Implementation of AI-Based and Day-Based Access Control Function in DACS-Based PBNM Scheme

Kazuya Odagiri,[†] Shogo Shimizu[††], Naohiro Ishii[†††]

[†] Sugiyama Jogakuen University, 464-8662, 17-3Hosigaokamotomachi Chiksa-ku,Nagoya, Aichi, Japan
[††] Gakushuin Women's College, Tokyo, Japan
[†††] Advanced Institute of Industrial Technology, Tokyo, Japan

Summary
In the current Internet system, there are many problems using anonymity of the network communication such as personal information leaks and crimes using the Internet system. This is why TCP/IP protocol used in Internet system does not have the user identification information on the communication data, and it is difficult to supervise the user performing the above acts immediately. As a study for solving the above problem, there is the study of Policy Based Network Management (PBNM). This is the scheme for managing a whole Local Area Network (LAN) through communication control for every user. In this PBNM, two types of schemes exist. As one scheme, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme with affinity with existing internet. By applying this DACS Scheme to Internet system management, we will realize the policy-based Internet system management. In this paper, AI-Based and Day-Based automatic access control function in DACS-based PBNM Scheme is implemented.

Keywords:
policy-based netwok management; DACS Scheme; NAPT; AI

1. Introduction

In the current Internet system, there are many problems using anonymity of the network communication such as personal information leaks and crimes using the Internet system. As a study for solving the problems, Policy Based Network Management (PBNM) [2] exists. The PBNM is a scheme for managing a whole Local Area Network (LAN) through communication control every user, and cannot be applied to the Internet system. This PBNM is often used in a scene of campus network management.

In the existing PBNM, there are two types of schemes. The first is the scheme of managing the whole LAN by locating the communication control mechanisms on the path between network servers and clients. The second is the scheme of managing the whole LAN by locating the communication control mechanisms on clients.As the second scheme, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme. As the works on the DACS Scheme, we showed the basic principle of the DACS Scheme, and security function [14]. After that, we implemented a DACS System to realize a concept of the DACS Scheme. By applying this DACS Scheme to Internet system, we will realize the policy-based Internet system management. Then, the Wide Area DACS system (wDACS system) [15] to use it in one organization was showed as the second phase for the last goal. As the first step of the second phase, we showed the concept of the cloud type virtual PBNM, which could be used by plural organizations [16]. After it, basic system design for PBNM scheme for multi-domain management utilizing data science and AI is proposed [17]. In this paper, an AI-Based and Day-Based automatic access control function realizing on it is shown.In Section 2, motivation and related research for this study are described. In Section 3, the existing DACS Scheme is described. In section 4, implementation result of the AI-Based and Day-based automatic access control function is described.

2. Motivation and Related Research

In the current Internet system, problems using anonymity of the network communication such as personal information leak and crimes using the Internet system occur. Because TCP/IP [1] protocol used in Internet system does not have the user identification information on the communication data, it is difficult to supervise the user performing the above acts immediately. However, it becomes possible to use PBNM, which has two types of schemes. The first scheme is the scheme described in Figure 1. The standardization of this scheme is performed in various organizations. In IETF, a framework of PBNM [2] was established. Standards about each element constituting this framework are as follows. As a model of control information stored in the server called Policy Repository, Policy Core Information model (PCIM) [3] was established. After it, PCMIe [4] was established by extending the PCIM. To describe them in the form of Lightweight Directory Access Protocol (LDAP), Policy Core LDAP Schema

Manuscript received January 5, 2026
Manuscript revised January 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.1.3

(PCLS) [5] was established. As a protocol to distribute the control information stored in Policy Repository or decision result from the PDP to the PEP, Common Open Policy Service (COPS) [6] was established. Based on the difference in distribution method, COPS usage for RSVP (COPS-RSVP) [7] and COPS usage for Provisioning (COPS-PR) [8] were established. RSVP is an abbreviation for Resource Reservation Protocol. The COPS-RSVP is the method as follows. After the PEP having detected the communication from a user or a client application, the PDP makes a judgmental decision for it. The decision is sent and applied to the PEP, and the PEP adds the control to it. The COPS-PR is the method of distributing the control information or decision result to the PEP before accepting the communication.

