Hindawi
Mathematical Problems in Engineering
Volume 2020, Article ID 3528439, 18 pages
https://doi.org/10.1155/2020/3528439

Research Article

Multilevel Security Network Communication Model Based on Multidimensional Control

Lifeng Cao, Xin Lu, Zhensheng Gao, Mengda Han, and Xuehui Du

He'nan Province Key Laboratory of Information Security, Zhengzhou, Henan 450001, China

Correspondence should be addressed to Xin Lu; 1209774364@qq.com

Received 20 February 2020; Revised 28 March 2020; Accepted 30 March 2020; Published 12 May 2020

Academic Editor: José António Fonseca de Oliveira Correia

To solve the problems associated with the application of multilevel security to actual networks, such as flexibility, availability, security, and secure communication, this study proposes a multilevel security network communication model based on multidimensional control. In the model, access control is retained on the basis of security labels. In addition, relational restraints among protection domains, credibility degree restraints of subjects on security attributes, aggregation inference control restraints, and secure tunnel control restraints are introduced and applied. Thus, secure information exchange within a multilevel security network information system is ensured. Moreover, using this model, multilevel security virtual networks with logical and independent characteristics can be built to accomplish secure interconnection and communication between nonequivalent members, thereby reducing the probability of information leakage. Finally, the security of the model is confirmed by applying the nontransitive, noninterference theory, and the typical application of the model in actual networks is described.

1. Introduction

Although the rapid development of cloud computing [1], 5G [2], Internet of Things (IoT) [3], and other emerging technologies has brought great convenience to people, these technologies also pose a threat to the security of network and information owing to their openness, data sharing, and other characteristics [4–6]. At present, research on data security, such as on preserving privacy [7, 8], information security transmission and sharing [9, 10], and information encryption [11], plays a prominent role in information security. However, most of these studies are aimed at single-level data security and do not consider multilevel data security. Note that due to the complexity and diversity of information, different sensitivity levels of information exist in the network. Therefore, to ensure the security of information at different sensitivity levels in the network, multilevel security networks [12] have emerged.

Owing to the various security levels in multilevel security networks, information systems face several problems such as those related to establishing intersystem communication relations, controlling interdomain subject-object access security, and transmission of information at different levels after interconnection [13]; these problems directly affect the availability of multilevel security networks. Establishing secure communication is the key to realizing secure interconnection and interoperability of information systems. Therefore, in order to realize multilevel security interconnection of network information systems, attention must be paid to establish a multilevel security-oriented network security communication model and implementation of multilevel security control and security transmission.

In recent years, many scholars have carried out research on the problems and requirements of multilevel security models. In previous studies, the usability and adaptability of a multilevel security model were improved [14, 15], but since the model was highly dependent on the access control characteristics of the Bell–LaPadula (BLP) model [16], the access flexibility between various subject-object levels was limited. In other studies, a unified representation of multilevel security strategies was provided [17], and an application isolation model was proposed for secure computing environments, ensuring dynamic security of applications in the domain during operation [18]. In addition, a multilevel security model based on the BLP model was proposed to realize dynamic adjustment of the

security level of subject-access-object in the model, and the flexibility of the multilevel security model was improved to a certain extent [19]. However, the model was mainly applicable to private cloud environments, and it controls the operations of users through a mandatory access model, which compromises the flexibility and compatibility of the model to a certain extent. A new multilevel secure access control model (V-MLR) was proposed [20], which not only provides a secure communication mechanism for virtual machine monitors (VMMs) and virtual machines (VMs) but also updates the communication mechanism synchronously with varying information in a VMM. However, this model relies on the overall performance of the VMM system. Lan et al. [21] proposed a safe and practical integrated network security strategy model. The architecture of the model comprises three parts: security system, secure connection of the network, and security transmission of data and key management. This model realizes secure communication and management of data, but it does not solve the problem of multilevel interconnection and aggregation inference control. Information flow control [22] is another typical technology in multilevel security research; it focuses on access control research, which is usually used in security level control of information systems. However, information flow control is difficult to implement in a network because it cannot be well combined with security communication. In the above research, although the multilevel security model has been improved in terms of flexibility, adaptability, compatibility, and other aspects, it is still unable to integrate with the network security communication and provide a more comprehensive consideration to many aspects.

In a previous study [23], a security policy model SBLP for multilevel security networks was presented, and its state machine model definition and state change rules were provided, which formally confirmed the security of the model. However, its rules were relatively simple, without considering the problem of easy deduction and leakage of sensitive information by data aggregation. Another study [24] presented a method to build a unified directed acyclic graph model (including both subjects and objects) by using partially ordered sets. This method was easy to realize and has greater utility in designing an access control model; however, such a model does not provide control rules for secure access between hosts and objects at different levels. Furthermore, multilevel security communication was realized by using a quantum key and IPSec [25]. In this method, a field was added to implement the control strategy based on the security of data packets, a key effective time was used to meet the different security requirements, the "one-time-pad" algorithm was used to provide unconditional security, and the process of transmitting data packets was described. However, in this method, the generation and use rules of the quantum key were complex. In another study, a multilevel security access control strategy was proposed for distributed systems [26]. Based on the multilevel security model, the management platform and middleware modules were added to ensure data confidentiality and access process security and control. However, the system did not consider information transmission security and the integrity and security of the system during its formulation. Although the aforementioned studies provided effective guidance for secure interconnection of multilevel security networks, data flow control in communication, and secure access between hosts and objects at different levels, they could not adequately solve the security problems faced by multilevel security in network applications. Problems such as object aggregation inferring highly sensitive information and poor flexibility of communication between hosts and objects at different levels still exist. In a previous study, the noninterference theory was applied to a behavior-based access control model to control the access of the subject to structured documents without describing the access to unstructured documents regularly [27]. Furthermore, some studies [27–29] provided an effective guidance for using the noninterference theory to prove the security of a multilevel security model. For the security of sensitive information, a new framework to secure information in fog cloud IoT was proposed in [30], which can realize the security sharing of data in different locations. In addition, a novel quantum steganography protocol based on the hash function and quantum entangled states was presented. The hash function is used to authenticate embedded secret messages, avoiding the attacks of message, man-in-the-middle, and no-message. The protocol provides guidance for secure sharing and access of information with various sensitivity levels. The existing network security communication model has great improvement in flexibility, adaptability, and other aspects [31–34], but most of them do not support the multilevel security attributes effectively; hence, they cannot fully meet the security communication requirements of multilevel security network information systems. Hence, it can be seen that the current research on multilevel security models do not sufficiently meet the actual requirements of multilevel security network communication, and they still face many problems, such as the following:

(1) The static nature of security labels makes multilevel security networks less flexible.

Multilevel security requires that a subject's access to an object strictly follows the simple security characteristics and "$*$" characteristic (state consistency characteristic) [35]. This restriction of multilevel security prevents access of legitimate network subjects, makes the implementation of the network more difficult, and renders the network less flexible and usable [36]. These issues are mainly caused by the static nature of security labels, which once allocated, will not change [37].

As Figure 1 shows, in a network environment, situations where high-level subjects write low-level objects and low-level subjects read high-level objects exist [38]. Resolving the problem of a subject's illegal access to objects under special circumstances is the key to improving the flexibility and adaptability of a BLP model network.

(2) The existence of object-sensitive levels results in the deduction and leakage of information by object

information aggregation in a multilevel security network.

Although the BLP model prevents information from leaking with the "read-down and write-up" rule, sensitive information can easily be leaked owing to the similarity and attribute dependency of objects.

In Figure 2, secret level subject s_1 reads "objects o_1 and o_2." Higher level (greater than the secret level) information is deducted from objects o_1 and o_2. Secret level subject s_2 can read "objects o_3, o_5, and o_6" and deduct higher level (more than the secret level) information from objects o_3, o_5, and o_6. Thus, the multilevel security network access control no longer follows only the security characteristics of "read-down, write-up" but also considers the relationship between objects.

(3) Multilevel security lacks a security channel mechanism because of which problems of information leakage and interference occur.

Existing multilevel security models do not support secure transmission adequately. Achieving efficient multilevel security network transmission based on an access control strategy is also an important consideration for realizing secure interconnection of multilevel security network information systems.

The adaptability of the existing secure transmission mechanism in a multilevel security network will be poor because it is not combined with security features such as network security hierarchy and multilevel security information. Moreover, the established security channel is single-level. The information in the domain protected by interconnected entities is transmitted confidentially by the same channel. Isolation of information of different security levels is difficult, while interference can be easily caused between information. In addition, prevention of information deduction and leakage caused by information aggregation is even more difficult. As shown in Figure 3, O_1 and O_3 have different security levels, but they are transmitted in the same channel (a single-level security channel shown in Figure 3). Low-level information easily interferes with high-level information, resulting in leakage. Therefore, in a multilevel security network, it is necessary to establish a multilevel security channel (dotted line in Figure 3) and build an independent, virtual, and logical multilevel security network to ensure isolation of information transmission at different levels.

Given the aforementioned problems, in order to improve the flexibility and adaptability of multilevel security in a network, it is essential to prevent information leakage risk and support the network security communication mechanism with multilevel security attributes, thus achieving secure interconnection among multilevel security network information systems. In meeting the abovementioned requirements, this study contributes in the following aspects:

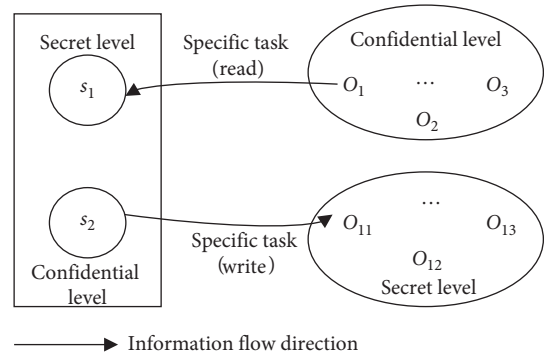

Figure 1: Subject's illegal access to an object.

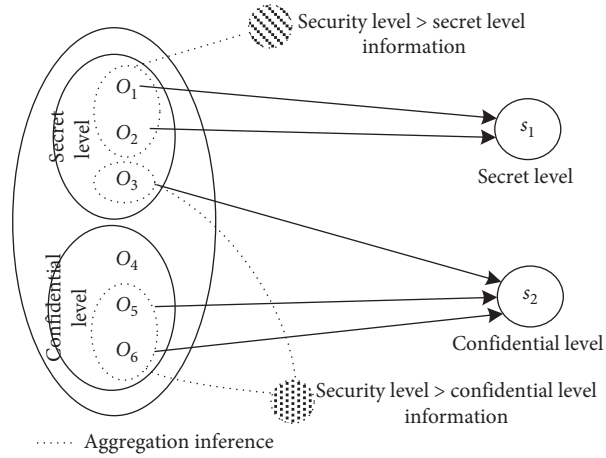

Figure 2: Object information aggregation and leakage.

