DOI: 10.23977/jaip.2023.060404
ISSN 2371-8412 Vol. 6 Num. 4

Security Impact of Federated and Transfer Learning on Network Management Systems with Fuzzy DEMATEL Approach

Safiye Turgay[1,a,*], Suat Erdoğan[2,b]

[1]Department of Industrial Engineering, Sakarya University, Sakarya, Turkey
[2]Maro International Information Technologies Consulting Development, Support Services Industry and Trade Joint Stock Company, İstanbul, Turkey
[a]safiyeturgay2000@yahoo.com, [b]suat_er@hotmail.com
[*]Corresponding author

Keywords: Fuzzy DEMATEL; Autonomic Network Management; Federated Learning; Transfer Learning; Security; Big Data

Abstract: Everyday using of the big data, machine learning algorithms, and related studies, ensuring data privacy and security have become a critical necessity. These features make them more vulnerable to cyber-attacks. The security of the stored data is also critical, and evaluating the processing of information in the autonomous network management of these systems. The criteria considers the account in the processing and security of data entering every field from the widespread industry examined. It is necessary to increase their awareness of negative and attack problems while these systems are working. Applications such as traditional machine learning and the use of cloud computing also involve risks regarding data security and personal data leakage. Cooperative learning pays due attention to the confidentiality of sensitive information by keeping the original training data hidden. By collecting, combining, and integrating heterogeneous data with collaborative learning together with a federated learning structure, data produced and stored. This study discusses the effect of federated and transfer learning on autonomous network management analyzes the security status parameters. The fuzzy DEMATEL method was preferred in exploring the parameters affecting the system state according to the degree of importance. Situational scenarios evaluated by considering the structure in which the features of cyber-physical systems examined together with federated learning. Data security factors discussed with the fuzzy DEMATEL

1. Introduction

Federated learning aims to solve the problem changing the data itself. The federated learning methodology can be adapted to create two models simultaneously in a multi-tasking learning framework if one also wants to adjust the results to its specific situation. Only machine learning parameters change, perform direct computations on encrypted data without prior decryption. These parameters can leak information about the underlying data samples despite such protective measures by performing multiple custom queries on specific datasets. Nodes' ability to query is an essential point of attention. In this study, the data privacy-based federated learning method and related criteria examined.

Federated learning allows resource-constrained edge devices such as cell phones and IoT (Internet of Things) machines to learn a shared model for prediction while keeping training data local. The primary purpose of this distributed structure minimizes the total loss function value. Statistical and systematic difficulties in training models with federated learning on distributed local devices make it challenging to apply in the real world. This approach contrasts traditional centralized machine learning techniques and classical decentralized methods discussed in distributed similarly.

Evaluation of the autonomous network management system is crucial for maintaining system performance and subsequent system behaviour for security with federated and transfer learning. This study focused on identifying the factors underlying federated and shared learning in the autonomous network management system, which are the best predictors of providers' organizational performance, and evaluating the impact of these factors on performance.

The primary purpose of the presented study is to develop a strategic performance measurement system using fuzzy DEMATEL to evaluate hybrid transfer learning strategies. It does not focus on any particular direction to translate the system's strategic goals into sensible performance metrics while minimizing information overload. The fuzzy DEMATEL preferred to examine the factors affecting each other comprehensively.

This study organized into five sections. A literature review of the performance appraisal approach focused on federated learning, and transfer learning presented in section 2. Section 3 presents the used techniques and. Section 4 applies and discusses the approach to rank the factors affecting federated learning and transfer learning in defined performance criteria. Finally, section 5 includes the conclusion and results.

2. Literature Survey

A Federated learning style feeds the central model from local models without seeing their data in machine learning applications. Local models train the model on its dataset. The weights and features of the trained model transferred to the central model. The primary model updated according to the incoming parameters. After the update, the new parameters transferred to the local models. Thanks to this set of values, the central model can work with high accuracy and performance without seeing the data. Confidentiality and security of both central and local parameters get essential when developing applications in federated learning. The application of federated knowledge that enables the development of performance machine learning models, especially in health, education, and banking, in which data privacy is essential.