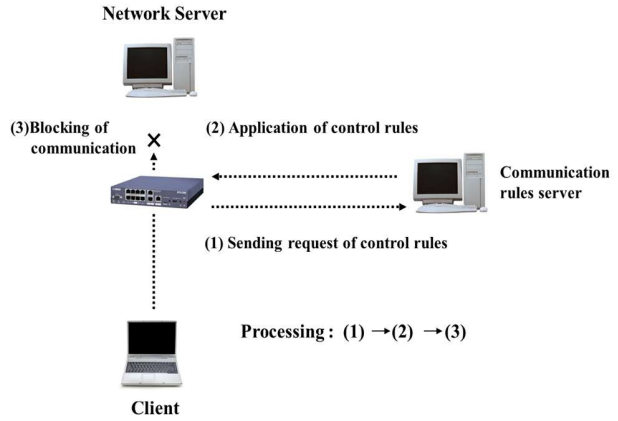

Figure 1. Principle in First Scheme

Next, in DMTF, a framework of PBNM called Directory-enabled Network (DEN) was established. Like the IETF framework, control information is stored in the server storing control information called Policy Server, which is built by using the directory service such as LDAP [9], and is distributed to network servers and networking equipment such as switch and router. As the result, the whole LAN is managed. The model of control information used in DEN is called Common Information Model (CIM), the schema of the CIM (CIM Schema Version 2.30.0) [11] was opened. The CIM was extended to support the DEN [10], and was incorporated in the framework of DEN. In addition, Resource and Admission Control Subsystem (RACS) [12] was established in Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN) of European Telecommunications Standards Institute (ETSI), and Resource and Admission Control Functions (RACF) was established in International Telecommunication Union Telecommunication Standardization Sector (ITU-T) [13].

However, all the frameworks explained above are based on the principle shown in Figure 1. As problems of these frameworks, two points are presented as follows. Essential principle is described in Figure 2. To be concrete, in the point called PDP (Policy Decision Point), judgment such as permission and non-permission for communication pass is performed based on policy information. The judgment is notified and transmitted to the point called the PEP, which is the mechanism such as VPN mechanism, router and Fire Wall located on the network path among hosts such as servers and clients. Based on that judgment, the control is added for the communication that is going to pass by.

The principle of the second scheme is described in Figure 3.By locating the communication control mechanisms on the clients, the whole LAN is managed. Because this scheme controls the network communications on each client, the processing load is low. However, because the communication control mechanisms need to be located on each client, the work load becomes heavy.

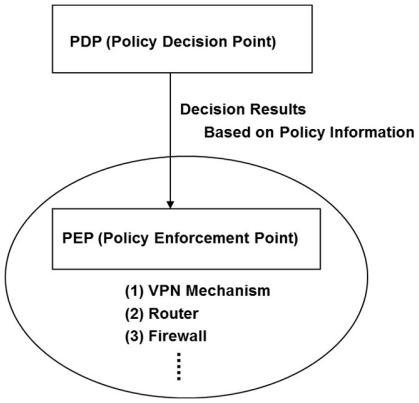

Figure 2. Essential Principle

When it is thought that Internet system is managed by using these two schemes, it is difficult to apply the first scheme to Internet system management practically. This is why the communication control mechanism needs to be located on the path between network servers and clients without exception. On the other hand, the second scheme locates the communication controls mechanisms on each client. That is, the software for communication control is installed on each client. So, by devising the installing mechanism letting users install software to the client easily, it becomes possible to apply the second scheme to Internet system management. As a first step for the last goal, we showed the Wide Area DACS system (wDACS) system [15]. This system manages a wide area network, which one organization manages. Therefore, it is impossible for plural organizations to use this system. Then, as the next step, we showed the cloud type virtual PBNM, which could be used by plural organizations in this paper.