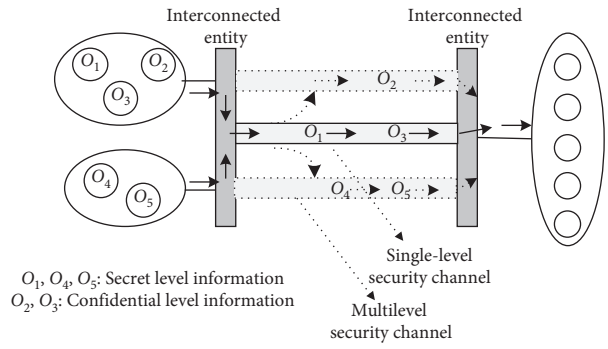

Figure 3: Information transmission interference problem.

(1) In this study, we use the concept of "domain" to abstract the complex information system, and on the basis of the domain, we analyze the problems existing in the security communication between multilevel security network information systems, establish a multilevel security-oriented network security communication model based on multidimensional control (MLS_NSCM), construct the network communication environment suitable for multilevel security, and realize object sharing and interoperability between different levels of information systems are realized.

(2) In the model, we design multilevel security control constraint rules and security channel control constraint rules, including 21 basic constraints of the model, and then we build a multilevel security virtual network. The model not only overcomes the problems of poor flexibility and adaptability of the BLP model and enhances the availability of the multilevel security model in the actual network but also reduces the risk of leakage caused by the aggregation of object information. Through multilevel security channel control, it realizes the mutual isolation of information of different levels and information with aggregation problems, thus reducing the possibility of information leakage and effectively improving the security of information systems.

(3) To verify the security and credibility of the model, we confirm the security of the model based on the noninterference theory, perform a comparative analysis of the security provided by the proposed model and existing models, and provide the typical application of the model in actual networks.

2. Model Building Concept

A network information system can be divided into domains [39, 40]. Therefore, in this study, the interdomain relationship of the system is considered as the basis to maintain the access control of security labels and integrate the interdomain relationship constraint, subject credibility constraint, object information aggregation inference, multilevel security channel establishment, and other controls in order to realize secure exchange of information between information systems. The schematic diagram of the building of the MLS_NSCM model is presented in Figure 4.

(1) The system is divided into a set of protected domains, and interdomain relations (i.e., hierarchical relations and peer-to-peer relations) are used to restrict interconnection relations, effectively implementing secure interconnection control and preventing arbitrary communication between domains.

(2) In the application layer, the credibility of the subject's security attributes is evaluated through a credibility evaluation mechanism, and the credibility threshold required by the subject and the object is taken as the basis of the multilevel security control of the network. This will solve the operation problem of the subject violating the multilevel security rules and accessing the object under special circumstances, for example, the access of s_1 to o_4 and the access of s_2 to o_5 in Figure 4. Every time the subject visits an object by violating rules, the credibility of the subject is evaluated and the method of dealing with the subject and object after the subject violates rules is considered such that the risk of system leakage is reduced and the reference relationship of the object is maintained. This process improves the flexibility and availability of the BLP model in network application.

(3) In the application layer, the relationship between objects is analyzed, control constraints are deduced based on aggregation, the access of subjects to relational objects is restricted, multilevel security is extended from security label access control to object relationship so as to reduce the risk of information leakage caused by object information aggregation, and the restriction of the BLP model on confidentiality security attributes is enhanced.

(4) According to secure channel rules, a multilevel security channel is established, and a logical, independent, autonomous, and dedicated multilevel security virtual subnet is constructed to ensure safe transmission and isolation of information at different sensitive levels in different flow directions, to realize noninterference of the channel, and to prevent objects with aggregation problems from using the same channel for transmission, thereby reducing the possibility of network information leakage.

Based on the above concepts, from the aspects of multilevel security control and secure channel control, under the assistance of technologies such as security labels and information objects, data stream binding, aggregation inference control, subject trust evaluation, and secure channel establishment, this study implements subject-object access control and security transmission at application and network layers in order to achieve secure communication between network information systems.

3. Model Multilevel Security Control Constraint Rules

3.1. Basic Constraints of Multilevel Security Control. The MLS_NSCM model obeys the multilevel security control rules of the BLP model, that is, simple security features and "$*$" characteristics. After extension, the access operation set of the model includes the operations of inflow (f_a), outflow (f_r), in-out flow (f_w), and execution (f_e).

Constraint 1

if $L(s) \le L(o)$ **then**

$s \xrightarrow{f_a} o$

endif

s is the subject, or the communication initiator, which can be a user, a host, a subnet, an address range, a user group, a subnet group, or an address group; o is the object, or the communication receiving end, which can be a file, a database, a web service, an FTP service, a subnet, a host, an address range, or an address group; and L is a security label function. Constraint 1 shows that if o's security label dominates s, s inflows to access o.

Constraint 2

if $L(s) \ge L(o)$ **then**

$s \xleftarrow{f_r \| f_e} o.$

endif

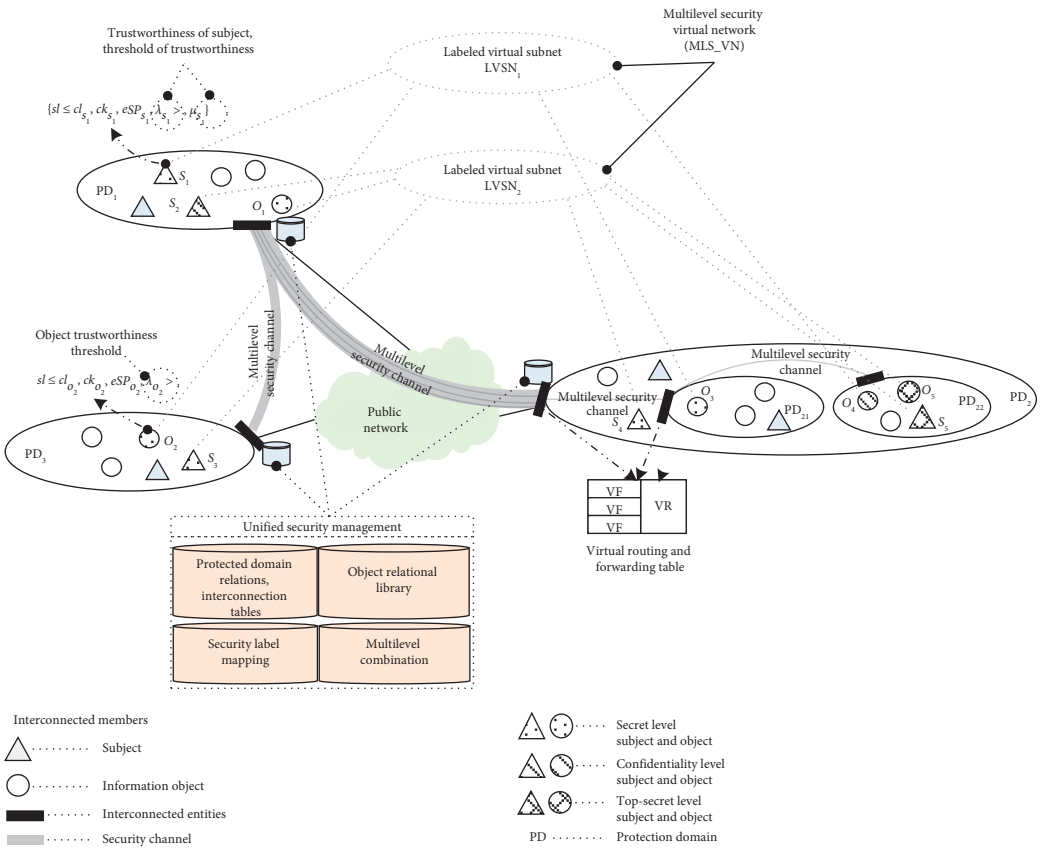

Figure 4: MLS_NSCM model building.

It indicates that if the security label of s dominates o, then s outflows to access or execute object o.

Constraint 3

if $L(s) = L(o)$ then
$s \xleftrightarrow{f_w} o$.
endif

It indicates that if the security labels of s and o dominate each other, then s inflows and outflows to access object o.

3.2. Protection Domain Control Constraints

Definition 1. Protection domain (PD): PD is a set of subjects and objects protected by interconnected entities to achieve interdomain data flow control. Interconnection members and entities are detailed in Definitions 5 and 6. From the definition of PD, it can be as small as a single terminal or as large as one or a group of subnets. The relationship and interconnection control between PDs are maintained in an interconnection table of PDs (PDT), and effective interconnection control between domains and within domains is implemented according to the PDT.

Constraint 4

if pd_i and pd_j have n-level relationship, i.e., $pd_i \triangleright_n pd_j$ **then**

/∗It implies that the pd_j n-fold contains pd_i∗/

pd_i and pd_j have an interactive relationship.

if $n = 0$ **then**

pd_i and pd_j are the same PD.

endif

if pd_i and pd_j do not have a hierarchical relationship **then**

The interaction between pd_i and pd_j is determined by the PDT.

if pd_i and pd_j have an interactive relationship **then**

It is recorded as $pd_i \longleftrightarrow pd_j$.

endif

Constraint 4 illustrates the interconnection control relationship between PDs in order to achieve mutual isolation between domains. The following are its main points:

(1) pd_i and pd_j have n-level relationship, which indicates that pd_j n-fold contains pd_i, i.e., pd_i is the subdomain of pd_j, and there is an interaction between the parent domain and the subdomain.

(2) There is no hierarchical relationship between pd_i and pd_j, which indicates that they are independent and reciprocal. Even if they have the same parent domain, there is no direct interaction between them, but the interaction is determined by the PDT.

Constraint 5

if $(pd_i \longleftrightarrow pd_j)$&& $(pd_j \longleftrightarrow pd_k)$ **then**
pd_i and pd_k do not necessarily obey $pd_i \longleftrightarrow pd_k$.
endif

The main manifestation is as follows:

(1) **if** $(pd_i \triangleright_l pd_j)$ && $(pd_j \triangleright_m pd_k)$ **then**
$pd_i \triangleright_{l+m} pd_k$.
endif

This relation indicates that pd_j l-fold contains pd_i,pd_k m-fold contains pd_j, and pd_k $(l+m)$-fold contains pd_i. The inclusion relationship defined here is transitive.

(2) **if** $(pd_i \triangleright_l pd_k)$ && $(pd_j \triangleright_m pd_k)$ && $(l \geq m)$ **then**
$pd_i \triangleright_{l-m} pd_j$.
endif

This relation indicates that pd_k l-fold contains pd_i,pd_k m-fold contains pd_j, and then pd_j $(l\text{-}m)$-fold contains pd_i. This shows that the inclusion has implication relation.