Rahatulain and Onari examined and proposed the cyber security model structure for manufacturing systems[1,2]. Skowrariski reviewed the blockchain-based multi-agent system architecture model for the cyber-physical system [3]. Also, Bolbot et al. conducted an extensive literature review and discussed the advantages and disadvantages of the cyber-physical system [4]. Hoffmann et al. developed a risk-based approach to cyber security and risk management model and defined risk definitions and measures [5]. Marotta et al. reviewed of cyber-insurance analysis comprehensively [6]. So, Ruan examined the cyber risk measurement architectural structure with an economic perspective and developed a risk calculation model [7]. Su et al. studied on Android-based mobile cyber-physical systems [8]. Akintolobu et al. analyzed future situations with the cyber risk assessment model [9]. Muhhopadhyay and his colleagues have explored the cyber-risk decision model [10]. Cardin addressed the issue of cyber security in production systems applications [11].

Barrere and colleagues examined the defence strategy structure of cyber security in industrial control systems, which can be achieved with minimal effort[12]. Yaacoub et al. determined the limits, problems and future situations that may be encountered in the security structure of cyber-physical systems [13].

Some of the studies related to the federated learning, which given in below. Bendiab et al. analysed the cloud federated identify management structure with a fuzzy cognitive map[14]. Tchoffa et al. examined product lifecycle management and federated learning structure with factory application [15]. Polap and his colleagues suggested the intelligent medical system together with federated learning and block chain structure and agent architecture [16]. Xia et al. have studied the federated learning structure in detail [17]. Ali et al. reviewed the definition of federated learning, its characteristics and its application in the IOT system [18]. With "Federated Learning," the person's privacy is protected, and the needed big data is obtained. Mostly, federated learning applications are related to the multi-user mobile services' use. This study brings the most efficient factors in federated learning which are discussed with the fuzzy DEMATEL approach.

3. Federated Learning

Federated Learning is a collaborative machine learning method where user data never leaves users' devices and the training process distributed among many users (Fig. 1). Federated learning recommended by Google; In order to prevent data privacy, the training model is distributed to more than one device and the training is done on the user devices. In classical machine learning, training data collected in a data, while in federated learning, contact information remains on user devices. The goal in federated learning is to find the vector of a neural network parameter that minimizes the expected empirical loss.

$$w(n+1) = w(n) + \eta(n) g^{w}(n) \tag{1}$$

3.1. Federated Learning Types

The solution of problems in Federated Learning carried out with Horizontal, Vertical and Federated Transfer learning.

3.1.1. Horizontal Federated Learning

It is used different scenarios are present in the examples (Bianco-Justicia et al.)[19]. However, their work is very similar, so the saved user properties are the same. In such cases, a horizontal Federated learning model can be created (Mothukuri et al. and Chen et al.2020) [20-22].

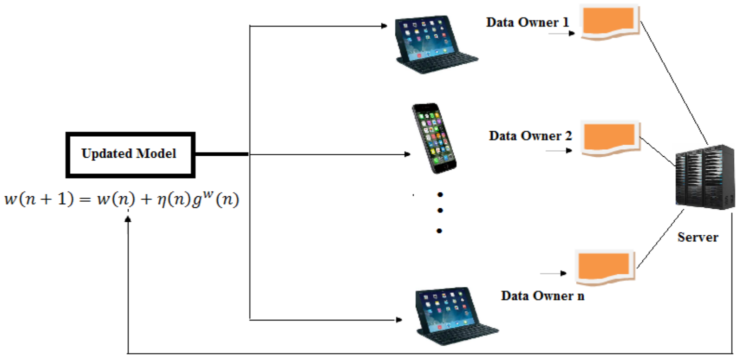


Figure 1: Federated Learning Main Structure

3.1.2. Vertical Federated Learning

It used when two datasets share the same users but differ in feature space (Fig. 2). As an example, suppose a bank and an e-commerce firm have the same customers. Since the records the income and spending behaviour and credit rating of its users, and the e-commerce company records the shopping browsing and purchasing history of its users, the user attributes are different from each other. Therefore, the size of the dataset that customers create is very large. The Vertical Federated Learning method is a computational process that can bring together and offer shopping suggestions according to the income level of the customers.