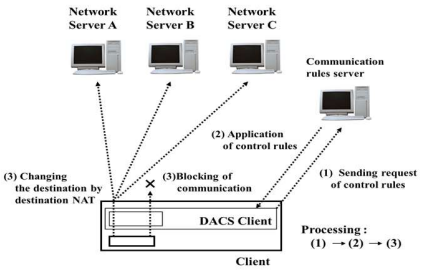

Figure 3. Principle in Second Scheme

3. Existing DACS SCHEME and wDACS System

In this section, the content of the DACS Scheme which is the study of the phase 1 is described.

3.1 Basic Principle of the DACS Scheme

Fig.4 shows the basic principle of the network services by the DACS Scheme. At the timing of the (a) or (b) as shown in the following, the DACS rules (rules defined by the user unit) are distributed from the DACS Server to the DACS Client.

(a) At the time of a user logging in the client.
(b) At the time of a delivery indication from the system administrator.

According to the distributed DACS rules, the DACS Client performs (1) or (2) operation as shown in the following. Then, communication control of the client is performed for every login user.

(1) Destination information on IP Packet, which is sent from application program, is changed.
(2) IP Packet from the client, which is sent from the application program to the outside of the client, is blocked.

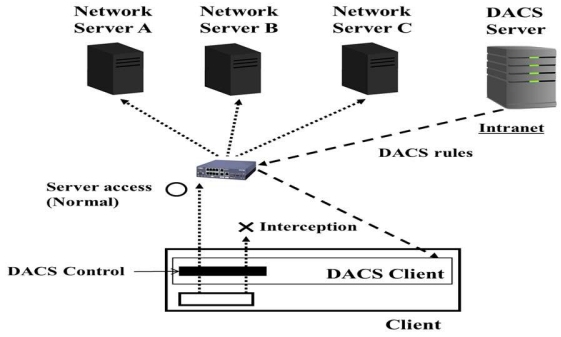

Figure. 4 Basic Principle of the DACS Scheme

An example of the case (1) is shown in Fig.4. In Fig.4, the system administrator can distribute a communication of the login user to the specified server among servers A, B or C. Moreover, the case (2) is described. For example, when the system administrator wants to forbid an user to use MUA (Mail User Agent), it will be performed by blocking IP Packet with the specific destination information.
In order to realize the DACS Scheme, the operation is done by a DACS Protocol as shown in Fig.5. As shown by (1) in Fig.5, the distribution of the DACS rules is performed on communication between the DACS Server and the DACS Client, which is arranged at the application layer. The application of the DACS rules to the DACS Control is shown by (2) in Fig.5.

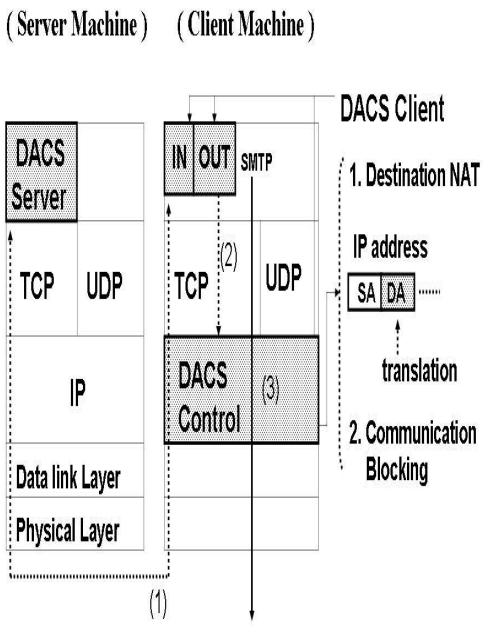

Figure 5 Layer Setting of the DACS Scheme

The steady communication control, such as a modification of the destination information or the communication blocking is performed at the network layer as shown by (3) in Fig.5.

3.2 Application to cloud environment

In this section, the contents of wDACS system are explained in Figure 6.