(3) **if** pd_i and pd_j are peer domains, pd_j and pd_k are peer domains, and there are interactions among peer domains as well as pd_i, pd_j, and pd_k are not equal **then**
pd_i and pd_k are also peer domains, and the interactions are controlled by the PDT.
endif

(4) **if** $(pd_i \longleftrightarrow pd_j)$ && $(pd_j \triangleright_m pd_k)$ **then**
$pd_i \longleftrightarrow pd_k$.
endif
This relationship indicates that pd_i and pd_j have an interaction relationship. pd_k n-fold contains pd_j; hence, there should be an interaction relationship between pd_i and pd_k, which indicates that subdomain interaction is based on parent-domain interaction.

(5) **if** $(pd_i \longleftrightarrow pd_j)$ && $(pd_k \triangleright_m pd_j)$ **then**
An interaction between pd_i and pd_k is not necessary.
endif
This relationship indicates that the parent domain pd_j of pd_k and pd_i has an interactive relationship, but pd_i and pd_k do not necessarily have an interactive relationship, but the relationship is controlled by the PDT.

3.3. Subject Credibility Constraints

Definition 2. Reliability in security attributes: this refers to the degree of trust that the subject will not destroy the information security attributes of the object.

Confidentiality credibility refers to the credibility that the subject will not leak information after visiting the object, which is expressed as $\mu_i(C)$, $i \in S$. $\lambda_i(C)$ denotes the confidence threshold ($i \in S \cup O$) of a subject or an object on the confidentiality security attributes such that the lowest reliability required by the system is determined.

Constraint 6

if $(L(s) \geq L(o))$ && $(s \xrightarrow{f_a} o)$ **then**
$\mu_s(C) \geq \lambda_s(C)$.
endif

When a high-level subject inflows to access a low-level object, it must control the scope of the subject to inflow to access the object. It requires that the credibility $\mu_s(C)$ of subject s in confidentiality should be no less than the minimum confidentiality credibility threshold $\lambda_s(C)$, which implies that subject s inflows to access object o with the current credibility is not enough for information leakage.

Constraint 7

if $(L(s) \leq L(o))$ && $(s \xrightarrow{f_r} o)$ **then**
$\mu_s(C) \geq \lambda_s(C)$ && $\mu_s(C) \geq \lambda_o(C)$.
endif

When a low-level subject outflows to access a high-level object, the credibility $\mu_s(C)$ of subject s should not be less than the minimum confidentiality credibility threshold $\lambda_s(C)$ of subject s so that it will not leak information. At the same time, the reliability of s in confidentiality should be no less than the reliability threshold of object o.

3.4. Aggregation Inference Control Constraints. Aggregation inference control of an object aims to reduce the risk of leakage caused by information object aggregation. By analyzing the relationship between objects, deducing the possibility of deriving higher-level information from relational objects, corresponding security strategies are formulated to control a subject's restricted access to relational objects. This study holds that relational objects mainly include similar objects and related objects. Similar objects refer to objects with similar contents and attributes, whereas related objects refer to those with some implicit deductive relationship, and they are also known as incompatible objects.

Definition 3. Incompatible object aggregation inference problem: let o_i and o_j be strongly correlated and denoted as $o_i \diamond o_j$. If the information of o_i and o_j is aggregated together and the probability that the information security level deduced is higher than the information security level of o_i and o_j exceeds a specific threshold, then o_i and o_j have an incompatible object aggregation inference problem.

Definition 4. Similar object aggregation inference problem: if k $(k \leq n)$ objects in some similar objects $o_1, o_2, \ldots, o_n$ are aggregated together, the deduced information security level is higher than the highest security level of these n objects, then it is considered that these n objects have the problem of clustering deduction of similar objects. It can be recorded as $\text{obj\_sim}(o_1, o_2, \ldots, o_i, \text{valve})$, $\text{valve} \leq n$.

Object relation is maintained by an object relation table (ORT), which contains two subtables: ORTI and ORTA. ORTI is an association relation table, organized in the form of $< o_i, o_j, \text{Incompatible} >$ to indicate that o_i and o_j are incompatible. ORTA refers to a similar object aggregation relation table, such as $< o_1, o_2, \ldots, o_i, \text{value} >$, and the value is the maximum number of similar objects that can be accessed by the subject.

Constraint 8

if $o_i \Diamond o_j$ **then**
  o_i and o_j are restricted by subject access.
endif

Constraint 8 shows that if o_i and o_j are incompatible objects, then the information security level $cl_{o_i o_j} > \max\{cl(o_i), cl(o_j)\}$ is derived from aggregation of o_i and o_j. That is, the deduced information has a higher level of information security than o_i and o_j. Subjects with a security level less than $cl_{o_i o_j}$ are prohibited from accessing o_j if they have ever visited o_i, and vice versa.

Constraint 9

if $\exists \text{obj\_sim}(o_1, o_2, \ldots, o_n, \text{valve})$ **then**
  The number of objects allowed to access is less than value.
endif

Constraint 9 shows that $o_1, o_2, \ldots, o_{\text{valve}}$ are deduced information level $cl > \max\{cl(o_1), \ldots, cl(o_{\text{valve}})\}$ after aggregation; that is, the information security level is higher than that of any object in $o_1, o_2, \ldots, o_{\text{valve}}$. There are two types of threshold selection for the similar object clustering problem: one is the quantitative aspect, wherein high-level information can be deduced from any "valve" objects; the other is the qualitative aspect, wherein there are k objects in $o_1, o_2, \ldots, o_n$. As long as any or more of these k objects are included, high-level information can be deduced, "valve" will be any one value from $k+1$ to n, and k objects are also called the special objects. Subjects with a security level less than cl can only access "valve-1" similar object. If special objects exist, they are absolutely not allowed to be accessed.

3.5. Subject-Object Level Adjustment Constraints

Constraint 10

if $(L(s) \le L(o))$ && $(s \xrightarrow{f_a} o)$ **then**
  s.addtxt $\longrightarrow$ filt_buff
  tmp_buff = chk_buf(vs, filt_buff)
  tmp_buff $\xrightarrow{\text{vs}}$ o
endif

"addtxt" denotes the data content added by subject s and inflow to access object o; "filt_buff" is a filter buffer area for filtering the content added by subject s to ensure the integrity of object o; "tmp_buff" is a temporary buffer for temporary storage of filtered content; "vs" is a virtual subject for checking data in buffer and adding checked content to object o; and "chk_buf" is a check function. Constraint 10 shows that when a low-level subject s inflows to access a high-level object o, s must be checked by vs in "filt_buff" to ensure the integrity of object o. The security level of vs must be consistent with the level of object o. vs adds the checked data to object o.

Constraint 11

if $cl(o.\text{txt} + s.\text{addtxt}) > cl(o.\text{txt})$ **then**
  Create a new object o' (o' = o.txt + s.addtxt)
  Keep the original object o unchanged
endif

Constraint 11 shows that the security level of fused data is higher than that of object o after fusing the data of subject s into object o with the original data of o. To ensure the reference relationship of other subjects to object o, we create new objects (data are fusion data) and keep the object o unchanged.

Constraint 12

if $(cl(o) > cl(s))$ && $(s \xleftarrow{f_r} o)$ **then**
  $L(s) = L(o.\text{addtxt})$
endif

Constraint 12 indicates that the security level of low-level subjects must be upgraded when a low-level subject s inflows to access a high-level object o. This is because if the security level of s remains unchanged, it is easy for s to divulge the information of high security level known to the subject or object of the same level. Moreover, the security level of s is raised temporarily. When o passes the period of confidentiality, the security level of s will return to its original level.

3.6. Security Label Mapping Constraints

Constraint 13. Security label transfer mapping.

The security labels in pd_i and pd_j are heterogeneous. If the security label transfer of subject s in pd_i is mapped to that in pd_j, the permissions obtained by subject s in pd_j include the following: (1) s can write the object dominated by security label sl_{pd_j}; (2) s can read the object dominated by security label sl_{pd_j}. At the same time, other subjects in domain pd_i who have control over s can obtain the privileges of s in domain pd_j.

Constraint 13 illustrates the cross-domain access problem of subjects in domain pd_j when security labels are heterogeneous between domains. At this time, the security labels in domain pd_j are assigned to s by virtual subject mapping, and other subjects that control the security labels in domain pd_i have the rights of s in domain pd_j. At this time, through virtual subject mapping, security labels in domain pd_i are assigned to s, and other subjects with dominant rights of s security labels have the privileges of subject s in domain pd_j.

Constraint 14. Security label circular transfer mapping. The security labels in domains pd_i and pd_j are heterogeneous. The security label of the subject in domain pd_i is mapped to

that in pd_{jj}. The security label of the subject in domain pd_j is mapped to that in pd_i.

if the information system level of pd_i is not greater than that of pd_j, **then**
$sl_{pd_i}^{s_1} \le sl_{pd_j}^{s_1}$
$sl_{pd_j}^{s_2} \ge sl_{pd_i}^{s_2}$
endif

Constraint 14 refers to the principle of security label mapping when two or more information systems are passed in a circular manner. Its purpose is to prevent the implicit elevation of the subject level caused by the circular transmission.

Constraint 15. Security label nontransitive mapping.

The security labels in pd_i and pd_j are heterogeneous. If the security labels of subject s in pd_i are mapped nontransitively to those in pd_j, subject s in pd_i obtain privileges if and only if they are the objects with security labels equal to sl_{pd_j}. Other subjects with a dominant relationship to s are prohibited from having the privileges of s in domain pd_j.

Constraint 15 refers to the scope of s accessible in domain pd_j when it is accessed across domains and prohibits the proliferation of privileges to prevent the possibility of information leakage.

4. Model Secure Channel Control Constraint Rules

The MLS_NSCM model is designed to ensure confidentiality, integrity, and credibility of data sources in secure channels.

4.1. Security Channel Classification Constraints. A multilevel security channel has a certain level of security, and the purpose is to protect the security of different sensitive data streams. The higher the level of security, the stronger the protection provided by the security channel.

Definition 5. Interconnected members: this refers to all subjects and objects involved in the security interconnection of multilevel security network information systems. If "CM" represents the set of interconnected members, $\exists \mathrm{cm}_i \in \mathrm{CM}$, and then $cm_i \in S \cup O$.

Definition 6. Interconnected entities: this refers to devices or components that are securely interconnected in a network information system to protect interconnected members. If "CE" denotes the set of interconnected entities, $\mathrm{ce} \in \mathrm{CE}$.

Definition 7. Multilevel security channel: this refers to the special security channel based on the multilevel security network and multilevel data transmission achieved through encapsulation, encryption, authentication, and other technologies. If "lst_k" is multilevel channel k, then the multilevel secure channel is defined as $lst_k = \{ < \mathrm{ce}_i, \mathrm{ce}_j, < cl_{\mathrm{ce}_i}, cl_{\mathrm{ce}_j} >, lSA_k > | \mathrm{ce}_i, \mathrm{ce}_j \in \mathrm{CE} \}$. Here, lSA_k provides multilevel security association (SA: a set of policies and keys used to protect information) for lst_k, including the encapsulation protocol, encryption and authentication algorithms, session key, and data stream direction.