3.1.3. Federated Transfer Learning

In federated learning, where such a small number of data can be used to present effective solutions and increase model performances (Fig. 2).

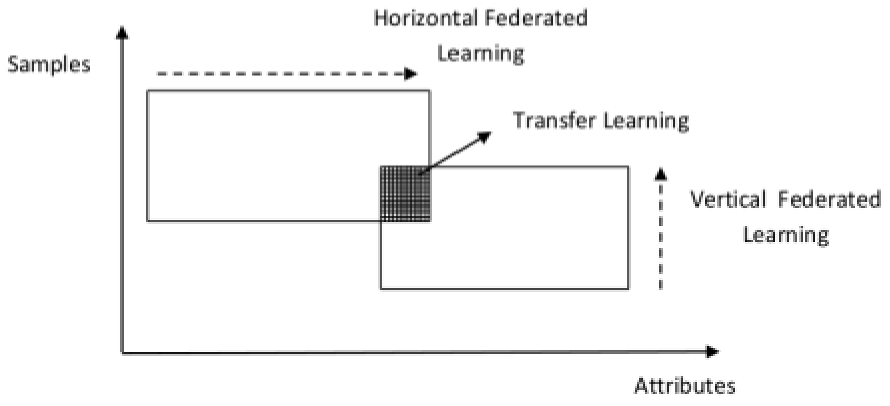


Figure 2: Transfer Learning

Below factors affect the proposed federated to transfer learning framework. These factors evaluated by experts and listed in order of importance with the fuzzy DEMATEL method.

C1- Security and Authentication: Safety and security limits defined and boundaries set. Security limits and risk factors defined together and shared with the end devices in the relevant algorithm application structure, along with model updates. It is very important in terms of privacy, effectiveness and efficiency of the application area of federated learning. The most obvious security threats are communication bottlenecks, backdoor attacks, and poisoning. The process of securely recording user attributes and data requires the use of a strong encryption algorithm.

C2-Privacy- Security: In federated learning, the development of privacy algorithms is important for data security, as privacy data stays on local machines and updates pushed to servers. Within the scope of the privacy approach, there are different data security models;

Secure collection- It is a set of encryption that allows multiple parties to make collective calculations and ensures that the information of the parties entering the information not known to other parties. It used for authentication, encryption and transmission of local updates with the secret share set. It used effectively in application areas such as secure collection, secure auction, confidentiality-protected estimation and comparison.

Differential Privacy: In this model, noise added to the incoming data. At the same time, data security ensured by hiding the information comes from. These processes done with methods such as input, output perturbation, objective perturbation or exponential mechanism. The trained modelling applied primarily to centralized datasets.

C3-Reliability: In order to ensure the protection of data privacy, it aimed to ensure the reliability of the data in the personalization datasets to increase performance, by collecting them from mobile devices and backing up the data on mobile devices with a global mobile update process. An example is the unreliable update status of low-quality data due to high-speed activity, which can be in a data poisoning attack. In mobile networks, it has been revealed that the reliability of unified learning tasks is increased, thus meeting the requirements of reliability, sustainability, usability and security.

C4- Anonymity: The ability to protect user privacy, the user's f-anonymity model, and the training of the data with the model parameters and algorithm instead of sharing the information, allows the data to uses in an educated manner with the changing datasets trial arrangements.

C5- Limited Disclosure: The ability to request a minimum number of user attributes and use them only for specified purposes. Scalability allows for resource optimization and selection of edge devices according to their computational power.

C6- Communication: The process enables the exchange of user attribute requests with a special encryption algorithm over secure channels by using secure communication protocols such as HTTPS and SSL. The basic structure is that multiple devices can use a common machine-learning algorithm without sharing their private data. Multiple devices are required to change learned model updates frequently and it is very important for federated learning and transfer learning to use a common communication line properly. Therefore, the necessity of using collaborative machine learning structure in the use of large-scale network structure such as the Internet of Things arises. The necessity of using the distributed algorithm is emerging for the transmission and the communication infrastructure to respond to this load. With the combination of federated learning and machine learning algorithms, intelligent, autonomous decision-making and inference performed.

