resource scheduling path of the cloud network. The occurrence of the above VSEFs and IDFs will surely bring endogenous security problems to the multi-cloud resource scheduling inference system.

3.2. Endogenous security model for reasoning systems

The endogenous security model of the inference system, demonstrated in Figure 3, comprises four layers of distinct inference engines.

- Heterogeneous 1. Principle-based reasoning system based on meta knowledge includes meta knowledge data representation: raw data, data elements, element parameters; and principle reasoning system: axiom of business, business formula, business rules.
- Heterogeneous 2. Rule-based reasoning system based on expert knowledge includes expert knowledge data representation: business rule characteristic, rule characteristic parameters; and rule reasoning system: business rules, rule-based reasoning.
- Heterogeneous 3. Case-based reasoning system includes business case data representation: case structure characteristic, structural characteristic parameters; and case-based reasoning system: successful instances, case-based reasoning.
- Heterogeneous 4. AI algorithm reasoning system based on machine learning includes data representation of machine learning model: AI model characteristic, model characteristic parameters; and AI algorithm reasoning: AI algorithm, AI algorithm reasoning.

The principle-based reasoning system based on meta knowledge is the most basic reasoning method and can be used in both rule-based reasoning and case-based reasoning, while rule-based reasoning can be used in case-based reasoning. The feature characteristic parameters representation of business knowledge in all the above reasoning systems is uniform.

The elements of the heterogeneous redundancy reasoning systems set L with 4 reconfigurable equivalent multi-clod resource scheduling function F are equal to 15 and are the sum of the combinations in C_4^n,where $n \in (1,2,3,4)$.

For reasoning scenario elements j (j = 1, 2, 3, 4), i.e., meta-knowledge-based reasoning, rule-knowledge-based reasoning, instance-knowledge-based reasoning, and AI algorithm-based reasoning, design flaws or loopholes are allowed to exist that are different in nature (patterns of differences) from the other elements in the set L.

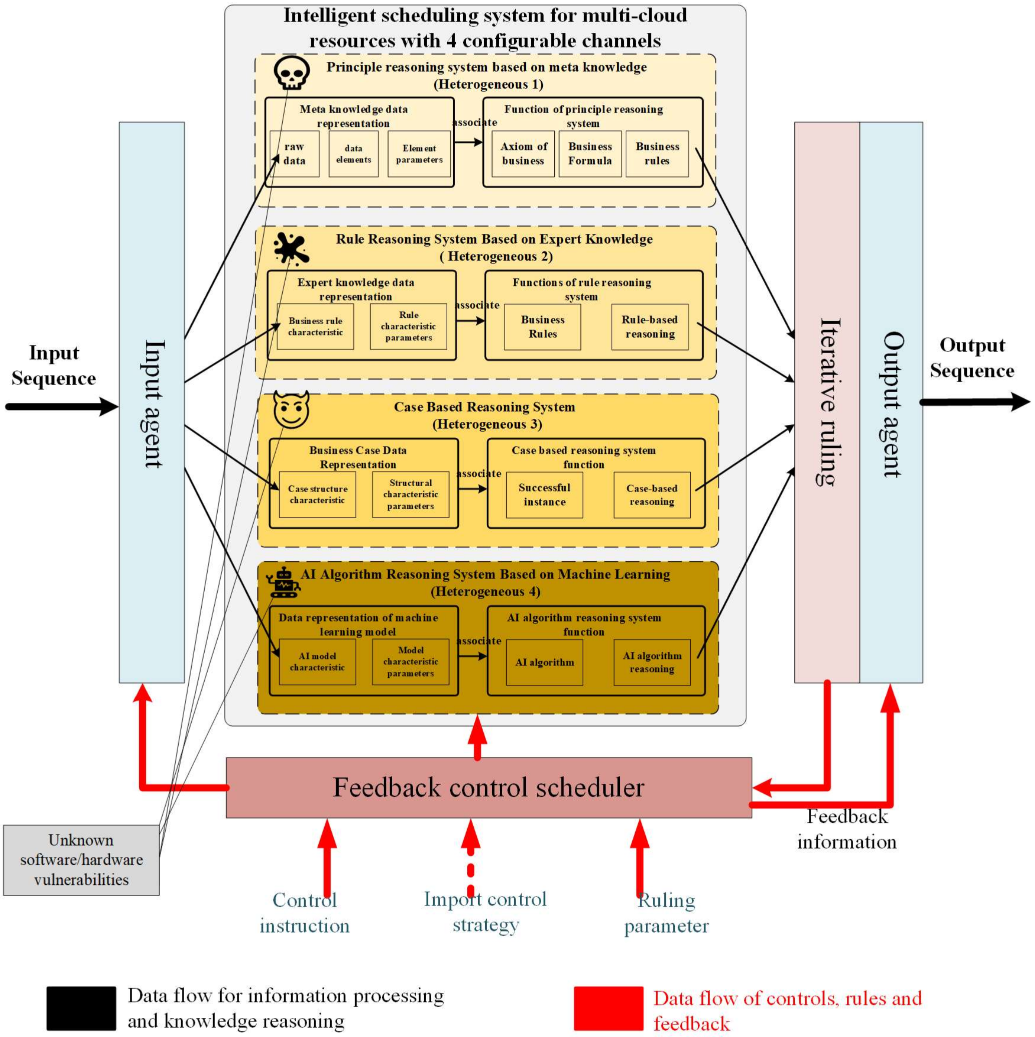
Intelligent scheduling system for multi-cloud resources with 4 configurable channels
Principle reasoning system based on meta knowledge (Heterogeneous 1)
Meta knowledge data representation
raw data
data elements
Element parameters
associate
Function of principle reasoning system
Axiom of business
Business Formula
Business rules
Rule Reasoning System Based on Expert Knowledge (Heterogeneous 2)
Expert knowledge data representation
Business rule characteristic
Rule characteristic parameters
associate
Functions of rule reasoning system
Business Rules
Rule-based reasoning
Case Based Reasoning System (Heterogeneous 3)
Business Case Data Representation
Case structure characteristic
Structural characteristic parameters
associate
Case based reasoning system function
Successful instance
Case-based reasoning
AI Algorithm Reasoning System Based on Machine Learning (Heterogeneous 4)
Data representation of machine learning model
AI model characteristic
Model characteristic parameters
associate
AI algorithm reasoning system function
AI algorithm
AI algorithm reasoning
Input Sequence
Input agent
Iterative ruling
Output agent
Output Sequence
Feedback control scheduler
Feedback information
Unknown software/hardware vulnerabilities
Control instruction
Import control strategy
Ruling parameter
Data flow for information processing and knowledge reasoning
Data flow of controls, rules and feedback

Figure 3. Endogenous security model for reasoning systems in multi-cloud resource scheduling.