Constraint 16. The security level of multilevel secure channel lst_k is determined by the level of data transmitted by the channel, and its constraints are described as follows:

DL$_1$: if $(\mathrm{ce}_i \longleftarrow \mathrm{ce}_j) \&\& (f_r || f_a)$ **then**
$cl(lst_k) = lst_k.lt_k.cl_{\mathrm{ce}_j}$
DL$_2$: if $(\mathrm{ce}_i \longrightarrow \mathrm{ce}_j) \&\& (f_r \| f_a)$ **then**
$cl(lst_k) = lst_k.lt_k.cl_{\mathrm{ce}_i}$
DL$_3$: if $(\mathrm{ce}_i \longleftrightarrow \mathrm{ce}_j) \&\& f_w$ **then**
$cl(lst_k) = lst_k.lt_k.cl_{\mathrm{ce}_i} = lst_k.lt_k.cl_{\mathrm{ce}_j}$
DL$_4$: if f_e **then**
$cl(lst_k) = cl(s)\}$;
endif

Constraint 16 shows that the secure channel level is related to the direction of the channel data flow because the data transmitted in the channel are related to the source end of the data flow. **DL$_1$** and **DL$_2$** reflect that, in the operation of inflow and outflow, the level of security of the channel is consistent with the level of security at the source end of channel data flow, whether it is a low-level subject inflow to access a high-level object, a high-level subject outflow to access a low-level object, or a high-level subject inflow to access a low-level object and a low-level subject outflow to access a high-level object. **DL$_3$** reflects that the data flow is bidirectional in the inflow and outflow operations. Because the security level between the communication peers is the same, the security channel level should be the same as the security level of the communication peers. **DL$_4$** reflects that the security level of the security channel is consistent with that of the subject in the execution operation because the security level of the subject is higher than that of the object in the operation.

4.2. Security Channel Protection Constraints. Despite the unidirectionality of the secure channel, in the actual network environment, owing to the bidirectionality of the communication protocol, there is actually a bidirectional data flow in the secure channel. Therefore, effective control of data flow in the multilevel secure channel is particularly important. Hence, this study formulates the protection rules of a secure channel to ensure legitimacy of data flow in a channel.

Constraint 17. lSA_k includes $\overrightarrow{lSA_k}$ and $\overleftarrow{lSA_k}$, representing the SA in two directions. If the flow direction of data stream in lst_k is $\mathrm{ce}_i \longleftarrow \mathrm{ce}_j$, the protection rules are described as follows:

if $lst_k.lt_k.cl_{\mathrm{ce}_i} > lst_k.lt_k.cl_{\mathrm{ce}_j}$ **then**
$I(\overrightarrow{lSA_k}) > I(\overleftarrow{lSA_k})$
else $I(\overleftarrow{lSA_k}) > I(\overrightarrow{lSA_k})$
endif

Constraint 17 states the following: (1) there exists unidirectionality in secure channel security association; that is, $\mathrm{ce}_i \longrightarrow \mathrm{ce}_j$ and $\mathrm{ce}_i \longleftarrow \mathrm{ce}_j$ each have a SA to

protect the security of data flow in this direction. (2) Irrespective of forward or backward data flow, the strength of SA is related to the source endpoint of the data flow. If $ce_i \longleftarrow ce_j$ is a reverse flow and if $cl_{ce_i} > cl_{ce_j}$, the strength of the forward flow SA is higher than that of the reverse flow SA. Conversely, the strength of the reverse flow SA is higher than that of the forward flow SA. It can be seen that the strength of SA is mainly related to the security level of the source side of the data stream, but not to the size of the data in the data stream, where I () denotes the strength of the SA.

Constraint 18. lSA_k includes $\overrightarrow{lSA_k}$ and $\overleftarrow{lSA_k}$, representing the SA in two directions. If the flow direction of data stream in lst_k is $ce_i \longleftrightarrow ce_j$, then its protection rules are as follows:

if $ce_i \longleftrightarrow ce_j$ **then**

$lst_k.lt_k.cl_{ce_i} = cl_{ce_j} lst_k.lt_k.cl_{ce_j}$

$\overrightarrow{lSA_k} = \overleftarrow{lSA_k}$

endif

Constraint 18 shows that, in the case of bidirectional data flow, the protection measures should be the same; that is, SA is bidirectional at this time.

4.3. Security Channel Noninterference Control Constraints. To strictly control the information leakage problem caused by information object aggregation, this study introduces the rule of no interference in secure channels, which restricts the object with an aggregation problem from using the same secure channel for protection transmission and prevents the deduction of information in the same secure channel.

Constraint 19. If the information objects protected by ce_i and ce_j have the problem of aggregation inference, then when transmitting these objects in secure channels, no interference between channels should be achieved. The rules are as follows:

if $(o_i, o_j \in ce_i \cup ce_j) \&\& \exists((o_i \diamondsuit o_j) || \text{obj\_sim}(o_i, o_j, 1))$ **then**

$o_i \longleftarrow lst_i;\ o_j \longleftarrow lst_j$

$lst_i \neq lst_j$

endif

Constraint 19 states that if a problem of aggregation inference exists between objects, the objects are prohibited from transmitting through the same secure channel to prevent information deduction. (1) Objects with the aggregation inference problem can belong to the same or different ce, but there is an interconnection between their ce. (2) In case of objects with aggregate deduction relationship, although their security levels may be the same and the security levels of the negotiation channels are the same, these objects must choose different security channels for secure transmission according to the requirements of Constraint 8 and Constraint 9.

4.4. Secure Channel Switching and Forwarding Control Constraints. Because a multilevel security network is composed of multiple domains, each domain is securely interconnected by ce, and the relationship is intricate. It is necessary to formulate corresponding rules for forwarding and exchange of the security channels in order to build a secure and usable multilevel security network.

Constraint 20. The interconnected entities of secure channel lst_m are ce_i and ce_k and those of secure channel lst_n are ce_k and ce_j; thus, ce_k is the common interconnected entity of lst_m and lst_n. Then, the secure channel is exchanged as follows:

if $(m \overset{\text{from } ce_i \text{ to } ce_j}{\longrightarrow} ce_j) \&\& (ce_k \longleftarrow \text{visible}(m))$ **then**

$$\begin{matrix}\text{decap}(lst_m(m)) \\ \text{encap}(lst_n(m))\end{matrix} \quad \begin{matrix} lst_m(m) \longrightarrow \\ \longrightarrow lst_n(m) \longrightarrow \end{matrix} \overset{\text{decap}(lst_n(m))}{ce_j} \qquad ce_k$$

endif

Constraint 20 reflects the situation of secure channel switching, where "visible ()" is a visual function, and "visible (∗)" is visible to "∗"; "encap" is secure channel encapsulation, and "decap" is secure channel deencapsulation. Figure 5 illustrates secure channel switching.

The key points of secure channel switching include the following: (1) there is a common interconnected entity between secure channels; the prerequisite for secure channel exchange is that data information needs to be forwarded across the interconnected entity. For example, the common interconnected entity of lst_m and lst_n is ce_k. (2) In secure channel switching, it implies that lst_m and lst_n have the data flow directions of $ce_i \longrightarrow ce_k$ and $ce_k \longrightarrow ce_j$. Only when they have such direction of data flow, can they be allowed to exchange information. (3) Data m protected by the secure channel are visible to the interconnected entity ce_k; that is, there will be no leakage problems, such as aggregation inference. (4) The essence of secure channel exchange is that data m are protected by two secure channels and is unpackaged and reencapsulated at ce_k. Data m are the original text at ce_k.

Constraint 21. The interconnected entities at both ends of the secure channel lst_m are ce_i and ce_k, while those at both ends of lst_n are ce_k and ce_j, respectively. The interconnected entities at both ends of lst_p are ce_i and ce_j. ce_k is the common interconnected entity end of lst_m and lst_n; hence, the secure channel is forwarded as follows:

if $(m \overset{\text{from } ce_i \text{ to } ce_j}{\longrightarrow} ce_j) \&\& (ce_k \longleftarrow \text{invisible}(m))$ **then**

$$lst_p \quad (m) \overset{lst_m(lst_p(m))}{\longrightarrow} \overset{\begin{matrix} lst_p(m)=\text{decap}(lst_m(lst_p(m))) \\ lst_n(lst_p(m))=\text{encap}(lst_p(m)) \end{matrix}}{ce_k} \longrightarrow$$

$$lst_n(lst_p(m)) \longrightarrow$$

$$\begin{matrix} lst_p(m)=\text{decap}(lst_n(lst_p(m))) \\ m=\text{decap}(lst_p(m)) \end{matrix}$$

$$ce_j$$

endif

Constraint 21 reflects the situation of secure channel forwarding, in which "invisible ()" is an invisible function and "invisible (∗)" means invisible to "∗." It differs from

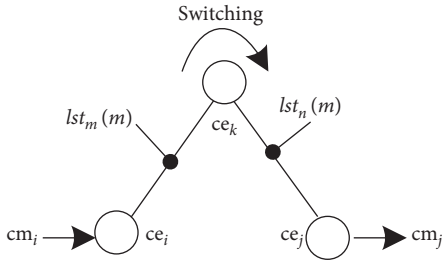

Figure 5: Secure channel switching.

Constraint 20 in two aspects: (1) in this rule, data m are not visible to the interconnected entity ce_k. At this time, ce_k can only encapsulate the encapsulated data again but cannot decompose the existing encapsulated data. (2) The essence of secure channel forwarding is that one channel is nested and encapsulated by another channel, and then data are forwarded along the new channel.

5. Multilevel Security Virtual Network

In the MLS_NSCM model, the establishment of multilevel secure channels will allow the members of the decentralized and independent multilevel security network construct a virtual and exclusive secure communication environment. Under the rules of multilevel security control constraints and security channel control constraints, the restricted subject-object access in the multilevel security virtual network can be effectively controlled.

Multilevel security virtual network (MLS_VN): this network is composed of multiple labeled virtual networks (LVSNs), composed of interconnected members, interconnected entities, multilevel security channels, and security policies. It can be represented by the following eight tuples:

$$\mathrm{LVSN}_{\mathrm{id_{lvsn}}} = \{\mathrm{id_{lvsn}}, \mathrm{id}_{m\mathrm{lnsd}}, \mathrm{CM}, \mathrm{CE}, \mathrm{LST}, \mathrm{MLSP}, \mathrm{VFT}, \mathrm{App}\}. \quad (1)$$

① $\mathrm{id_{lvsn}}$ is the identification of LVSN.

② $\mathrm{id_{mlnsd}}$ denotes the security domain identity of the network.

③ CM is a set of interconnected members protected by the LVSN and CE is a set of interconnected entities constructed by the LVSN, and they belong to the same security domain.