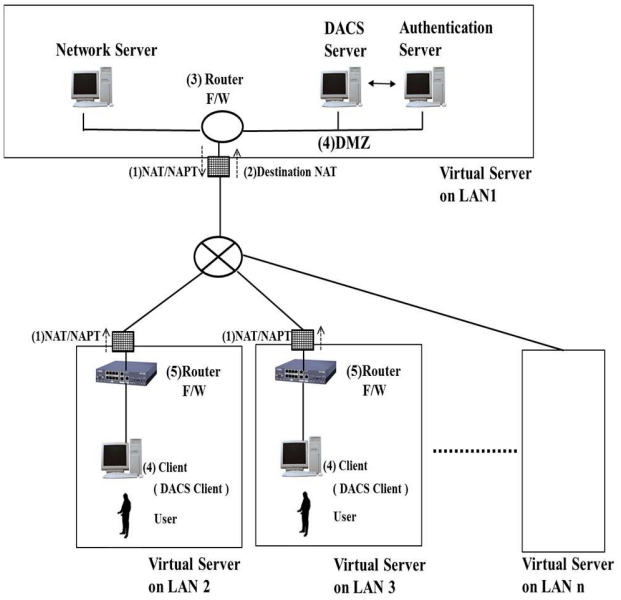

Figure 6. Basic System Configuration of wDACS system

First, as preconditions, because private IP addresses are assigned to all servers and clients existing in from LAN1 to LAN n, mechanisms of NAT/NAPT are necessary for the communication from each LAN to the outside. In this case, NAT/NAPT is located on the entrance of the LAN such as (1), and the private IP address is converted to the global IP address towards the direction of the arrow. Next, because the private IP addresses are set on the servers and clients in the LAN, other communications except those converted by Destination NAT cannot enter into the LAN. But, responses for the communications sent form the inside of the LAN can enter into the inside of the LAN because of the reverse conversion process by the NAT/NAPT. In addition, communications from the outside of the LAN1 to the inside are performed through the conversion of the destination IP address by Destination NAT. To be concrete, the global IP address at the same of the outside interface of the router is changed to the private IP address of each server. From here, system configuration of each LAN is described. First, the DACS Server and the authentication server are located on the DMZ on the LAN1 such as (4). On the entrance of the LAN1, NAT/NAPT and destination NAT exists such as (1) and (2). Because only the DACS Server and network servers are set as the target destination, the authentication server cannot be accessed from the outside of the LAN1. In the LANs form LAN 2 to LAN n, clients managed by the wDACS system exist, and NAT/NAPT is located on the entrance of each LAN such as (1). Then, F/W such as (3) or (5) exists behind or with NAT/NAPT in all LANs

3.3 The Cloud Type Virtual PBNM for the Common Use Between Plural Organizations

In this section, after the concept and implementation of the proposed scheme were described, functional evaluation results are described.

In Figure 7 which is described in [16], the proposed concept is shown. Because the existing wDACS Scheme realized the PBNM control with the software called the DACS Server and the DACS client, other mechanism was not needed. By this point, application to the cloud environment was easy. The proposed scheme in this paper realizes the common usage by plural organizations by adding the following elements to realize the common usage by plural organizations: user identification of the plural organizations, management of the policy information of the plural organizations, application of the PKI for code communication in the Internet, Redundant configuration of the DACS Server (policy information server), load balancing configuration of the DACS Server, installation function of DACS Client by way of the Internet. In the past study [14], the DACS Client was operated on the windows operation system (Windows OS). It was because there were many cases that the Windows OS was used for as the OS of the client. However, the Linux operating system (Linux OS) had enough functions to be used as the client recently, too. Therefore, to prove the possibility of the DACS Scheme on the Linux OS, the basic function of the DACS Client was implemented in this study. The basic functions of the DACS Server and DACS Client were implemented by JAVA language.