The workflow of the intelligent system for multi-cloud resource scheduling is as follows: the requirement for multi-cloud resource scheduling is entered from the input sequence of the system. The input agent then uniformly analyzes and consolidates the data to form representations of meta knowledge data, expert knowledge data, business instance data, and machine learning model data. According to the endogenous security mechanism, the default selection strategy of the dynamic heterogeneous reasoning system is utilized to invoke the relevant dynamic heterogeneous reasoning system. The output agent of the system generates the reasoning results of the output sequence and completes the self-learning case of the knowledge system.

When faced with a sudden security threat, the immune response system is triggered automatically. This, alongside the activation of other heterogeneous reasoning systems, is designed to maintain the normal functioning of the system and achieve a redundant backup immune effect.

3.3. Reliability assessment methods for endogenous security reasoning systems in multi-cloud resource scheduling

The following is a quantitative analysis and comparison of the reliability of single channel modules and multi-redundant channel modules.

Due to uncertain internal resource depletion or external threat attacks, we assume that the failure events of the channel units included in the system follow an exponential distribution.

Fault density function:

$$f(t) = \lambda e^{-\lambda t} \tag{1}$$

Unreliability:

$$F(t) = 1 - e^{-\lambda t} \tag{2}$$

Reliability:

$$R(t) = 1 - F(t) = e^{-\lambda t} \tag{3}$$

Failure rate:

$$\lambda(t) = \frac{f(t)}{R(t)} = \lambda \tag{4}$$

Mean time between failures:

$$MTBF = \frac{1}{\lambda} \tag{5}$$

According to the definition and reliability logic diagram of a parallel system, its unreliability mathematical model is:

$$F_s(t) = \prod_{i=1}^{n} F_i(t) \tag{6}$$

where $F_s(t)$ represents the system's unreliability, and $F_i(t)$ represents the ith unit's unreliability.

Set the failure rates of the two channel modules as λ_1 and λ_2. The unreliability can be obtained by using the following formulas:

$$F_1(t) = 1 - e^{-\lambda_1 t}$$

$$F_2(t) = 1 - e^{-\lambda_2 t}$$

According to Eq (6), the unreliability of the dual redundant module composed of two channel modules is:

$$F_s(t) = \prod_{i=1}^{2} F_i(t) = F_1(t) * F_2(t) = \left(1 - e^{-\lambda_1 t}\right) * \left(1 - e^{-\lambda_2 t}\right) = 1 - e^{-\lambda_1 t} - e^{-\lambda_2 t} + e^{-(\lambda_1 t + \lambda_2 t)} \quad (7)$$

According to Eq (3), the reliability of dual redundancy module is:

$$R_s(t) = 1 - F_s(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 t + \lambda_2 t)} \quad (8)$$

In particular, when the control module and task management module adopt the same redundancy in the dual redundancy design, namely $\lambda_1 = \lambda_2 = \lambda$. According to Eq (8), the reliability of dual redundancy module is:

$$R_s(t) = 2e^{-\lambda t} - e^{-2\lambda t} \quad (9)$$

Assuming that the mean time between failures (MTBF) of the single channel module is 20000 h, it can be seen from Eq (5) that the failure rate of the single channel module is

$$\lambda_{p1} = \frac{1}{MTBF} = 0.00005.$$

According to Eq (3), the reliability of the single channel module for 2000 hours is

$$R_{p1}(t) = e^{-\lambda_{p1} t} = 0.9048.$$

According to Eq (9), the reliability of the dual redundant channel module for 2000 hours is

$$R_{p2}(t) = 2e^{-\lambda_{p1} t} - e^{-2\lambda_{p1} t} = 0.9909.$$

Table 1. List of the reliability of endogenous security reasoning systems in different redundant channels.

Working hours	Single channel	Dual channels	Three channels	Four channels
20,000	0.3678	0.6004	0.7474	0.8403
16,000	0.4493	0.6968	0.8330	0.9080
12,000	0.5488	0.7964	0.9082	0.9586
8000	0.6703	0.8913	0.9642	0.9882
4000	0.8187	0.9671	0.9940	0.9989
2000	0.9848	0.9909	0.9991	0.9999

Table 1 lists the reliability of endogenous security reasoning systems in different redundant channels. It can be seen that the reliability of the system can be greatly improved after the multi-redundant channel design is adopted, that is, the task reliability of the system has been greatly improved.

4. Designing an endogenous security reasoning system in multi-cloud resource scheduling

4.1. Data flow security protection system

4.1.1. Security capability component classification and grading

Based on the security industry experience and with reference to the information security technology related standards, the security components in the cloud network system can be categorized and graded. The system security protection level, security layering and security capability components correspond to the following Table 2.

Table 2. Security component classification hierarchy list.

Security level	Security layer	Security capability component
2	Terminal	Terminal virus defense
2	Data	Data identification
2	Data	Document encryption
2	Application	Website content monitoring
2	Application	Web page tamper proof (extranet)
2	Cloud	WAF (internet outlet)
2	Cloud	VPN
2	Cloud	Firewall (FW)
2	Cloud	Fortress machine
2	Cloud	Vulnerability scanning
2	Network	Mobile malicious program
2	Network	Network abnormal traffic monitoring
2	Network	Flow direction monitoring
2	Network	Online log retention
2	Network	Stiff wood creep detection
2	Network	Unrecorded website detection
2	Network	Domain name information security management
2	Network	Spam message interception
2	Network	IDC/ISP
3	Terminal	Terminal access management
3	Terminal	Terminal data leakage prevention
3	Data	Data desensitization
3	Data	Database audit
3	Data	Network DLP
3	Data	Data encryption
3	Application	Unified access (4A)
3	Application	Mobile app shell

Continued on next page

Security level	Security layer	Security capability component
3	Application	Code audit
3	Cloud	IPS (internet outlet)
3	Cloud	WAF (intranet outlet)
3	Cloud	Anti-Virus Gateway
3	Cloud	Honeypot system (extranet)
3	Cloud	Full flow (extranet)
3	Network	DNS
4	Terminal	Enterprise terminal leakage prevention
4	Data	Data destruction
4	Application	Web page tamper proof (intranet)
4	Application	Mimicry defense
4	Cloud	Host protection
4	Cloud	Honeypot system (intranet)
4	Cloud	Full flow (intranet)
4	Network	Attack traceability

4.1.2. Changes in security components for data flowing through different levels of protection

The cloud network data flow environment needs to focus on the security components that need to be changed as the data flows through different levels of protection.