C7- Integrity: It uses the process of ensuring the integrity of identity information with the control and verification mechanism. It is the making of necessary inferences by using machine learning algorithms together with private data and collective and general data. It aims to ensure data integrity, take the necessary precautions against possible attacks and protect the integrity structure.

C8-Interoperability: The assessment of data compatibility depends on user trust; interoperability emerges as a personalized nature of the collaborative learning process. It aimed to determine the outlier data sets evaluate the local data distribution performances and to find the integration structure with the minimum deviation. The degree of integration checked by the central server.

C9- Availability: The ability of the system, such as a high percentage of uptime.

C10 – Authorization: It takes into account the data privacy structure with the scalable.

4. Fuzzy DEMATEL Method

DEMATEL (The Decision Making Trial and Evaluation Laboratory) method groups the factors in a cause-effect structure to analyse the causal relationship. It has also been successfully applied in some areas and possible to analyse the uncertain situations, especially with the fuzzy DEMATEL method. It has a wide application range of multi-criteria decision-making problems.

4.1. DEMATEL process steps

Step 1: Determination of the problem criteria and fuzzy evaluation scale.

At this stage, n factors affecting each other and evaluates by m decision makers determined to use in the solution of the problem. According to the problem, the decision makers and/or making uses the literature decided by taking the opinion those factors should be choose. Decision makers (in Table 1) create significant relationships between identified factors. $M_{g_i}^1, M_{g_i}^2, \dots, M_{g_i}^m$ where all the $M_{g_i}^{j} (j = 1, 2, \dots m)$ are triangular fuzzy numbers (TFNs).

Step2: Creating the direct relationship matrix.

A pair wise comparison matrix with linguistic expressions is created by each expert to measure the level of relations between the criteria $\{C_1,C_2,\dots,C_n\}$. Assuming that the decision group consists of p experts, p decision matrices obtained. It represented as a fuzzy direct relationship matrix. It is formed by taking the average which performed by H number of experts. The fuzzy direct relation matrix has dimensions of n x n and is calculated using the equation (2) below [23-25].

$$\tilde{a}_{ij} = \frac{1}{N}\sum_{k=1}^{N} \tilde{x}_{ij}^{k} \tag{2}$$

It creates the fuzzy direct relationship matrix, pair wise comparisons which made between the factors by using linguistic expressions by the decision makers. Thus, the effect of one factor on another factor tried to measure. Since there are m decision makers, m direct relationship matrices of nxn size obtained.

Table 1: The Linguistic variables and triangular fuzzy numbers for importance

Linguistic variables	Fuzzy number	Triangular fuzzy number	Triangular fuzzy reciprocal number
Equally Important (EI)	$\tilde{1}$	(1, 1, 3)	(1/3, 1, 1)
Weekly Important (WI)	$\tilde{3}$	(1, 3, 5)	(1/5, 1/3, 1)
Strongly Important (SI)	$\tilde{5}$	(3, 5, 7)	(1/7, 1/5, 1/3)
Very Important (VI)	$\tilde{7}$	(5, 7, 9)	(1/9, 1/7, 1/5)
Absolutely Important (AI)	$\tilde{9}$	(7, 9, 9)	(1/9, 1/9, 1/7)

$\tilde{X}\left(\tilde{X} = [\tilde{x}_{ij}]_{m\times n}\right.$, the fuzzy mean matrix obtained by normalizing $\tilde{A}$ using equations (3) and (4).

$$\tilde{X} = \lambda \times \tilde{A} \tag{3}$$

$$\lambda \;= \min\left[\frac{1}{\max_i \sum_{j=1}^{n}|a_{ij}|}, \frac{1}{\max_j \sum_{i=1}^{n}|a_{ij}|}\right] \tag{4}$$

Step 3. The degree of possibility of $M_2 = (l_2, m_2, u_2) \geq M_1 = (l_1, m_1,$ defined (in Fig. 3).