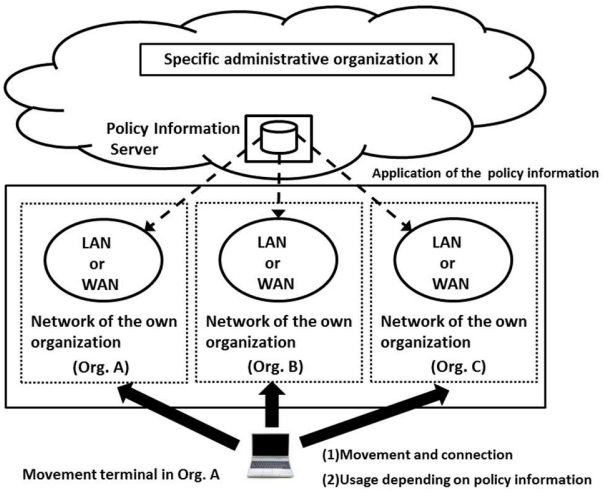

Figure 7. Cloud Type Virtual PBNM for the Common Use between Plural Organizations

3.4 The Cloud Type Virtual PBNM for the specific domain

This scheme is to manage the plural networks group. In Figure 8, the content of it is explained. Specifically, as a logical range to manage organization A and organization B, network group 1 exists. Similarly, as a logical range to manage organization C and organization D, network group 2 exists. These individual network groups are existing methods listed in Figure 7. When plural network groups managed by this existing scheme exist, those plural network groups are targeted for management by this proposed method.

For example, when user A belonging to org. A in network group1 uses the network which org. C belonging to network group2 which is a different network group holds, administrative organization Y for network group2 refers for policy information of user A for administrative organization X of network group1 and acquires it. After it, in the form that policy information registered with Network Group2 beforehand is collated with the policy information, the final policy information is decided. As a result, the policy information is applied to the client that user A uses in network group2, and the communication control on the client is performed. When a user moves plural network groups as well as the specific network group, it is thought that the PBNM scheme to keep a certain constant management state is realized.

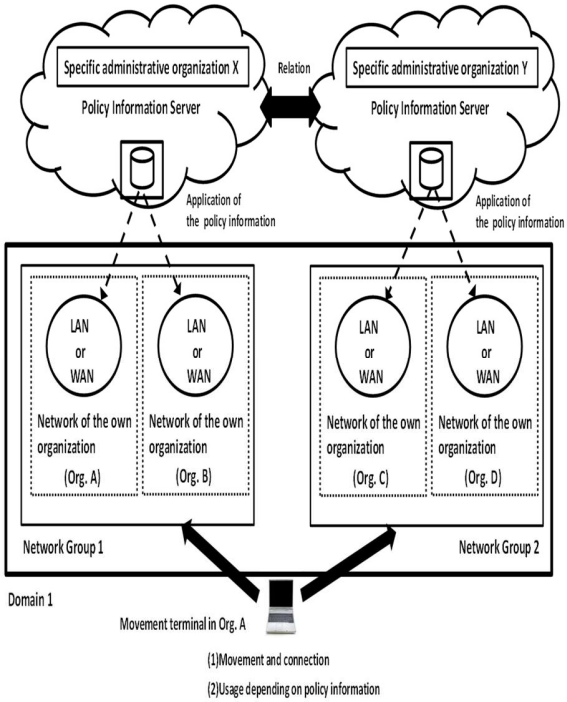

Figure 8. Cloud Type Virtual PBNM for the Specific Domain

The proposed user authentication system also has a distributed system form. For example, when user A belonging to org. A in network group1 accesses the network of the network group1, the user authentication process is generated for the user authentication server for the network group1. On the other hand, when user A belonging to org. A in network group1 accesses the network of the network group 2, the user authentication process is generated for the user authentication server for the network group1 as Figure.9.