A function of data flow security protection level adjustment related components can be designed. Referring to Table 2.

- Adjustments must be made to security level 3 components when there is data flow between protection level 2 and protection level 3.
- Adjustments to security level 4 components are necessary when transferring data between protection level 3 and protection level 4.
- When data flows between protection level 2 and protection level 4, it is necessary to adjust security level 3 and 4 components.

4.2. Data flow security for multi-cloud resource scheduling

The main strategies are:

- Private cloud resources offer better security value compared to public and industry clouds.
- When deciding between industry and public cloud options, consider the economic impact of billing costs.
- It is important to note that different clouds offer varying degrees of data security. Choose the most appropriate security assurance capabilities according to your needs.
- The varying cloud usage methods have different reliability and resource utilization benefits, thus it’s crucial to opt for the one that offers optimal reliability and resource utilization benefits.

These principles are also the basis for reasoning rules and also for selecting the feature space when using AI algorithms as shown in Table 3.

Table 3. Attribute characteristics of multi-cloud resource scheduling.

Symbols	Attribute Name	Supplementary note
C_1, C_2, C_{pub}, C_{pri}	Name of cloud	Indicate the first and second public cloud, public cloud, and private cloud, respectively.
C_{maxvol}	Maximum cloud storage capacity	
C_{used}	Cloud storage space assigned	
C_{rem}	Remaining cloud storage space	
$C_{occratio}$	Cloud storage space utilization	
C_{cat}	Classification of clouds	Common cloud classifications include public, private and industry clouds.
C_{eco}	Cloud economics metrics	
C_{sec}	Security capability levels for the Cloud	For example, information security assurance level protection level 2, level 3 and level 4.
C_{perf}	Integrated performance of cloud usage	Cloud usage performance and reliability
C_{dem}	Cloud space demanded	Cloud space to be allocated
C_{demsec}	Cloud space demanded security level	Security level of cloud space to be allocated
C_{sch}	Cloud selected for scheduling	

Main reasoning rules are shown in Table 4.

Table 4. Main reasoning rules.

No.	Name of rule	Rule application process
Rule 1	Private cloud first	In multi-cloud resource scheduling, if C_{pub} and C_{pri} are public and private clouds respectively, then private cloud C1 is selected first. $C_{sch} = C_{pri}$
Rule 2	Choose a cloud with lower operating costs first	In multi-cloud resource scheduling, if C_1, C_2 are both public clouds, and C_1 is more low-cost than C_2, then C1 is selected first. $C_{sch} = C_1$
Rule 3	Cloud with higher security level first	In multi-cloud resource scheduling, if C_1, C_2 are both public clouds, and C_1 is higher security level than C_2, then C1 is selected first. $C_{sch} = C_1$cc
Rule 4	First choose the cloud with higher overall performance	In multi-cloud resource scheduling, if C_1, C_2 are both public clouds, and C_1 is higher overall performance than C_2, then C1 is selected first. $C_{sch} = C_1$

Based on the size of data storage space and data flow security protection level division of existing multiple cloud networks, with the help of cloud network security components, the intelligent scheduling of multiple cloud network resources is carried out according to the user's cloud network data space size and security protection level requirements.

4.3. Endogenous security models for reasoning systems tailored to application scenarios

We customize the endogenous security model of the inference system based on the application scenario of cloud network resource scheduling in data flow security. Since the number of heterogeneous redundant knowledge reasoning functions is 2, the endogenous secure dual-channel multi-cloud resource scheduling intelligent reasoning system model, as shown in Figure 4, has a set of three different reasoning system scenarios with three different reasoning elements: rule-based reasoning scenarios, AI algorithmic reasoning scenarios, and scenarios with both rule-based reasoning and AI algorithmic reasoning.

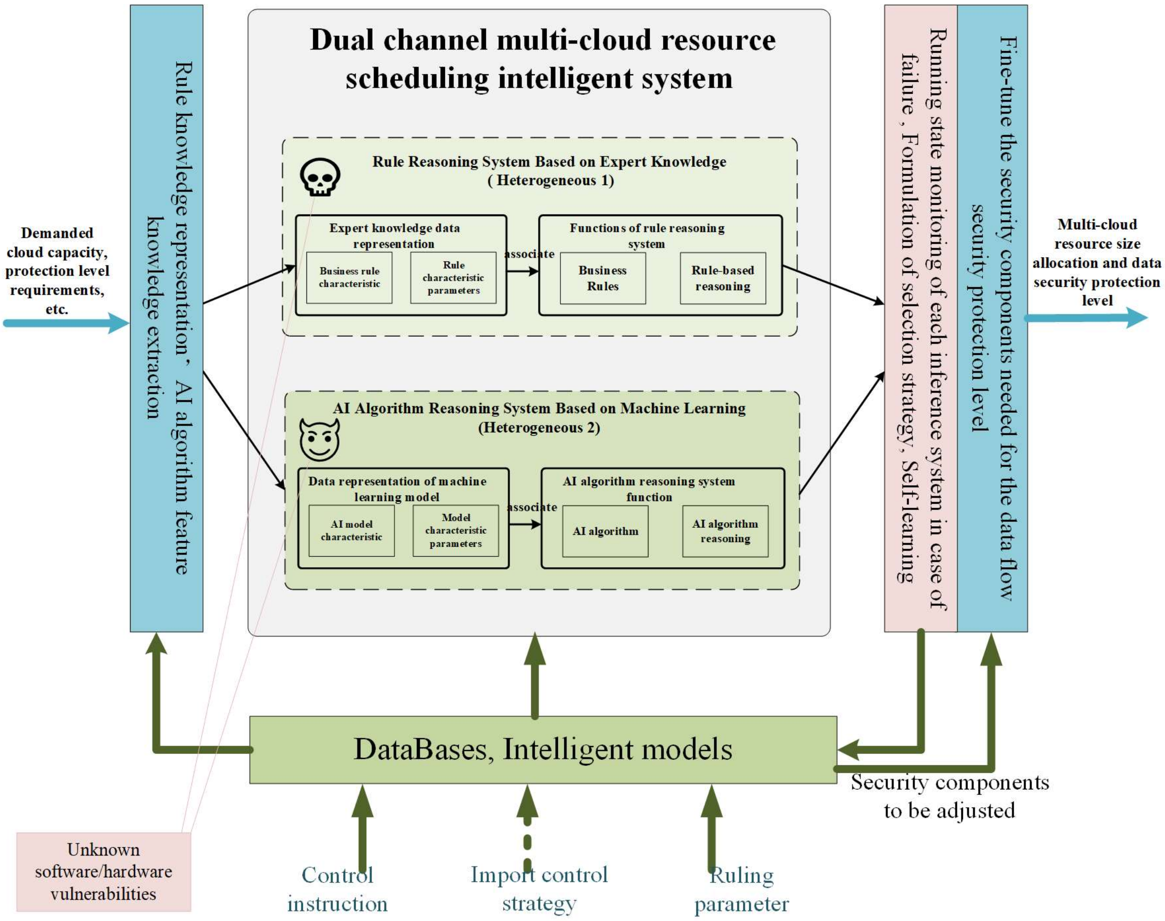
Dual channel multi-cloud resource scheduling intelligent system
Rule Reasoning System Based on Expert Knowledge (Heterogeneous 1)
Expert knowledge data representation
Business rule characteristic
Rule characteristic parameters
associate
Functions of rule reasoning system
Business Rules
Rule-based reasoning
AI Algorithm Reasoning System Based on Machine Learning (Heterogeneous 2)
Data representation of machine learning model
AI model characteristic
Model characteristic parameters
associate
AI algorithm reasoning system function
AI algorithm
AI algorithm reasoning
Demanded cloud capacity, protection level requirements, etc.
Rule knowledge representation、AI algorithm feature knowledge extraction
Running state monitoring of each inference system in case of failure , Formulation of selection strategy, Self-learning
Fine-tune the security components needed for the data flow security protection level
Multi-cloud resource size allocation and data security protection level
DataBases, Intelligent models
Security components to be adjusted
Unknown software/hardware vulnerabilities
Control instruction
Import control strategy
Ruling parameter