④ LST is a multilevel secure channel set, while VFT is the channel exchange and forwarding relationship in LST.

⑤ MLSP is a multilevel security communication policy set, and App is an application of the information system. The multilevel security communication strategy, MLSP, includes the multilevel secure control strategy and secure transmission strategy. The former mainly relies on the comparison between the subject and object security labels as well as needs multilevel security control constraint rules to restrict subject-object access. The latter is mainly used to protect data in the transmission process and to control the establishment and use of secure channels through the rules of secure channel control constraints.

6. Model Security Analysis

To analyze the security of the MLS_NSCM model, the model's security is verified through the nontransitive, noninterference theory, proposed by Rushby [41], and its related conclusions. This theory is used to analyze the rationality, effectiveness, and security of data flow control, and it serves as a good method to study the channel control strategy in a multilevel security network environment [42–44].

6.1. Nontransitive, Noninterference Theory. The basic idea of the nontransitive, noninterference theory is as follows [45]: two domains (security domains) u and v in the system are observed from the perspective of domain v. If the operation in domain u does not affect the subsequent output state of domain v, that is, the system state observed by domain v before and after the operation of domain u is the same, domain u is said to be noninterference to domain v.

Definition 8 (see [46]). Let system M be a finite automaton that consists of the following components:

① The system state set S, $s_0 \in S$, is the initial state.

② "A" is the system operation set, such as input, command, and instruction.

③ "OU" is the output set of the system.

④ step: $S \times A \longrightarrow S$ is a one-step state execution transition function.

⑤ output: $S \times A \longrightarrow \mathrm{OU}$ is the output function of the system.

⑥ run: $S \times A^* \longrightarrow S$ is a multistep state execution transition function. $\mathrm{run}(s, \Lambda) = s$, and Λ is an empty sequence. $\mathrm{run}(s, a \circ \alpha) = \mathrm{run}(\mathrm{step}(s, a), \alpha)$, and "$\circ$" is a connector.

⑦ "D" denotes the domain, and dom: $A \longrightarrow D$ denotes the system action execution domain.

⑧ The interdomain interference relation "$\sim>$" is a binary reflexive relation in the domain, and its complementary relation "$\not\sim> = (D \times D) \backslash \sim>$" is a noninterference relation. Information flow security policy refers to information flow rules between different domains, which can be represented by "$\sim>$" to illustrate the information flow relationship between security domains.

In the nontransitive, noninterference theory, a purge function of action sequence is defined as follows.

Definition 9 (see [46]). $v \in D$, $\alpha \in A^*$ is a sequence of actions, and $\mathrm{purge}(\alpha, v)$ is a subsequence of α. This subsequence is the remaining sequence after clearing the sequence of actions related to domain u in α; then, $u \not\sim> v$, that is,

$$\text{purge}(\Lambda, v) = \Lambda,$$
$$\text{purge}(a \circ \alpha, v) = \begin{cases} a \circ \text{purge}(\alpha, v), & \text{if dom}(a) \sim> v, \\ \text{purge}(\alpha, v), & \text{otherwise.} \end{cases} \quad (2)$$

The main function of the purge function is to delete all operations that do not interfere with domain v from the execution sequence α. If the outputs of the system before and after deletion are consistent, the system conforms to noninterference [47]. Thus, the nontransitive, noninterference model provides the system security requirements as

$$\text{output}(\text{run}(s_0, \alpha), a) = \text{output}(\text{run}(s_0, \text{purge}(\alpha, \text{dom}(a))), a). \quad (3)$$

To facilitate system security verification, the system security expansion theorem covering only one-step state has been given and proved in [41].

Theorem 1. *(Unwinding Theorem): " ~> " is the information flow security policy of system M. If the following conditions are satisfied, system M is considered to be safe relative to " ~> ". The proof is given in [41].*

① *Output consistency:* $s \overset{dom(a)}{\sim} t^{output(s,a)=output(t,a)}$, *which implies that if two states are equivalent, then they perform the same operation and the output from the operation domain is identical.*

② *One-step consistency:* $s \overset{u}{\sim} t^{step(s,a) \overset{u}{\sim} step(t,a)}$, *which implies that if two states are equivalent, then they are still equivalent after performing the same operation in both states.*

③ *Local coincidence:* $dom(a) \not\sim> u \longrightarrow s \overset{u}{\sim} step(s, a)$, *which implies that in a certain state, if the execution domain does not interfere with the target domain, the state after execution is equivalent to the original state.*

6.2. MLS_NSCM Model Security Proof. To verify the access control model conveniently, the abstract concept of access control is given in the nontransitive, noninterference model, which involves the following main elements:

① N is a set of object names; all the names of object o in information systems are taken from the set of object names N; o (n) denotes the object whose name is n.

② V is a set of object values; the value of object o in information system is derived from set V.

③ contents: $S \times N \longrightarrow V$ is a value function, indicating that the object named $n \in N$ takes $v \in V$ when the information system state is $s \in S$.

④ Function "observe: $D \longrightarrow \text{P}(N)$" represents the set of readable (outflow f_r) objects in domain D, where P is the set of permissions.

⑤ Function alter: $D \longrightarrow \text{P}(N)$ represents a set of writable (inflow f_a) objects in domain D.

To verify the security of the MLS_NSCM model, the following functions are given according to the access control and transmission rules.

① Function write: $D \longrightarrow P(N)$ represents the set of readable and writable objects (inflow and outflow f_w) in domain D.

② Function execute: $D \longrightarrow P(N)$ represents the set of executable objects in domain D.

③ Function impatile: $D \times o \longrightarrow C(N)$ represents a set of objects incompatible with object o, and C is a set with aggregation inference problems.

④ Function sim: $D \times o \longrightarrow C(N)$ denotes the set of objects that have similar object aggregation inference problem as object o.

⑤ Function encap: $m \longrightarrow lst_k(m, lSA_k)$ denotes that lSA_k is used to encapsulate, encrypt, and authenticate the transmitted information in a secure channel, where m is the content of transmission.

⑥ Function decap: $lst_k(m, lSA_k) \longrightarrow m$ denotes that lSA_k is used to decompose, decrypt, and authenticate channel information.

⑦ Function filt: $m \longrightarrow m'$ means filtering m, removing content that affects the integrity of the object and ensuring the integrity of the object when information flows in.

Based on the model control rules, the hypothesis conditions for the secure communication monitor of the MLS_NSCM model system are given as follows:

HY_1: $n \in \text{observe}(u) \Longleftrightarrow ck(u) \subseteq ck(n) \wedge (cl(u) \geq cl(n) \vee (cl(u) \leq cl(n) \wedge \mu_{s\in u} \geq \lambda_{s\in u} \wedge \mu_{s\in u} \geq \lambda_{o(n)})) \wedge \text{impatile}(u, n) \wedge \text{sim}(u, n) \wedge lst_k(n, lSA_k)$

HY_2: $n \in \text{alter}(u) \Longleftrightarrow ck(u) \subseteq ck(n) \wedge ((cl(u) \leq cl(n) \wedge \text{filt}(n)) \vee (cl(u) \geq cl(n) \wedge \mu_{s\in u} \geq \lambda_{s\in u})) \wedge lst_k(n, lSA_k)$

HY_3: $n \in \text{wirte}(u) \Longleftrightarrow cl(u) = cl(n) \wedge ck(u) \subseteq ck(n) \wedge \mu_{s\in u} \geq \lambda_{o(n)} \wedge \text{impatile}(u, n) \wedge \text{sim}(u, n) \wedge lst_k(n, lSA_k)$

HY_4: $n \in \text{execute}(u) \Longleftrightarrow cl(u) \geq cl(n) \wedge ck(u) \subseteq ck(n) \wedge \mu_{s\in u} \geq \lambda_{s\in u} \wedge \mu_{s\in u} \geq \lambda_{o(n)} \wedge lst_k(n, lSA_k)$

Theorem 2. *The MLS_NSCM model system M is secure for information flow strategy in access control if it satisfies the security communication monitoring hypotheses and model access control rules.*

Proof. To prove Theorem 2, it must be proved that the MLS_NSCM model system satisfies the reference monitor hypotheses under the assumption of secure communication monitor, and Theorem 1 is valid.

(1) Output consistency

Let $n \in \text{observe}(u)$, where n is an object in the set of objects readable by domain u. Hypothesis $\mathbf{HY_1}$ shows that only when object $o(n)$ does not have aggregation inference relationship and can the highly trusted subject in domain u be allowed to outflow to access objects, thus controlling the escalation of

information aggregation and preventing the possibility of leakage.

If object $o(n)$ does not perform write operations in any state of the system, $\text{contents}(s,n) = \text{contents}(t,n)$ holds.

If object $o(n)$ is added by domain v at a certain time, then $n \in \text{alter}(v)$. According to hypotheses $\mathbf{HY_2}$ and $\mathbf{HY_3}$ and the rules of multilevel security control constraints, when the subject in domain u inflows to access object $o(n)$, it needs to filter the inflow information to prevent the destruction of the integrity of object $o(n)$. Moreover, if the inflow of information results in the increase in the security level of object $o(n)$, a new object $o'(n')$ is created and object $o(n)$ remains unchanged. These operations do not change the access relationship of subject to $o(n)$ in domain u. It can be seen that when domain u performs read operation in two states, it still conforms to the control rules of model outflow operation. Therefore, under states s and t, $\text{contents}(s,n) = \text{contents}(t,n)$ holds.

It can be seen that if $\overset{u}{\sim}$ is the state equivalence relation on the model system M, then M meets the requirements of $s \overset{u}{\sim} t \longrightarrow \forall n \in \text{observe}(u)$: $\text{contents}(s,n) = \text{contents}(t,n)$; hence, $s \overset{\text{dom}(a)}{\sim} > t^{\text{output}(s,a)=\text{output}(t,a)}$ holds.

In addition, $\mathbf{HY_4}$ is usually used for the management operation of the system; hence, the output of the system is the same when the same operation is performed under state s or t.

Therefore, system M conforms to output consistency.

(2) One-step consistency

To prove the one-step$_u$consistency, it is necessary to prove that $s \overset{u}{\sim} t^{\text{step}(s,a) \sim \text{step}(t,a)}$, and as defined by the noninterference model system, it can be equivalent to $s \overset{u}{\sim} t^{\text{contents}(\text{step}(s,a),n)=\text{contents}(\text{step}(t,a),n)}$; that is, the object named n takes the same value as operation a in state s and t. Let us discuss $n \in observe(u)$ in three cases.