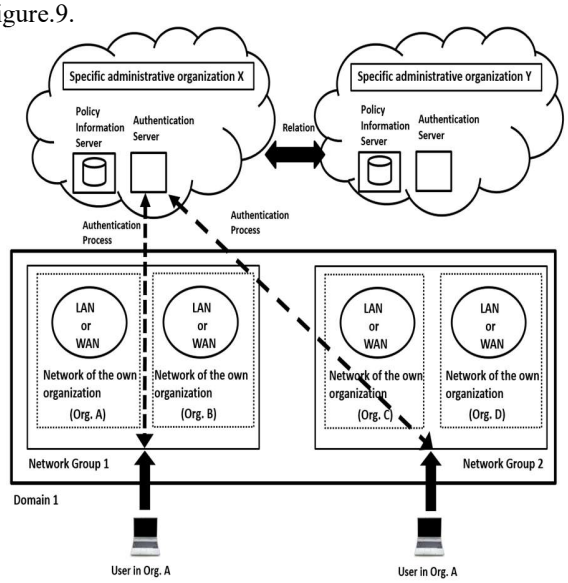

Figure 9. Concept of the proposed user authentication method

3.5 AI-Based Cloud Type Virtual PBNM for the Specific Domain

In this section, concept of cyber physical type of Internet PBNM is described.

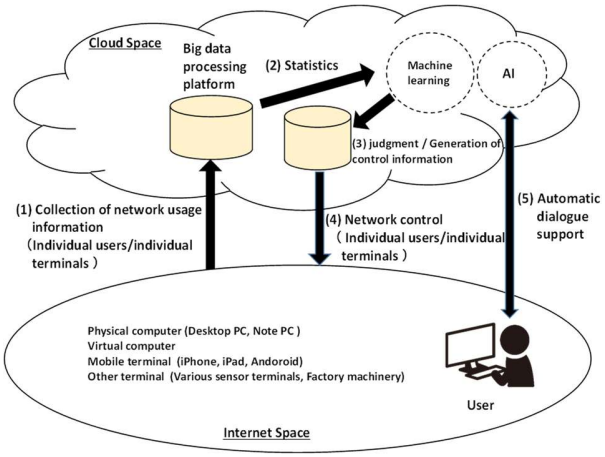

Figure 10. Image of cyber physical Type of Internet PBNM

To extend to the proposed scheme described in the previous chapters, operation automation of the proposed scheme is required. Since the Internet system is an autonomous decentralized network, network operation management is performed for each organizational unit. Therefore, it is also necessary to make the proposed scheme an operation management scheme that can support autonomous decentralized type. In some cases, it may be possible to collectively manage the operation of a certain range of networks. Therefore, it is necessary to automate operation management as much as possible. Therefore, it is necessary to adopt a scheme that supports cyber-physical systems that utilize AI, big data, and IOT as shown in Figure 10.

4. Implementation result of Ai-Based and Day-Based Automatic Access Control Function in DACS-Based PBNM Scheme

In Figure.10, system process of AI-Based automatic access control function is described. Through Processes from (1) to (8), the access control function is activated. First, when a user accesses many kinds of network services, the access logs for them are delivered to DACS Server from DACS Client each time, and stored as big date in a NO SQL database system such as Hadoop. They are aggregated and stored in Relational Database Management System (RDBMS) as PostgreSQL as statical date. The process up to this point is implemented using the JAVA language. Next, the statical data in RDBMS is converted to csv file format data, and taken into AI as learning data. The AI makes predictions based on time series analysis, and makes a prediction data. For example, it predicts the number of accesses from a specific client to a specific server in the future, such as the next day, next week, or next month. The process up to this point is implemented using the Python.

Based on that prediction, DACS rules are recreated on DACS Server. Then, they are sent and applied to DACS Client, and the future web access will be recontroled. In Figure.7, Initially, Web SV1 was accessed, but as a result of recontrol, it was changed to access Web SV2. The important point to note here is that Web SV1 and Web SV2 are servers with the same content and are subject to access control.