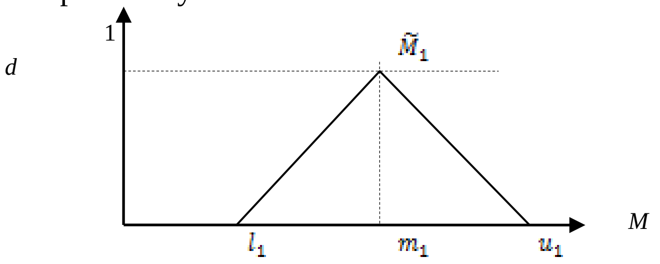


Figure 3: The intersection of the fuzzy number

Step 4: Calculate the total relationship matrix. The fuzzy total relationship matrix calculated with the help of the following equation (5)[26].

$$\tilde{T} = \tilde{X}\left(1 - \tilde{X}\right)^{-1} \tag{5}$$

Step 5: Identification of Influencing and Affected Factors. and values are calculated by summing the total relationship matrix T. I and I values represent direct and indirect relationships between criteria, respectively. It can be calculated with the help of equations (6) and (7).

$$\tilde{D}_i = \sum_{i=1}^{n} \tilde{T}_{ij} \qquad (i = 1,2,\dots,n) \tag{6}$$

$$\tilde{R}_i = \sum_{j=1}^{n} \tilde{T}_{ij} \qquad (j = 1,2,\dots,n) \tag{7}$$

Step 6: Defuzzification of fuzzy values. They contain three values since they still derived from triangular fuzzy numbers. In order to make them a single value, the defuzzification method is applied. At this stage, these values clarified. The defuzzified I and I values are calculated using the following equations (8) and (9). The abbreviation “def” here is an abbreviation of the word “defuzzifying”, which means clarification, and describes the clarrified values[27,28].

$$D_i^{\widetilde{Def}} + R_i^{\widetilde{Def}} = \frac{1}{4}(l + 2n + u) \tag{8}$$

$$D_i^{\widetilde{Def}} - R_i^{\widetilde{Def}} = \frac{1}{4}(l + 2n + u) \tag{9}$$

Step 7: Creating the relationship diagram. The relationship diagram that visually expresses the importance between the criteria and the cause-effect relationship with the total effect is created with the values $\left(D_i^{\widetilde{Def}} + R_i^{\widetilde{Def}}\right)$, $\left(D_i^{\widetilde{Def}} - R_i^{\widetilde{Def}}\right)$.

Step 8: Obtaining the cause-effect relationship diagram. Analysis performed by drawing a cause-effect relationship diagram with the help of the clarification method.
The weights of the criteria are found with the Eq(10) in below.

$$w_i = \left\{D_i^{\widetilde{Def}} + R_i^{\widetilde{Def}^2}\left(D_i^{\widetilde{Def}} + R_i^{\widetilde{Def}}\right)\right\}^{1/2}$$

$$W_i = \frac{w_i}{\sum_{i}^{n} w_i} \tag{10}$$

The $\left(D_i^{\widetilde{Def}} + R_i^{\widetilde{Def}}\right)$ value represents the importance and the total effect value of the criteria, while the $\left(D_i^{\widetilde{Def}} - R_i^{\widetilde{Def}}\right)$ value determines the direction of the relations between the criteria and allows them grouped as cause-effect criteria. The $\left(D_i^{\widetilde{Def}} + R_i^{\widetilde{Def}}\right)$ and $(D\left(D_i^{\widetilde{Def}} - R_i^{\widetilde{Def}}\right)$ values, which determine the relationship direction and degree of impact of the criteria, can be interpreted in four different ways. Table 2 explains the interpretation of the criteria according to these values[29,30].