① $\text{contents}(\text{step}(s,a),n) \neq \text{contents}(s,n)$
If operation a is executed under state s and the value of object resource $o(n)$ changes, then $o(n)$ must execute operation $n \in \text{alter}(\text{dom}(a)) \vee \text{write}(\text{dom}(a))$ by execution domain $\text{dom}(a)$. Because of $n \in \text{observe}(u)$, $\text{dom}(a) \sim > u$ can be obtained, and then $\text{observe}(\text{dom}(a)) \subseteq \text{observe}(u)$ can be known. Therefore, $s \overset{u}{\sim} t$ implies $s \overset{\text{dom}(a)}{\sim} t$. From the model control constraints, it can be seen that, after object $o(n)$ is written, its integrity and citation relationship remain unchanged; hence, $\text{contents}(\text{step}(s,a),n) = \text{contents}(\text{step}(t,a),n)$ holds.

② $\text{contents}(\text{step}(t,a),n) \neq \text{contents}(t,n)$. The same is true for this situation as well.

③ $\text{contents}(\text{step}(s,a),n) = \text{contents}(s,n) \wedge \text{contents}(\text{step}(t,a),n) = \text{contents}(t,n)$. Because of $s \overset{u}{\sim} t$ and $n \in \text{observe}(u)$, $\text{contents}(\text{step}(s,a),n) = \text{contents}(\text{step}(t,a),n)$ holds.

Therefore, it can be seen that system M conforms to one-step consistency.

(3) Local coincidence

To prove $\text{dom}(a) \not<> u \longrightarrow s \overset{u}{\sim} \text{step}(s,a)$, we can prove that its converse negative proposition is valid; that is, $\exists n \in \text{observe}(u)$: $\text{contents}(s,n) \neq \text{contents}(\text{step}(s,a),n)^{\text{dom}(a) \sim > u}$.

(iii) Because $\text{contents}(s,n) \neq \text{contents}(\text{step}(s,a),n)$, obviously $n \in \text{alter}(\text{dom}(a)) \vee \text{write}(\text{dom}(a))$; therefore, we need to only prove that $n \in (\text{alter}(\text{dom}(a)) \vee \text{write}(\text{dom}(a))) \wedge n \in \text{observe}(u)^{\text{dom}(a) \sim > u}$. The following aspects of analysis and proof are considered in this study.

① When low-level subjects inflow to access high-level objects and high-level subjects outflow to access low-level objects:
$n \in \text{alter}(\text{dom}(a)) \wedge n \in \text{observe}(u) \longrightarrow cl(\text{dom}(a)) \leq cl(o(n)) \wedge \text{filt}(n)$,

$cl(u) \geq cl(o(n)) \wedge \text{impatile}(u,n) \wedge \text{sim}(u,n) \longrightarrow cl(\text{dom}(a)) \leq cl(u) \wedge \text{filt}(n) \wedge \text{impatile}(u,n) \wedge \text{sim}(u,n)$

② When low-level subjects inflow to access high-level objects and low-level subjects outflow to access high-level objects:
$n \in \text{alter}(\text{dom}(a)) \wedge n \in \text{observe}(u) \longrightarrow cl(\text{dom}(a)) \leq cl(o(n)) \wedge \text{filt}(n)$
$cl(u) \leq cl(o(n)) \wedge \mu_{s\in u} \geq \lambda_{s\in u} \wedge \mu_{s\in u} \geq \lambda_{o(n)} \wedge \text{impatile}(u,n) \wedge \text{sim}(u,n) \longrightarrow \text{filt}(n) \wedge \mu_{s\in u} \geq \lambda_{s\in u} \wedge \mu_{s\in u} \geq \lambda_{o(n)} \wedge \text{impatile}(u,n) \wedge \text{sim}(u,n) \wedge \text{upgrade}(u,s)$

③ When high-level subjects inflow to access low-level objects and high-level subjects outflow to access low-level objects:
$n \in \text{alter}(\text{dom}(a)) \wedge n \in \text{observe}(u) \longrightarrow cl(\text{dom}(a)) \geq cl(o(n)) \wedge \mu_{s\in u} \geq \lambda_{s\in u}$

$cl(u) \geq cl(o(n)) \wedge \text{impatile}(u,n) \wedge \text{sim}(u,n) \longrightarrow \mu_{s\in u} \geq \lambda_{s\in u} \wedge cl(u) \geq cl(o(n)) \wedge \text{impatile}(u,n) \wedge \text{sim}(u,n)$

④ When high-level subjects inflow to access low-level objects and low-level subjects outflow to access high-level objects:
$n \in \text{alter}(\text{dom}(a)) \wedge n \in \text{observe}(u) \longrightarrow cl(\text{dom}(a)) \geq cl(o(n)) \wedge \mu_{s\in \text{dom}(a)} \geq \lambda_{s\in \text{dom}(a)}$
$cl(u) \leq cl(o(n)) \wedge \mu_{s\in u} \geq \lambda_{s\in u} \wedge \mu_{s\in u} \geq \lambda_{o(n)} \wedge \text{impatile}(u,n) \wedge \text{sim}(u,n) \longrightarrow \mu_{s\in \text{dom}(a)} \geq \lambda_{s\in \text{dom}(a)} \wedge \mu_{s\in u} \geq \lambda_{s\in u} \wedge \mu_{s\in u} \geq \lambda_{o(n)} \wedge \text{impatile}(u,n) \wedge \text{sim}(u,n) \wedge \text{upgrade}(u,s)$

Of course, if domain A flows in and out of the object, the situation is similar to that of (1–4). In summary, situation ①: $cl(\mathrm{dom}(a)) \le cl(u)$; furthermore, content filtering and the constraints of aggregation inference control are applied to object $o(n)$, and the operation of $\mathrm{dom}(a)$ to object $o(n)$ does not change the reference relationship of $o(n)$. This implies that domain $\mathrm{dom}(a)$ can inflow domain u; that is, $\mathrm{dom}(a) \sim> u$. Situation ②: $cl(\mathrm{dom}(a)) \le cl(u)$; the content filtering of object $o(n)$ ensures its integrity, and the reference relationship of object $o(n)$ does not change after operation a. At the same time, the credibility of a subject in domain u on the confidentiality security attribute is required to be higher than the threshold of confidentiality credibility of its own and that of $o(n)$. Moreover, the security level upgrade of subject s_u that outflows to access $o(n)$ in domain u is carried out, which follows Constraint 12. Similarly, the reference relationship of s_u with other objects is not changed. Situation ③: in domain $\mathrm{dom}(a)$, the credibility of subject s_a in confidentiality security attributes is higher than its own credibility threshold such that the possibility of s_a leakage is reduced. According to Constraint 11, the operation of s_a to $o(n)$ does not change its reference relationship and $cl(u) \ge cl(o(n))$. Moreover, the aggregation inference control is applied to $o(n)$; hence, domain $dom(a)$ can flow into domain u. Situation ④: similarly, the credibility of subject s_a in the confidentiality security attribute in domain $\mathrm{dom}(a)$ is higher than its own credibility threshold, and the operation to $o(n)$ does not change the reference relationship of $o(n)$. At the same time, the current confidentiality credibility of subject s_u in domain u is higher than the credibility threshold of its own and that of $o(n)$. The aggregation inference control of $o(n)$ and the upgrading of subject s_u are executed, and the reference relationship of subject s_u to other objects is not changed.

In summary, we can see that the security policy of domain $\mathrm{dom}(a)$ inflowing to domain u is valid, that is, $\mathrm{dom}(a) \sim> u$. Thus, $n \in (\mathrm{alter}(\mathrm{dom}(a))) \vee \mathrm{write}(\mathrm{dom}(a)) \wedge n \in \mathrm{observe}(u)^{\mathrm{dom}(a) \sim> u}$ is proved. Therefore, according to the equivalence relation, $\exists n \in \mathrm{observe}(u)$: $\mathrm{contents}(s, n) \neq \mathrm{contents}\ (\mathrm{step}(s, a), n)^{\mathrm{dom}(a) \sim> u}$ is valid. According to its converse negative proposition, $\mathrm{dom}(a) \not\sim> u \longrightarrow s \overset{u}{\sim} \mathrm{step}(s, a)$ is valid.

Note that Theorem 2 meets the three requirements of Theorem 1. Therefore, the security of Theorem 2 is proved. □

Theorem 3. *The MLS_NSCM model system M is secure for information flow strategy in transmission if it satisfies the security communication monitoring hypothesis and model security channel control constraint rules.*

Proof. The security of system M transmission is not only related to the secure channel protocol and multilevel SA (e.g., channel key and cryptographic algorithm) but also to the forwarding and exchange of secure channels. The premise of this proof is that the channel protocol is secure. Because the strength of the channel key and cryptographic algorithm can be tested by special tools, this study only needs to explain the security of forwarding and switching transmission. Figure 5 is used as an example to prove that system M is secure for information flow strategy in transmission.

① Hypotheses HY_1–HY_4 show that any operation in the system needs to be protected by a secure channel. The strength of channel protection is related to the security level of interconnected members, and rules are constrained by 15 and 16.

② The secure channel between ce_i and ce_k is lst_m, that between ce_j and ce_k is lst_n, that between ce_i and ce_j is lst_p, and ce_k is the transit node of secure channels lst_m and lst_n. According to constraints 20 and 21, the direction of information flow is the same when forwarding and exchanging information flow between ce_i-ce_k-ce_j. That is, if ce_i has an inflow to access ce_j, $ce_i \sim> ce_k \sim> ce_j$ is valid, and if ce_j has an outflow to access ce_i, $ce_i <\sim ce_k <\sim ce_j$ is valid. For the switching operations of secure channels, Constraint 20 shows that the transmission information between ce_i and ce_j is protected by lst_m and lst_n, which is visible to ce_k and does not cause aggregation inference problems. Access control follows multilevel security control constraint rules and is proved in Theorem 2. For the forwarding operations of secure channels, Constraint 21 shows that the transmission information between ce_i and ce_j is protected by lst_p, and the encapsulated data are protected by lst_m and lst_n; hence, the transmission information is invisible to ce_k. Following the $ce_i \sim> ce_j$ information flow strategy, the security of policy is proved in Theorem 2. We see that $ce_i \sim> ce_k \sim> ce_j$ and $ce_i <\sim ce_k <\sim ce_j$ information flow strategy $\sim>$ are secure; that is, system M is secure for information flow strategy $\sim>$ in transmission. □

7. Network Architecture and Case Analysis Based on MLS_NSCM

7.1. Fundamental Multilevel Security Virtual Network. According to the MLS_NSCM model, a multilevel security virtual network MLS_VN can be constructed, as shown in Figure 6.

Different security interconnected entities can construct labeled virtual subnets according to their interconnection relationships. Each subnet is constructed on the basis of multiple security channels, and the level of each security channel is determined by the security level of the interconnected members. In each labeled virtual subnet, the subject-object access follows multilevel security control rules, and the security of information transmission is guaranteed by multilevel security channels. In an MLS_VN, when the nodes with communication relationship cannot communicate directly, it needs to follow Constraint 20 and Constraint 21 to forward or exchange secure channels.