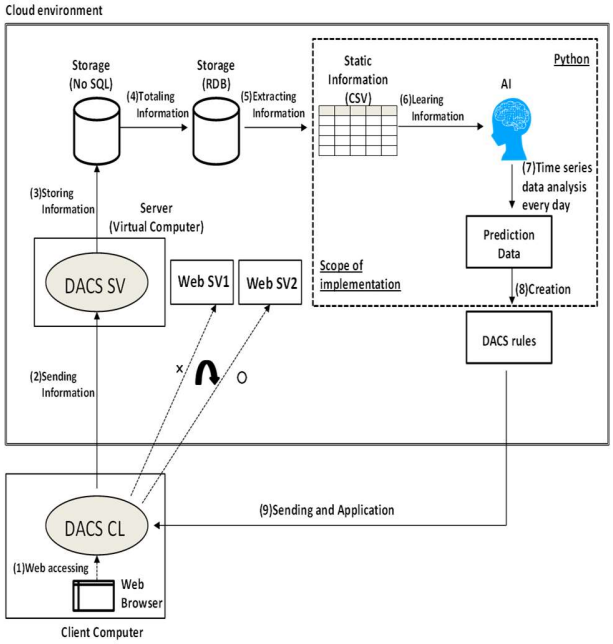

Figure 11.AI and Day-Based Automatic Access Control Function PBNM

The range of this implementation is the dotted line in the upper right corner of Figure 11. From here, the implementation results will be shown. In figure.8, The format and part of sample data of the csv-file extracted from RDB is shown. The rightmost column shows the number of times that a user using a particular client accesses a particular server during the day.

user_name	rev-IP-Address	dest-IP-Address-before	dest-IP-Address-after	Port	Date	Access-num
user1	133.24.224.2	145.44.232.3	165.28.219.4	80	2023/1/1	180
user1	133.24.224.2	145.44.232.3	165.28.219.4	80	2023/1/2	460
user1	133.24.224.2	145.44.232.3	165.28.219.4	80	2023/1/3	395
user1	133.24.224.2	145.44.232.3	165.28.219.4	80	2023/1/4	231
user1	133.24.224.2	145.44.232.3	165.28.219.4	80	2023/1/5	353
user1	133.24.224.2	145.44.232.3	165.28.219.4	80	2023/1/6	160
user1	133.24.224.2	145.44.232.3	165.28.219.4	80	2023/1/7	345
user1	133.24.224.2	145.44.232.3	165.28.219.4	80	2023/1/8	461
user1	133.24.224.2	145.44.232.3	165.28.219.4	80	2023/1/9	327
user1	133.24.224.2	145.44.232.3	165.28.219.4	80	2023/1/10	370

Figure.8 Extracted csv file

```
[12]: import csv
      import numpy as np
      import pandas as pd

[13]: from prophet import Prophet

[14]: df = pd.read_csv('in.csv')

[15]: #Processing to extract 2 columns
      df=df.loc[:,['Date','Access-num']]

      #Column name change process
      df.columns=['ds','y']

[16]: #Implementation process of time-series future prediction
      m=Prophet()
      m.fit(df)
      future = m.make_future_dataframe(periods=1)

      15:51:33 - cmdstanpy - INFO - Chain [1] start processing
      15:51:33 - cmdstanpy - INFO - Chain [1] done processing

[17]: forecast = m.predict(future)

[18]: #Predicted value acquisition process
      df_forecast=forecast[['ds', 'yhat']].tail(1)
      df_forecast['yhat']

[18]: 424    285.000388
      Name: yhat, dtype: float64
```

Figure.9 Implementation Code by Python

In Figure.9, a prototype program code for time series forecasting using Prophet was shown. After importing the csv file, we converted it to a data frame using Pandas. After that, I extracted the two columns to be analyzed (the date column and the access count column every day) and changed them to the necessary data column names to input them into Prophet. Finally, we fed the data into a machine learning model created using Prophet to predict the number of accesses for the next day. With this sample data, the predicted number of accesses for the next day was approximately 285.A mechanism will be introduced to calculate whether the T-statistic falls within or deviates from the 95% interval, and if it does deviate, access will be blocked.After this process, it is necessary to add a process to change the value of DACA rules based on a preset threshold value, so that if the value deviates from the threshold value range, the communication destination server is changed. The subsequent processing begins in the processing phase of existing programs written in Java.