Figure 4. Dual channel intelligent system model with endogenous security in multi-cloud resource scheduling.

4.3.1. Input agent

Supporting polymorphic knowledge representation.

Input sequence:

- Multi-cloud resource scheduling requirements.
- Demanded cloud capacity, protection level requirements, etc.

Polymorphic knowledge representation:

- AI algorithm feature knowledge extraction: the attribute features are shown in Table 3.
- Rule knowledge representation: as Table 4 parses the premise of the rule used for reasoning.

4.3.2. Heterogeneous knowledge reasoning system engine functions

Two heterogeneous functions:

- *Rule reasoning system based on expert knowledge (Heterogeneous 1)*

The rule-based reasoning algorithm, as shown in Algorithm 1, is given below.

```
Algorithm 1 Rule-Based Reasoning Algorithm (Heterogeneous 1)
1.  Input Data: multi-cloud resource scheduling operations
2.  Initialize Security Policy Parameters: SP0(ST0, Zone0= {Clouds, Networks, Security-levels})
3.  Configure Cloud Network Data Flow Security Policy: SP (ST, Zone)
4.  Call rules in order of priority:
    a. Rule 1: Choose a private cloud first
    b. Rule 2: Choose a cloud with lower operating costs first
    c. Rule 3: Choose a cloud with a high level of security first
    d. Rule 4: Choose a cloud that has high overall performance first
5.  Allocate multi-cloud resources: SP = SP + SP0 = {MaxST, MinZone0} = {Max (ST, ST0), Min (Zone, Zone0)}
6.  Call function of data flow security protection level adjustment related components
7.  Output operation scheme of resource scheduling
```

- *AI algorithm inference reasoning system based on machine learning (Heterogeneous 2)*

Feature selection:

In each multi-cloud resource scheduling operation, feature combinations with high relevance are selected to form a vector representation and stored as a training set in the database.

In the multi-cloud resource scheduling operation, the C_{rem}, C_{sec}, C_{eco}, C_{perf} feature parameters are the key parameters that reflect the business operation strategy. Among them, C_{sec}, C_{eco} feature parameters are relatively fixed in the scheduling operation process, so we should focus on C_{rem}, C_{perf} feature parameters. For example, in the scenario with two clouds, if we focus only on the remaining storage space of the clouds $C1.C_{rem}$ $350\ GB$, $C2.C_{rem}$ $200\ GB$ and the allocated space C_{dem} $100\ GB$ each time, the feature space vector can be represented as follows:

$$(C_{dem},\ C1.C_{rem},\ C2.C_{rem}) = (100, 350, 200).$$

Selection of KNN algorithm:

The KNN algorithm handles the classification problem with high immunity and reliability. The above features ensure that the KNN algorithm works well in intelligent processing of running logs in multi-cloud resource scheduling scenarios. When using the KNN algorithm, the model parameter k is set to 3, and we can take the three nearest neighbor samples each time.

4.3.3. Iterative judging criteria and self-learning of AI algorithms

Design of endogenous security immunization mechanisms:

The selection of a particular heterogeneous redundant reasoning system to participate in the reasoning task should be uncertainty specific.

- Running state monitoring of each inference system in case of failure.
- Formulation of selection strategy, such as selection triggered by failure of any of the reasoning systems, random selection, specific selection, and priority selection.

Self-learning of AI algorithms involves saving the output sequences of each resource scheduling operation policy execution into the training sample library, while using the updated training sample library for learning and training of AI algorithms to obtain the latest model parameters.

4.3.4. Feedback control scheduler

Databases and AI models:

Databases: Datasets of scheduling operation logs for multi-cloud resources, cloud feature database, multi-cloud resource Security Policy Library (SPL), list of layered and graded security capability components and resource scheduling operation database.

AI models: Business rule and AI algorithm bases.

4.3.5. Output agent

Multi-cloud resource size allocation and data security protection level in the resulting sequence of inference system outputs are compared with the input user requirements to fine-tune the security components needed for the data flow security protection level to form the final sequence of outputs that satisfy the user requirements.