The communication between different labeled virtual subnets needs to be routed and forwarded through virtual routing devices, and only the labeled virtual subnets with communication relationship have virtual routing

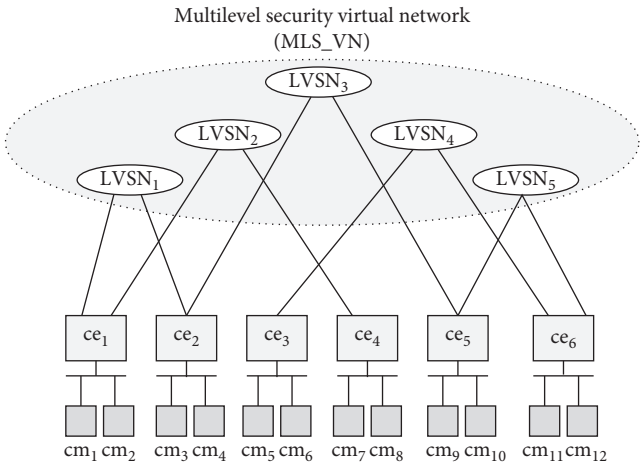

Figure 6: Multilevel security virtual network construction.

relationship. According to the virtual routing relationship, the security channel of the system information flow is encapsulated and unpackaged until the destination of the communication. Figure 7 shows the schematic of secure communication between labeled virtual subnets.

As the figure shows, when subject s in $LVSN_1$ accesses an object in $LVSN_2$, the virtual routing device first determines whether $LVSN_1$ and $LVSN_2$ have a communication relationship. The communication relationship can be either direct or indirect. If so, it can be transmitted through a multilevel secure channel. The data stream from $LVSN_1$ is decrypted and decomposed, and the data stream is encrypted and encapsulated to another secure channel for forwarding, until it reaches the destination labeled virtual subnet $LVSN_2$, thus completing the secure communication between different virtual subnets.

7.2. Typical Application Case and Comparative Analysis of MLS_NSCM Model. To describe the application of the MLS_NSCM model in a real network, this paper presents a typical application case of multilevel network. The MLS_NSCM model was applied in the case, and the characteristics of MLS_NSCM model and the common models are analyzed according to the case. The case is shown in Figure 8.

The application scenario consists of a service platform and protection domains pd_1 and pd_2. The service platform includes a unified security label management subsystem, a subject credibility evaluation subsystem, and an aggregated information level deduction subsystem. The unified security label management subsystem is responsible for the generation, distribution, and maintenance of security labels in the unified security domain; the subject credibility evaluation is responsible for evaluating the credibility of a subject's illegal access and restricting the subject's illegal operation on an object; aggregated information level deduction is responsible for mining object information in the unified security domain, calculating the possibility of aggregated information deducing higher level information, and forming object

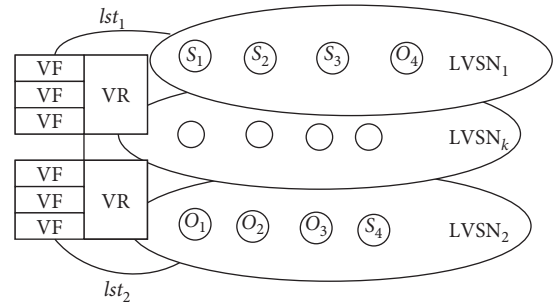

Figure 7: Secure communication between labeled virtual subnets.

relationship tables ORTI and ORTA according to the threshold set by the system.

Assuming that A, B, M, and N are similar objects, with their levels being secret and the access threshold being 3; C and P are related objects, with their levels being secret and confidential, respectively, and the relationship being incompatible. Subject s_1 is classified as secret, and subject s_2 is classified as confidential. It is assumed that there is an interconnection relationship between protection domains.

When the control device receives a request by subject s_1 to access object N, subject and object security labels are compared. Because $cl(s_1) > cl(N)$, s_1 can perform f_w on N, but because N has similar objects, it also checks the access history library of subject s_1. If s_1 has visited objects A, B, and M, it is forbidden to visit object N. Otherwise, access is allowed and transmitted through the secure channel between the interconnected devices i and j. The transmission process follows the secure channel control rules.

When s_1 requests access to object P, because $cl(s_1) > cl(P)$, s_1 is not allowed to access object P. Because of the special application of the network, subject s_1 must visit object P; then, subject s_1 needs to evaluate its credibility. If the credibility of s_1 is greater than the minimum threshold of object P, subject s_1 is allowed to access object P. However, because object C and object P are incompatible, it is checked whether s_1 has visited object C. If s_1 has visited object C, the access of s_1 to object P is prohibited; otherwise, it is allowed. Finally, the secure channel is chosen to encapsulate, encrypt, and authenticate the data according to the channel security parameters to ensure secure data transmission. If the level of object P outflow information is higher than that of subject s_1, the security level of s_1 must be adjusted to that of object P outflow information.

When s_2 requests inflow to access object C, it compares subject and object security labels. Because $cl(s_2) > cl(C)$, s_2 does not allow access to object C. However, owing to the special application of the network, subject s_2 must access object C; hence, the credibility of subject s_2 is evaluated. If the credibility of s_2 is greater than the threshold of the credibility that subject s_2 will not deliberately leak information, its access to object C is allowed. However, because object P and object C are incompatible, it is checked whether s_2 has visited object P. If s_2 has visited object P, the access of s_2 to object C is prohibited; otherwise, it is allowed. It also uses secure channels for transmission. If the level of

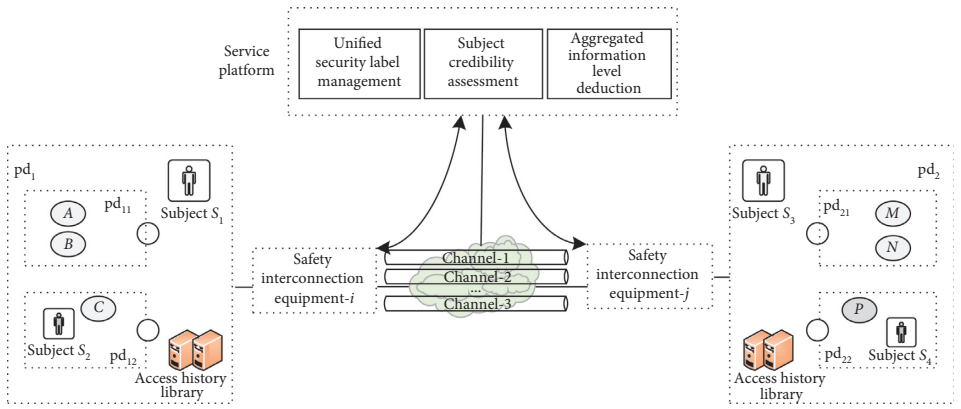

Figure 8: Typical application scenarios of the MLS_NSCM model.

information flowing from subject s_2 to object C is higher than that of object C, a new object C' is created.

By applying the MLS_NSCM model to the above cases, we prove that the model has good compatibility in actual multilevel networks. Through the analysis of the model security described in Section 6, the information flow in the application case of multilevel security networks protected by the model can realize secure transmission and access. In addition, the model provides control methods under special circumstances, such as security control when a subject illegally operates an object and security constraints for aggregation inference problems. This embodies flexibility, expansibility, universality, and other characteristics of the model in its application in multilevel networks.

To better reflect the effectiveness of the MLS_NSCM model, a comparative analysis is performed between the MLS_NSCM model and the common multilevel security models on the basis of the above case.

(1) Labeled-IPsec [31].

This method achieves the integration of IPSec and multilevel security features by adding security tags to the SA. Although this method can realize a secure interconnection between different protection domains and ensure the security of data transmission, IPSec only solves the problem of secure communication between peers. However, a multilevel security network mostly contains nonpeer members. For example, when the security levels of subjects s_1 and s_2 are different, it is impossible to negotiate the secure channel for communication. Moreover, some problems exist, such as cooperation between label access control and IPSec, security communication between heterogeneous information systems, and the aggregation inference of sensitive information, which affect the flexibility of multilevel network communication. In addition, this method only aims to solve the problem of secure interconnection and communication among network members but does not solve the problem of security control of different levels of subject access objects, such as the security access of s_1 to object A in the domain and to object P outside the domain.

(2) Network transmission security control model (NTSCM) [32].

This model provides the method of data transmission between networks of different security levels, thus realizing secure transmission of data between the networks and solving the communication problem between nonpeer members. However, the following problems exist in the model:

① Aggregation inference control problem: when objects A and B are transferred from domain pd_{11} to domain pd_{21}, A, B, M, and N are aggregated. Because they are similar objects and the threshold value is 3, when more than three data are aggregated, it is easy to infer the high-level information, which leads to the risk of leakage. When object C is transferred from domain pd_{12} to domain pd_{22}, if it is aggregated with its associated object P, it is easy to infer high-level sensitive information through analysis, leading to leakage. When the data are transmitted in two directions, there is also the problem of leakage caused by aggregation inference.

② This model does not address the security operation between subjects and objects at different levels in the network, and there are security risks in data access. For example, if low-level subject s_1 illegally accesses high-level object P, if it is not protected, sensitive information in P will be leaked.

(3) Multilevel security model based on noninterference theory in cloud (DIFC-B) [33].

This model uses the idea of distributed information flow control and combines the Biba model and BLP model to ensure the integrity and confidentiality of multilevel information systems. The model ensures the normal operation between the subjects and the objects in the system. However, the following problems still exist:

Table 1: Characteristics comparison between the MLS_NSCM model and other common models.

Characteristic	Labeled-IPsec	NTSCM	DIFC-B	IFCloud	MLS_NSCM
Access security	✓	✗	✓	✓	✓
Communication security	✗	✓	✗	✗	✓
Flexibility	✗	✓	✗	✓	✓
Generality	✓	✓	✗	✗	✓
Expansibility	✗	✓	✓	✓	✓
Network compatibility	✓	✗	✓	✓	✓
Aggregation inference control	✗	✗	✗	✗	✓

① This model needs to strictly follow the Biba model and BLP model. For example, subject s_1 at the secret level can access objects A and B at the secret level, so when there is an operation violating the rules of the two models, the model cannot operate. For example, subject s_1 requests access to object P, but the security level of s_1 is less than that of object P. According to the DIFC-B model, access is not allowed, but due to the special needs of the subject, s_1 must access P, which cannot be realized in the DIFC-B model; therefore, the model lacks flexibility of access.

② This model only refers to the safe operation of information and does not provide a method to establish the safe channel. Thus, it cannot guarantee the security of information transmission in the network channel. That is, when domain pd_1 transmits information to domain pd_2, the security of information in channels 1, 2, and 3 cannot be guaranteed.

③ This model does not solve the problem that sensitive information is inferred from aggregation among objects, the same as the analysis of point (2)-①.

④ This model is based on the multilevel security model of the cloud platform, which is mainly aimed at the distributed cloud computing environment, with certain limitations and poor generality.