5. Conclusion

In this paper, AI-Based automatic load balancing function is proposed. In the near future, detailed design, implementation, and evaluation of this proposed method will be carried out. Completion of this method will provide a basis for extending the proposed method to a wider range of the entire Internet.

References

[1] V. CERF and E. KAHN, “A Protocol for Packet Network Interconnection,” IEEE Trans. on Commn, vol.COM-22, May 1974, pp.637-648.

[2] R. Yavatkar, D. Pendarakis and R. Guerin, “A Framework for Policy-based Admission Control, ” IETF RFC 2753, 2000.

[3] B. Moore at el., “Policy Core Information Model -- Version 1 Specification, ” IETF RFC 3060, 2001.

[4] B. Moore., “Policy Core Information Model (PCIM) Extensions, ” IETF 3460, 2003.

[5] J. Strassner, B. Moore, R. Moats, E. Ellesson, “ Policy Core Lightweight Directory Access Protocol (LDAP) Schema,” IETF RFC 3703, 2004.

[6] D. Durham at el., “The COPS (Common Open Policy Service) Protocol, ” IETF RFC 2748, 2000.

[7] S. Herzog at el., “COPS usage for RSVP,” IETF RFC 2749, 2000.

[8] K. Chan et al., “COPS Usage for Policy Provisioning (COPS-PR),” IETF RFC 3084, 2001.

[9] CIM Core Model V2.5 LDAP Mapping Specification, 2002.

[10] M. Wahl, T. Howes, S.Kille, “Lightweight Directory Access Protocol (v3),” IETF RFC 2251, 1997.

[11] CIM Schema: Version 2.30.0, 2011.

[12] ETSI ES 282 003: Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN); Resource and Admission Control Subsystem (RACS); Functional Architecture, June 2006.

[13] ETSI ETSI ES 283 026: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification, April 2006.

[14] K. Odagiri, R. Yaegashi,M. Tadauchi, and N. Ishii, “Secure DACS Scheme, “Journal of Network and Computer Applications,” Elsevier, Vol.31, Issue 4, 2008, pp.851-861, November.

[15] K. Odagiri, S. Shimizu,M. Takizawa and N. Ishii, “Theoretical Suggestion of Policy-Based Wide Area Network Management System (wDACS system part-I),” International Journal of Networked and Distributed Computing (IJNDC), Vol.1, No.4, November 2013, pp.260-269.

[16] K. Odagiri,S. Shimizu, N. Ishii, M. Takizawa, “Suggestion of the Cloud Type Virtual Policy Based Network Management Scheme for the Common Use between Plural Organizations,” Proc of Int. Conf. on International Conference on Network-Based Information Systems (NBiS-2015),pp.180-186,Septmber, 2015

Kazuya Odagiri received the degree of B.S in 1998 from Waseda University. He is an Associate Professor in Sugiyama Jogakuen University now. In addition, he got his Ph.D. in Aichi Institute of Technology. He engages in a study of network management.

Shyogo Shimizu received the degree of B.S in 1996 from Osaka University and the degree of M.S in 1998 from Nara Institute of Science and Technology, Nara. He got his Ph.D. in Nara Institute of Science and Technology in March 2001. He is now Associate Professor in Gakushuin Women’s College.

Naohiro Ishii received the B.E., M.E. and Dr. of Engineering degree from Tohoku University, Japan in 1963, 1965 and 1968, respectively. He was a professor in Department of Intelligence and Computer Science at Nagoya Institute of Technology. From 2003, he was a professor in Department of Information Science at Aichi Institute of Technology until 2019. He belongs to Advanced Institute of Industrial Technology now. His research interest includes computer engineering, artificial intelligence, and human interface.