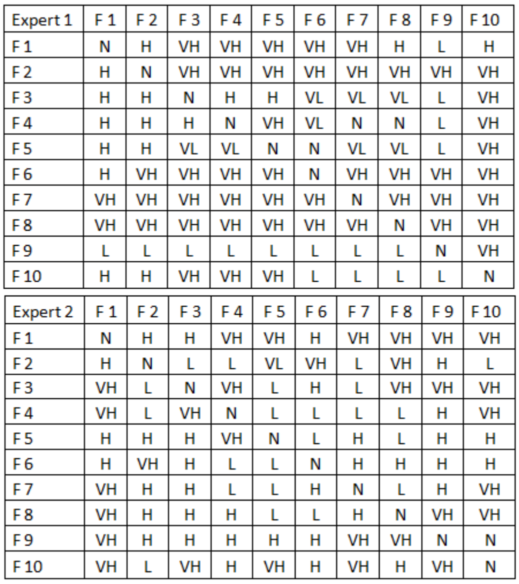
Table 2: Interpretation of Priority (D+R) and $\left(D_i^{\widetilde{Def}} - R_i^{\widetilde{Def}}\right)$ relationship values of criteria

(D-R) value	(D+R) value	Characteristic of the criterion
Positive	High	There are causal criteria and these criteria have a high effect on other problem criteria. Since the criteria in the causal group have the ability to affect.
Positive	Low	It is classified as causal criteria because it has a positive D-R value in these criteria.
Negative	High	Criteria's have a large influence on these criteria. With the development of causal criteria, it is possible for these criteria to develop indirectly.
Negative	Low	Criteria's are not very much influenced by causal criteria. Their influence on the outcome of the problem is weak.

5. Implementation

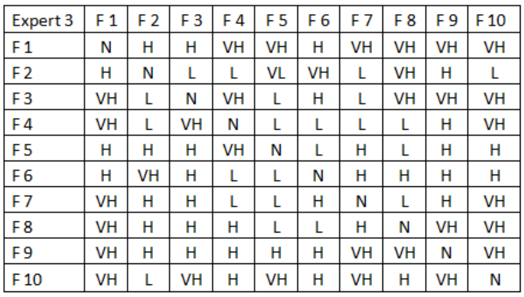
In the first part of the application, the criteria affecting the federated transfer learning structure were determined. The criteria evaluated in the study are "Security and Authentication" (F1), "Privacy-Security" (F2), "Reliability" (F3), "Anonymity"(F4), "Limited Disclosure" (F5), "Communication" (F6) are "Integrity" (F7), "Interoperability" (F8) , "Availability" (F9) and "Authorization" (F10). In the first stage, the expert group asked to evaluate the cause-effect relationship between the relevant criteria and the fuzzy DEMATEL method used for this. For the importance of these criteria in affecting the security structure, 4 different expert opinions on the subject were consulted. Pairwise comparisons made by experts in terms of the effect of each dimension on another dimension (Table 3). Because of the preliminary study, ten critical criteria that could be effective were determined.

Table 3: The linguistic evaluation of an expert for the dimensions

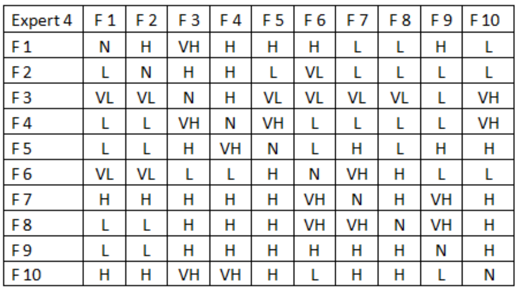


Expert 1	F 1	F 2	F 3	F 4	F 5	F 6	F 7	F 8	F 9	F 10
F 1	N	H	VH	VH	VH	VH	VH	H	L	H
F 2	H	N	VH	VH	VH	VH	VH	VH	VH	VH
F 3	H	H	N	H	H	VL	VL	VL	L	VH
F 4	H	H	H	N	VH	VL	N	N	L	VH
F 5	H	H	VL	VL	N	N	VL	VL	L	VH
F 6	H	VH	VH	VH	VH	N	VH	VH	VH	VH
F 7	VH	VH	VH	VH	VH	VH	N	VH	VH	VH
F 8	VH	VH	VH	VH	VH	VH	VH	N	VH	VH
F 9	L	L	L	L	L	L	L	L	N	VH
F 10	H	H	VH	VH	VH	L	L	L	L	N