5. Experiment on endogenous security DHR features of the constructed intelligent reasoning system in multi-cloud resource scheduling

The environment used for the experiment, see Figure 3, consists of two parts: a multi-cloud resource scheduling intelligent system with endogenous security and dual-channel redundancy and an external attacker, in which the multi-cloud resource scheduling intelligent system with endogenous security and dual-channel redundancy consists of a multi-cloud resource scheduling demand input, a multi-cloud resource scheduling intelligent system, and a scheduling operation scheme output; the external attack part is responsible for various attacks on the resource scheduling system and for interfering with the reasoning channel that destroys the current working state. The objectives and contents of the experiment are detailed in Table 5.

Table 5. The objectives and contents of the experiment of endogenous security DHR features.

No.	Experiment name	Experimental contents
Experiment 1	Dynamic feature	● Setting the dynamic channel selection policy. ● External attack is applied to the current working channel so that the channel cannot work normally. ● Verifying whether the system can automatically switch to another channel so that the system can continue to maintain the working state, and loading the security components to repair the reasoning channel damaged by the attack.
Experiment 2	Heterogeneous feature	● Selecting a rule-based reasoning channel and an AI algorithm KNN-based reasoning channel. ● Accomplishing the task of multi-cloud resource scheduling operation ● Verify whether the results of the output scheduling operation scheme are consistent.
Experiment 3	Redundant feature	● Calculating and comparing the reliability of a single rule-based reasoning channel, a single AI algorithm-based reasoning channel, and a dual-channel redundant reasoning system working continuously for a period of time. ● Verify the practical effect of reliability enhancement in redundant channel mode.

5.1. *Dynamic feature*

The dynamic feature is shown by the uncertainty of heterogeneous reasoning systems selected to participate in reasoning tasks. The following measures will ensure the uncertainty of the reasoning task involved in the selection of heterogeneous redundant reasoning systems:

Table 6. The situation of using random selection strategy to select the inference engine.

Task name	Random number	Selected inference engine
Task1	23	Rule Based (Heterogeneous 1)
Task2	68	AI Algorithm (Heterogeneous 2)
Task3	54	AI Algorithm (Heterogeneous 2)
Task4	17	Rule Based (Heterogeneous 1)
Task5	6	AI Algorithm (Heterogeneous 2)
Task6	85	Rule Based (Heterogeneous 1)
Task7	39	Rule Based (Heterogeneous 1)

- Formulation of selection strategies, such as random selection, specific selection and priority selection. The Table 6 shows the situation of using random selection strategy to select an inference engine for each task. It can be seen from the table that the uncertainty of inference engine selection is guaranteed. According to the parity of random integers, they correspond to different heterogeneous inference systems.
- External attack is applied to the current working channel so that the channel cannot work normally.
- Running state monitoring of each inference system, the application program of each inference system can ensure that when an exception occurs, another inference system can turn to the formal working

mode by providing whether the running state is normal.

5.2. Heterogeneous feature

The heterogeneous feature is shown by the consistency of results achieved by heterogeneous reasoning systems. The same reasoning task should obtain the same reasoning result in two heterogeneous reasoning systems. The experimental requirements are detailed in Table 7 below.

Table 7. Experimental requirements for the heterogeneous feature of reasoning systems with endogenous security.

Experimental procedure	Experimental content	Detailed description
1. Initial parameter setting	(1) Selecting dual channels	a) Rule-based inference channel b) AI algorithm KNN based reasoning channel
	(2) Initial state of multi-cloud space and security policy	a) Multi-cloud maximum storage, allocated space and remaining space b) Cloud network security protection zones c) Cloud security levels
	(3) Multi-cloud resource scheduling operations task	a) Resource space, security level requirements, multi-cloud residual space
2. Rule-based reasoning system (Heterogeneous 1)	Resource scheduling process	a) Resource scheduling operation arithmetic rules b) Channel 1 output scheme
3. KNN-based reasoning system (Heterogeneous 2)	Resource scheduling process	a) Input parameters and algorithm description of the KNN algorithm b) Channel 2 output scheme
4. Experimental conclusion judgment	Comparing resource scheduling output schemes for two-channel reasoning for consistency	a) If the output schemes of channel 1 and channel 2 are the same, functional consistency is successfully verified. b) Otherwise, the functional consistency is inconsistent and the verification fails.

5.2.1. Initial parameter setting

1) Selecting dual channels

Here dual redundant inference channels are chosen, rule-based inference channel and KNN-based inference channel.

2) Initial state of multi-cloud space and security policy

First, security policy (SP) includes security tokens (*ST*) and security area (Zone):

$$SP\ (ST,\ Zone)$$

Then, security policy library (SPL):

$$SPL = \{SP1, SP2, SP3 \ldots\}$$

Initial SP parameters:

$$SP0(ST0, Zone0)$$

Initial cloud C1:

$$C1.C_{used} = 1650GB$$

$$C1.C_{rem} = 350GB$$

Initial cloud C2:

$$C2.C_{used} = 800GB$$

$$C2.C_{rem} = 200GB$$

Cloud C1 and C2 initial states are shown in Table 8.

Table 8. Cloud C1 and C2 initial states.

ID	Name of Cloud	Maximum storage space	Cloud space used	Cloud space remaining	Boundary	Security level
ID0	C1	2000 GB	1650 GB	350 GB	N1, N2	Level 2
	C2	1000 GB	800 GB	200 GB	N3, N4	Level 2

(i) Cloud network data flow security policy configuration:

$$SP\ (ST, Zone).$$

(ii) Implementation of security policies at all layers of data flow security protection system:
Calling Algorithm 1: Rule-based reasoning algorithm to *MinZone* and *MaxST*.

$$\begin{aligned} SP &= SP + SP0 \\ &= \{MaxST, MinZon0\} \\ &= \{Max\ (ST, ST0), Min\ (Zone, Zone0)\} \end{aligned} \tag{10}$$

3) Multi-cloud resource scheduling task

The multi-cloud resource scheduling intelligent reasoning system training sample set in Table 9 is a repository of historical operations. Now only the features $C1.C_{rem}$, $C2.C_{rem}$ in the Table 3 are taken, and they can be serialized as follows:

$$(C_{dem},\ C1.C_{rem},\ C2.C_{rem}) = (100, 350, 200).$$

Table 9. Resource scheduling intelligent reasoning system training sample set.