(4) Double-layer information flow control model (IFCloud) [34].

In this model, the subject and the object are tagged with security level labels. Based on the concept of centralized and decentralized information flow control, the double-layer security control of information can be realized, thus solving the security access of the subject to the object in the case and realizing the dynamic adjustment of the security labels. Therefore, better flexibility is achieved. This model does not realize the security protection of data in the process of cross-domain communication, the same as the analysis of point (3)-②. In addition, the model does not have the safety control ability of aggregation inference, the same as the analysis of point (2)-①.

According to the above analysis, the comparative analysis of each model is shown in Table 1.

To sum up, the four common models have certain shortcomings in the aspects such as security, flexibility, network compatibility, generality, and scalability. By contrast, the MLS_NSCM model can realize the security operation and communication of multilevel networks more efficiently.

8. Conclusions

In this study, by analyzing the characteristics of multilevel security networks and the problems associated with existing models, a network security communication model was proposed. The model integrates multilevel security control, protection domain control, security attribute reliability constraint, aggregation inference control, and multilevel security channel establishment. In the model, by introducing the credibility of subjects in confidentiality security attributes, the problem of operation of a subject's illegal access to objects under special circumstances in multilevel security networks is resolved to a certain extent. Furthermore, the method of dealing with subjects and objects after a subject's illegal operation is fully considered to enhance the network availability of the BLP model. By aggregation inference control constraints, the access of the subject to the associated objects is limited, which reduces the risk of information leakage caused by the aggregation of objects and enhances the restriction of the BLP model on the confidentiality security attributes. At the same time, by establishing multilevel security channels, a logical, independent, and multilevel virtual subnet is constructed, which realizes secure interconnection between nonpeer members and ensures the security and noninterference of information transmission. Compared with other models, the proposed MLS_NSCM model exhibits better flexibility, adaptability, and security.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundations of China (grant nos. 61502531 and 61702550)

and the National Key Research and Development Plan (grant nos. 2018YFB0803603 and 2016YFB0501901).

References

[1] L. Ajey, *Cloud Computing-Disruptive Technologies for the Militaries and Security*, vol. 132, pp. 167–185, Springer, Berlin, Germany, 2019.

[2] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 118–131, 2020.

[3] R. Gad, A. A. El-Latif, S. Elseuofi et al., "IoT security based on iris verification using multi-algorithm feature level fusion scheme," in *Proceedings of the 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2019.

[4] A. A. A. EL-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5G networks," *Future Generation Computer Systems*, vol. 100, pp. 893–906, 2019.

[5] K. W. Manpreet, N. H. Malka, and H. Nadeesha, "Cloud computing security issues of sensitive data," *Handbook of Research on the IoT, Cloud Computing, and Wireless Network Optimization*, pp. 60–84, IGI Global, Pennsylvania, PA, USA, 2019.

[6] A. A. A. EL-Latif, M. S. Hossain, and N. Wang, "Score level multibiometrics fusion approach for healthcare," *Cluster Computing*, vol. 22, no. S1, pp. 2425–2436, 2019.

[7] A. A. EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar et al., "Controlled alternate quantum walks based privacy preserving healthcare images in internet of things," *Optics & Laser Technology*, vol. 124, Article ID 105942, 2020.

[8] R. Duan, C. X. Gu, Y. F. Zhu et al., "Efficient identity-based fully homomorphic encryption over NTRU," *Journal on Communications*, vol. 38, pp. 66–75, 2017.

[9] L. Li, M. S. Hossain, A. A. A. EL-Latif, and M. F. Alhamid, "Distortion less secret image sharing scheme for Internet of Things system," *Cluster Computing*, vol. 22, no. S1, pp. 2293–2307, 2019.

[10] A. A. EL-Latif, B. Abd-El-Atty, S. Elseuofi et al., "Secret images transfer in cloud system based on investigating quantum walks in steganography approaches," *Physica A: Statistical Mechanics and its Applications*, vol. 541, Article ID 123687, 2020.

[11] A. A. EL-Latif, B. Abd-El-Atty, M. S. Hossain et al., "Efficient quantum information hiding for remote medical image sharing," *IEEE Access*, vol. 6, pp. 21075–21083, 2018.

[12] X. Y. Meng, *Research of Multilevel Security Network*, Xidian University, Xian, China, 2008.

[13] C. Lee, L. H. Yin, and Y. C. Guo, "A cluster-based multilevel security model for wireless sensor networks," in *7th Intelligent Information Processing (IFIP) TC 12 International Conference*, pp. 320–330, Springer, Berlin, Germany, 2012.

[14] P. C. Cheng, P. Rohatgi, and C. Keser, "Fuzzy multi-level security: an experiment on quantified risk- adaptive access control," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 222–230, Berkeley, CA, USA, May 2007.

[15] Z. Y. Tan, D. Liu, and T. G. Gu, "A multilevel security model with credibility characteristics," *Acta Electronica Sinica*, vol. 36, pp. 1637–1641, 2008.

[16] E. B. David, *Bell–La Padula Model*, Springer, Berlin, Germany, 2011.

[17] Y. B. Bao, *Modeling and Verification of Security Policy System Based on Logic*, University of Chinese Academy of Sciences, Beijing, China, 2012.

[18] L. Gong, *Research on Application Security Transparent Supportive Platform Architecture and Model*, Information Engineering University, Zhengzhou, China, 2013.

[19] H. W. Xue, Y. L. Zhang, Z. E. Guo, and Y. Q. Dai, "A multilevel security model for private cloud," *Chinese Journal of Electronics*, vol. 23, pp. 232–235, 2014.

[20] H. Zhu, Y. F. Xue, Y. Zhang et al., "VMLR: a multilevel security model for virtualization," in *Proceedings of the 2013 5th International Conference on Intelligent Networking and Collaborative Systems*, Xian, China, September 2013.

[21] A. Y. Lan, B. Li, R. S. Huang, X. Zhang, and G. L. Feng, *Research on Network Security Strategy Model*, pp. 389–394, Springer, Berlin, Germany, 2016.

[22] C. Wang, *Research on Multi-Class Interconnected Access Control Model Based on Information Flow Strong Restrain*, Information Engineering University, Zhengzhou, China, 2012.

[23] W. Bai, Q. Wu, and X. P. Zhang, "Improved BLP model for multi-level secure network," *Journal of Computer Applications*, vol. 33, pp. 134–136, 2013.

[24] J. S. Wang, S. J. Liu, and H. B. Zhang, *Research on Multilevel Security Access Control Policy Processing Method*, ITE, London, UK, 2014.

[25] D. Liu, L. Zhang, Y. S. Fu et al., "A communication model in multilevel security network using quantum key," in *Proceedings of the 2015 Chinese Automation Congress (CAC)*, Wuhan, China, November 2015.

[26] M. X. Ma, G. Z. Shi, Y. Q. Wang, and H. J. Wang, "Multilevel secure access control policy for distributed systems," *Chinese Journal of Network and Information Security*, vol. 3, pp. 28–34, 2017.

[27] J. B. Xiong, Z. Q. Yao, J. F. Ma et al., "Action-based multilevel access control for structured document," *Journal of Computer Research and Development*, vol. 50, pp. 1399–1408, 2013.

[28] J. Shao, X. Chen, X. Du, and L. Cao, "Distributed multilevel security core architecture based on noninterference theory," *Journal of Computer Applications*, vol. 33, no. 3, pp. 712–716, 2013.

[29] Q. G. Li, Q. Liu, and Z. G. Qin, "Modeling and simulation of communication network based on topic model," *Journal of Computer Research and Development*, vol. 53, pp. 206–215, 2016.

[30] A. A. A. EL-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, "Secure quantum steganography protocol for fog cloud internet of things," *IEEE Access*, vol. 6, pp. 10332–10340, 2018.

[31] B. Sommerfeld, *Labeld IPsec phase 1: label-aware SADB design*, Sun Microsystems, Santa Clara, CA, USA, 2008.

[32] K. H. Wu and T. Ding, "The research of network transmission security control model," *Advanced Materials Research*, vol. 546-547, pp. 1136–1140, 2012.

[33] N. Zhou, G. Y. Lin, and Z. K. Li, "Multi-level security model based on noninterference theory in cloud," *Netinfo Security*, vol. 12, pp. 21–27, 2015.

[34] Z. Z. Wu, X. Y. Chen, X. H. Du et al., "Enhancing sensitive data security based-on double-layer information flow controlling in the cloud," *Acta Electronica Sinica*, vol. 9, pp. 2245–2250, 2018.

[35] M. Stamp, *Information Security Principles and Practice*, Tsinghua University Press, Beijing, China, 2nd edition, 2013.

[36] M. Su, F. H. Li, and G. Z. Shi, "Action-based multi-level access control model," *Journal of Computer Research and Development*, vol. 51, pp. 1604–1613, 2014.
[37] Y. P. Chi, T. T. Jiang, C. P. Dai, and W. Sun, "Design and implementation on multilevel security mandatory access control system for virtual machine based on BLP," *Netinfo Security*, vol. 10, pp. 1–7, 2016.
[38] Y. M. Liu, Q. K. Dong, and X. P. Li, "Study on enhancing integrity for BLP model," *Journal on Communications*, vol. 31, pp. 100–106, 2010.
[39] S. P. Li and H. B. Sun, "Research on information system security models," *Acta Electronica Sinica*, vol. 31, pp. 1491–1495, 2003.
[40] X. N. Cui, C. L. Wang, Q. Q. Pei, Y. H. Li, and Y. L. Shen, "Multiple security partition communication mechanism based on MILS CORBA," *Computer Science*, vol. 40, pp. 38–41, 2013.
[41] J. Rushby, "Noninterference, transitivity, and channel-control security policies," Technical report CSL-92-02, Stanford Research Institute, Menlo Park, CA, USA, 1992.
[42] C. D. Lv, *Research on Information Flow Security of Cloud Computing Based on Noninterference Models*, Beijing Jiaotong University, Beijing, China, 2016.
[43] L. Zhang, X. S. Chen, L. Liu, and X. Jin, "Trusted domain hierarchical model based on noninterference theory," *The Journal of China Universities of Posts and Telecommunications*, vol. 22, pp. 7–16, 2015.
[44] L. Gong, L. Tian, and F. L. Zhang, "Application information flow non-interference transmission model," in *Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology*, Harbin, China, September 2011.
[45] W. P. Liu and X. Zhang, "Research of duality and multi-level security model based on intransitive noninterference theory," *Journal on Communications*, vol. 30, pp. 52–58, 2009.
[46] X. Zhang, *Researches on Non-interference Trusted Model and the Implementation of Trusted Computing Platform Architecture*, Information Engineering University, Zhengzhou, China, 2009.
[47] X. U. Fu, "Intransitive noninterference trusted model supporting process codes modification," *Computer Engineering*, vol. 39, pp. 150–153, 2013.