ID	$C1.C_{eco}$	$C1.C_{rem}$	$C1.C_{eco}$	$C1.C_{rem}$	Operation scheme *(C1, C2)*	Class
1	6	200	5.5	700	(100, 0)	1
2	6	250	5.5	600	(50, 50)	2
3	6	750	5.5	100	(100, 0)	1
4	6	300	5.5	800	(0, 100)	3
5	6	400	5.5	200	(50, 50)	2
6	6	350	5.5	250	(50, 50)	2
7	6	450	5.5	100	(100, 0)	1
8	6	500	5.5	850	(0, 100)	3
……	……	……	……	……	……	……
N	6	350	5.5	200	(50, 50)	2
N + 1	6	300	5.5	150	(50, 50)	2

The resource scheduling results for the two heterogeneous inference systems should adhere to the same operation-scheme (50, 50), with cloud C1 and C2 assigned to schedule 50 GB of resource space each.

5.2.2. Rule-based reasoning system (Heterogeneous 1)

As you can see from Table 8, the current resource scheduling task is to allocate 100 GB of security level 3 storage and the associated application deployment. It can be serialized as follows:

$$(C_{dem},\ C1.C_{rem},\ C2.C_{rem}) = (100, 350, 200).$$

Calling Algorithm 1, multi-cloud resource calling rules 1–4 and Eq (10), the operation-scheme assigns 50 GB of resource space to clouds C1 and C2, resulting in corresponding resource scheduling results.

5.2.3. KNN-based reasoning system (Heterogeneous 2)

Now only the features $C1.C_{rem}$, $C2.C_{rem}$ in the Table 3 are taken, and multi-cloud resource scheduling demand can be serialized as follows:

$$(C_{dem},\ C1.C_{rem},\ \mathrm{C2.C_{rem}}) = (100, 350, 200).$$

When using the KNN algorithm, the model parameter k is set to 3. By querying Table 9, it has been determined that samples with the IDs 5, 6, and 7 are the three nearest neighbor samples. Since IDs 5 and 6 belong to Class 2 and ID 7 belongs to Class 1, it is classified as Class 2, using the operation scheme (50, 50).

5.2.4. Consistency of reasoning results

It can be seen from the above that this reasoning result of operation-scheme (50, 50) is the same as that of rule-based reasoning. Therefore, it verifies the consistency of results achieved by heterogeneous reasoning systems.

5.3. *Redundant feature*

Redundant feature is shown by reliability analysis of multi-channel reasoning in data flow security. The failure rate of the rule-based reasoning system is λ_1, and the failure rate of the AI-algorithm-based reasoning system is λ_2.

Due to uncertain internal resource depletion or external threat attacks, assuming that the mean time between failures (MTBF) of the rule-based reasoning channel of the single-channel module is 10000 h, it can be seen from Eq (5) that the failure rate of the single channel module is:

$$\lambda_1 = \frac{1}{MTBF} = 0.0001.$$

Assuming that the mean time between failures (MTBF) of the reasoning channel of the single channel module based on the AI algorithm is 8000 h, it can be seen from Eq (5) that the failure rate of the single channel module is:

$$\lambda_2 = \frac{1}{MTBF} = 0.000125.$$

It can be seen from Eq (3) that the reliability of rule-based reasoning channel of the single channel module working for 2000 h is:

$$R_1(t) = e^{-\lambda_1 t} = 0.8187.$$

It can be seen from Eq (3) that the reliability of reasoning channel based on AI algorithm of the single channel module working for 2000 h is:

$$R_2(t) = e^{-\lambda_2 t} = 0.7788.$$

According to Eq (8), the reliability of the dual redundant channel module for 2000 hours is:

$$R_s(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 t + \lambda_2 t)} = 0.9599.$$

Table 10. List of the reliability of the dual redundant channel reasoning system.

Working hours	AI algorithm-based reasoning	Rule-based reasoning	Dual redundant channel
8000	0.3679	0.4493	0.6519
6000	0.4724	0.5488	0.7619
4000	0.6065	0.6703	0.8703
2000	0.7788	0.8187	0.9599

The reliability of the reasoning system with different channel designs is shown in Table 10.

Table 10 lists the reliability of the reasoning system in multi-cloud resource scheduling with different channel designs. The reliability of the rule-based channel, the AI algorithm-based reasoning channel, and the dual redundant channel for 2000 hours are 0.7788, 0.8187, and 0.9599, respectively.

So far, the above three experiments validate the endogenous security DHR property of our designed multi-cloud resource scheduling intelligent system.

5.4. Experimental results

The above proves the endogenous DHR property of the dual-channel system, so that when the intelligent reasoning channel in the work process encountered external threats using known or unknown system vulnerabilities to attack the failure, one of the standby reasoning channels will be timely transformed into a normal working state, while loading security components to repair the failed channel, to ensure that the system always has the ability to self-heal. We have used the multi-cloud resource scheduling intelligent run log database to carry out experiments. The security and reliability of the whole reasoning system have improved, as shown in Table 11, and the endogenous security of the system is achieved.

Table 11. Some reasoning results of the endogenous dual-channel system.

Task name	Random number	Selected inference engine	Heterogeneous system 1 Operation scheme (C1, C2)	Heterogeneous system 2 Operation scheme (C1, C2)	Whole system state
Task 1	23	Rule Based (Heterogeneous 1)	(50, 50)	Failure, restored	Running continuously
Task 2	68	AI Algorithm (Heterogeneous 2)	Failure, restored	(100, 0)	Running continuously
Task 3	54	AI Algorithm (Heterogeneous 2)	Failure, restored	(50, 50)	Running continuously
Task 4	17	Rule Based (Heterogeneous 1)	(0, 100)	Failure, restored	Running continuously
Task 5	6	AI Algorithm (Heterogeneous 2)	Failure, restored	(50, 50)	Running continuously
Task 6	85	Rule Based (Heterogeneous 1)	(100, 0)	Failure, restored	Running continuously
Task 7	39	Rule Based (Heterogeneous 1)	(50, 50)	Failure, restored	Running continuously
Task n	……	……	……	……	……

6. Discussion

Different reasoning systems have different computational efficiencies and time delays, and in order to better support the demand of high-intensity cloud computing for low-latency cloud applications, the more efficient subsystems with rule-based reasoning system should be prioritized as the default setting option when deploying endogenous security reasoning systems for multi-cloud resource scheduling.

7. Conclusions

In this paper, we first apply endogenous security theory to a multi-cloud resource scheduling intelligent reasoning system for the first time. Second, we construct a dual-redundant endogenous security inference system in multi-cloud resource scheduling. Finally, we validate the endogenous security mechanism of the dual-redundant inference system by combining the historical operation data in the cloud resource intelligent scheduling of cloud network systems, and analyze the enhancement of system reliability by the dual-redundant inference system. The results show that our scheme outperforms several representative inference system schemes commonly used in practice.

In conclusion, the endogenous secure inference system incorporated in multi-cloud resource scheduling guarantees system security and significantly enhances system reliability when performing inference tasks. It is suitable for multi-cloud network resource scheduling scenarios with elevated security and reliability demands.

Going forward, we intend to focus on two areas to expand our research work. On one hand, we will conduct reliability tests on various types of inference systems in an organized and methodical manner to gather relevant data. On the other hand, we will strive to optimize and enhance the design of endogenous security mechanisms in inference systems to ensure they meet the new demands and challenges of enterprise digital transformation and ensure the security and reliability of multi-cloud resource invocation intelligent systems.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgment

This research has been sponsored by the National Key R&D Program for Privacy Data Protection (Project number: 2021YFB3101300), Topic 5 “Research on Key Technologies for the Protection of Personal Rights and Interests” (Project number: 2021YFB3101305).

Conflict of interest

The authors declare there is no conflict of interest.

References

1. P. Kühn, D. N. Relke, C. Reuter, Common vulnerability scoring system prediction based on open source intelligence information sources, *Comput. Secur.*, **131** (2023), 1103286. https://doi.org/10.1016/j.cose.2023.103286

2. S. Nazir, S. Patel, D. Patel, Assessing and augmenting SCADA cyber security: A survey of techniques, *Comput. Secur.*, **70** (2017), 436–454. https://doi.org/10.1016/j.cose.2017.06.010
3. J. Wu, Cyberspace endogenous safety, security, *Engineering*, **15** (2021), 179–185. https://doi.org/10.1016/j.eng.2021.05.015
4. B. Yang, S. Wang, Q. Cheng, T. Jin, Scheduling of field service resources in cloud manufacturing based on multi-population competitive-cooperative GWO, *Comput. Ind. Eng.*, **154** (2021), 107104. https://doi.org/10.1016/j.cie.2021.107104
5. Z. X. Sun, H. Huang, Z. Li, C. Gu, R. Xie, B. Qian, Efficient, economical and energy-saving multi-workflow scheduling in hybrid cloud, *Expert Syst. Appl.*, **228** (2023), 120401. https://doi.org/10.1016/j.eswa.2023.120401
6. G. Zhou, W. Tian, R. Buyya, K. Wu, Growable Genetic Algorithm with Heuristic-based Local Search for multi-dimensional resources scheduling of cloud computing, *Appl. Soft Comput.*, **136** (2023), 110027. https://doi.org/10.1016/j.asoc.2023.110027
7. G. Agarwal, S. Gupta, R. Ahuja, A. K. Rai, Multiprocessor task scheduling using multi-objective hybrid genetic Algorithm in Fog–cloud computing, *Knowledge-Based Syst.*, **272** (2023), 110563. https://doi.org/10.1016/j.knosys.2023.110563
8. W. Zhang, J. Xiao, W. Liu, Y. Sui, Y. Li, S. Zhang, Individualized requirement-driven multi-task scheduling in cloud manufacturing using an extended multifactorial evolutionary algorithm, *Comput. Ind. Eng.*, **179** (2023), 109178. https://doi.org/10.1016/j.cie.2023.109178
9. W. Xiong, M. K. Lim, M. L. Tseng, Y. Wang, An effective adaptive adjustment model of task scheduling and resource allocation based on multi-stakeholder interests in cloud manufacturing, *Adv. Eng. Inf.*, **56** (2023), 101937. https://doi.org/10.1016/j.aei.2023.101937
10. W. Zhang, Y. Zheng, W. Ma, R. Ahmad, Multi-task scheduling in cloud remanufacturing system integrating reuse, reprocessing, and replacement under quality uncertainty, *J. Manuf. Syst.*, **68** (2023), 176–195. https://doi.org/10.1016/j.jmsy.2023.03.008
11. X. Wang, H. Lou, Z. Dong, C. Yu, R. Lu, Decomposition-based multi-objective evolutionary algorithm for virtual machine and task joint scheduling of cloud computing in data space, *Swarm Evol. Comput.*, **77** (2023), 101230. https://doi.org/10.1016/j.swevo.2023.101230
12. Y. H. Wu, H. B. Li, RNNCTPs: A neural symbolic reasoning method using dynamic knowledge partitioning technology, *Knowledge-Based Syst.*, **268** (2023), 110481. https://doi.org/10.1016/j.knosys.2023.110481
13. G. Wang, Y. Zhang, F. Zhang, Z. Wu, An ensemble method with DenseNet and evidential reasoning rule for machinery fault diagnosis under imbalanced condition, *Measurement*, **214** (2023), 112806. https://doi.org/10.1016/j.measurement.2023.112806
14. Y. Gao, R. Bao, Z. Pan, G. Ma, J. Li, X. Cai, Q. Peng, Mechanical equipment health management method based on improved intuitionistic fuzzy entropy and case reasoning technology, *Eng. Appl. Artif. Intell.*, **116** (2022), 105372. https://doi.org/10.1016/j.engappai.2022.105372
15. M. B. Fard, A. Hamedani, M. Ebadi, D. Hamidi, K. Motlaghzadeh, M. Emarati, et al., Sustainable waste-to-energy plant site selection by a hybrid method of geographic information system and evidential reasoning: A case study Guilan province, *Process Saf. Environ. Prot.*, **176** (2023), 316–331. https://doi.org/10.1016/j.psep.2023.05.063

16. W. Xu, Y. Huang, S. Song, Y. Chen, G. Cao, M. Yu, et al., A new online optimization method for boiler combustion system based on the data-driven technique and the case-based reasoning principle, *Energy*, **263** (2023), 125508. https://doi.org/10.1016/j.energy.2022.125508
17. M. R. N. Kalhori, M. H. FazelZarandi, A new interval type-2 fuzzy reasoning method for classification systems based on normal forms of a possibility-based fuzzy measure, *Inf. Sci.*, **581** (2021), 567–586. https://doi.org/10.1016/j.ins.2021.09.060
18. J. Wang, Z. Zhang, G. Zhao, Task recommendation method for fusion of multi-view social relationship learning and reasoning in the mobile crowd sensing system, *Comput. Commun.*, **206** (2023), 60–72. https://doi.org/10.1016/j.comcom.2023.04.028
19. W. Xu, Y. Huang, S. Song, B. Chen, X. Qi, A novel online combustion optimization method for boiler combining dynamic modeling, multi-objective optimization and improved case-based reasoning, *Fuel*, **337** (2023), 126854. https://doi.org/10.1016/j.fuel.2022.126854
20. R. Yadav, A. Giri, S. Chatterjee, Understanding the users' motivation and barriers in adopting healthcare apps: A mixed-method approach using behavioral reasoning theory, *Technol. Forecasting Social Change*, **183** (2022), 121932. https://doi.org/10.1016/j.techfore.2022.121932
21. Z. Zhang, L. Wang, J. Duan, Y. M. Wang, An early warning method based on fuzzy evidential reasoning considering heterogeneous information, *Int. J. Disaster Risk Reduct.*, **82** (2022), 103356. https://doi.org/10.1016/j.ijdrr.2022.103356
22. Z. Zhao, J. Chen, K. Xu, H. Xie, X. Gan, H. Xu, A spatial case-based reasoning method for regional landslide risk assessment, *Int. J. Appl. Earth Obs. Geoinf.*, **102** (2021), 102381. https://doi.org/10.1016/j.jag.2021.102381
23. X. Long, H. Li, W. Ren, Y. Du, E. Mao, N. Ding, A parameter-extended case-based reasoning method based on a functional basis for automated experiential reasoning in mechanical product designs, *Adv. Eng. Inf.*, **50** (2021), 101409. https://doi.org/10.1016/j.aei.2021.101409
24. S. Chen, J. Liu, Y. Xu, A logical reasoning based decision making method for handling qualitative knowledge, *Int. J. Approximate Reasoning*, **129** (2021), 49–63. https://doi.org/10.1016/j.ijar.2020.11.003
25. A. Wang, X. Gao, A variable scale case-based reasoning method for evidence location in digital forensics, *Future Gener. Comput. Syst.*, **122** (2021), 209–219. https://doi.org/10.1016/j.future.2021.03.019
26. N. Cercone, A. An, C. Chan, Rule-induction and case-based reasoning: Hybrid architectures appear advantageous, *IEEE Trans. Knowl. Data Eng.*, **11** (1999), 166–174. https://doi.org/10.1109/69.755625
27. D. Sottara, P. Mello, M. Proctor, A configurable rete-oo engine for reasoning with different types of imperfect information, *IEEE Trans. Knowl. Data Eng.*, **22** (2010), 1535–1548. https://doi.org/10.1109/TKDE.2010.125
28. Y.Cao , Z. Zhou, C. Hu, W. He, S. Tang, On the interpretability of belief rule-based expert systems, *IEEE Trans. Fuzzy Syst.*, **29**(2021), 3489–3503. https://doi.org/10.1109/TFUZZ.2020.3024024
29. S. Guo, W. Zhou, K. Li, Multi-layer Case-based Reasoning Approach of Complex Product System, in *2012 Third World Congress on Software Engineering*, (2012), 107–110. https://doi.org/10.1109/WCSE.2012.27

30. R. Ouache, E. Bakhtavar, G. Hu, K. Hewage, R. Sadiq, Evidential reasoning and machine learning-based framework for assessment and prediction of human error factors-induced fire incidents, *J. Build. Eng.*, **49** (2022), 104000. https://doi.org/10.1016/j.jobe.2022.104000
31. S. Kierner, J. Kucharski, Z. Kierner, Taxonomy of hybrid architectures involving rule-based reasoning and machine learning in clinical decision systems: A scoping review, *J. Biomed. Inf.*, **144** (2023), 104428. https://doi.org/10.1016/j.jbi.2023.104428
32. H. Bride, C. H. Cai, J. Dong, J. S. Dong, Z. Hóu, S. Mirjalili, et al., Silas: A high-performance machine learning foundation for logical reasoning and verification, *Expert Syst. Appl.*, **176** (2021), 114806. https://doi.org/10.1016/j.eswa.2021.114806
33. Y. Chen, Z. Dai, H. Yu, B. K. H. Low, T. H. Ho, Recursive reasoning-based training-time adversarial machine learning, *Artif. Intell.*, **315** (2023), 103837. https://doi.org/10.1016/j.artint.2022.103837
34. L. Bellomarini, R. R. Fayzrakhmanov, G. Gottlob, A. Kravchenko, E. Laurenza, Y. Nenov, et al., Data science with Vadalog: Knowledge Graphs with machine learning and reasoning in practice, *Future Gener. Comput. Syst.*, **129** (2022), 407–422. https://doi.org/10.1016/j.future.2021.10.021
35. M. Namvar, A. Intezari, S. Akhlaghpour, J. P. Brienza, Beyond effective use: Integrating wise reasoning in machine learning development, *Int. J. Inf. Manage.*, **69** (2023), 102566. https://doi.org/10.1016/j.ijinfomgt.2022.102566
36. J. G. C. Krüger, A. de Souza Britto Jr, J. P. Barddal, An explainable machine learning approach for student dropout prediction, *Expert Syst. Appl.*, **233** (2023), 120933. https://doi.org/10.1016/j.eswa.2023.120933
37. R. Gao, S. Cui, H. Xiao, W. Fan, H. Zhang, Y. Wang, Integrating the sentiments of multiple news providers for stock market index movement prediction: A deep learning approach based on evidential reasoning rule, *Inf. Sci.*, **615** (2022), 529–556. https://doi.org/10.1016/j.ins.2022.10.029
38. J. Liu, Q. Qian, Reinforcement learning-based knowledge graph reasoning for aluminum alloy applications, *Comput. Mater. Sci*, **221** (2023), 112075. https://doi.org/10.1016/j.commatsci.2023.112075
39. N. Muslim, S. Islam, J. C. Grégoire, Reinforcement learning based offloading framework for computation service in the edge cloud and core cloud, *J. Adv. Inf. Technol.*, **13** (2022), 139–114. https://doi.org/10.12720/jait.13.2.139-146
40. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, Overview of 5g security challenges and solutions, *IEEE Commun. Stand. Mag.*, **2** (2018), 36–43. https://doi.org/10.1109/MCOMSTD.2018.1700063
41. H. Hu, J. Wu, Z. Wang, G. Cheng, Mimic defense: a designed-in cybersecurity defense framework, *IET Inf. Secur.*, **12** (2018), 226–237. https://doi.org/10.1049/iet-ifs.2017.0086