Expert 2	F 1	F 2	F 3	F 4	F 5	F 6	F 7	F 8	F 9	F 10
F 1	N	H	H	VH	VH	H	VH	VH	VH	VH
F 2	H	N	L	L	VL	VH	L	VH	H	L
F 3	VH	L	N	VH	L	H	L	VH	VH	VH
F 4	VH	L	VH	N	L	L	L	L	H	VH
F 5	H	H	H	VH	N	L	H	L	H	H
F 6	H	VH	H	L	L	N	H	H	H	H
F 7	VH	H	H	L	L	H	N	L	H	VH
F 8	VH	H	H	H	L	L	H	N	VH	VH
F 9	VH	H	H	H	H	H	VH	VH	N	N
F 10	VH	L	VH	H	VH	H	VH	H	VH	N



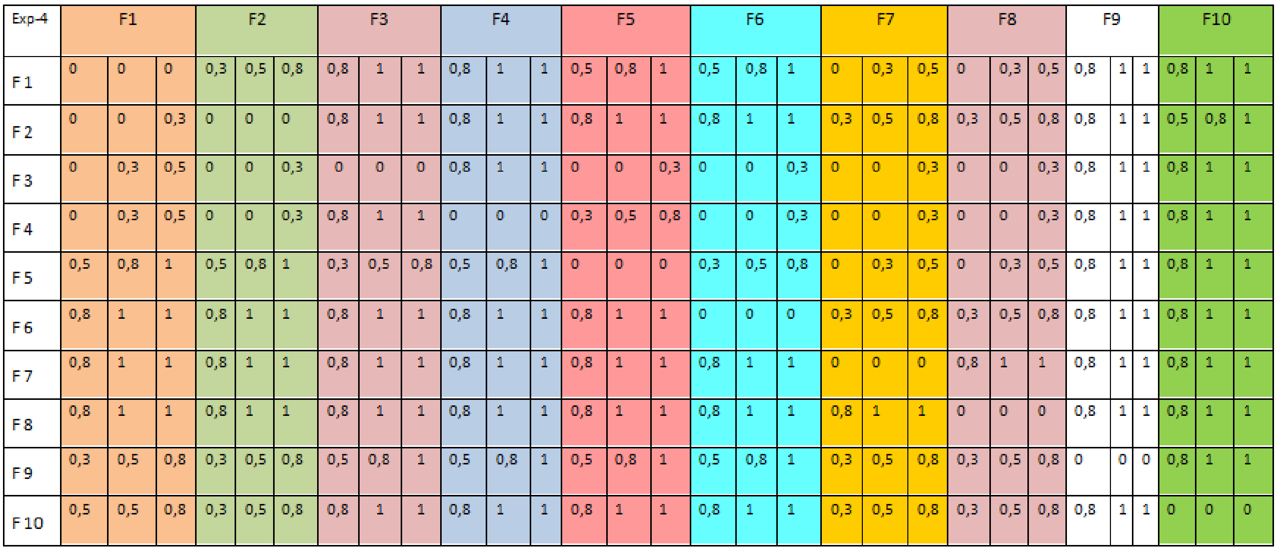
Expert 3	F 1	F 2	F 3	F 4	F 5	F 6	F 7	F 8	F 9	F 10
F 1	N	H	H	VH	VH	H	VH	VH	VH	VH
F 2	H	N	L	L	VL	VH	L	VH	H	L
F 3	VH	L	N	VH	L	H	L	VH	VH	VH
F 4	VH	L	VH	N	L	L	L	L	H	VH
F 5	H	H	H	VH	N	L	H	L	H	H
F 6	H	VH	H	L	L	N	H	H	H	H
F 7	VH	H	H	L	L	H	N	L	H	VH
F 8	VH	H	H	H	L	L	H	N	VH	VH
F 9	VH	H	H	H	H	H	VH	VH	N	VH
F 10	VH	L	VH	H	VH	H	VH	H	VH	N



Expert 4	F 1	F 2	F 3	F 4	F 5	F 6	F 7	F 8	F 9	F 10
F 1	N	H	VH	H	H	H	L	L	H	L
F 2	L	N	H	H	L	VL	L	L	L	L
F 3	VL	VL	N	H	VL	VL	VL	VL	L	VH
F 4	L	L	VH	N	VH	L	L	L	L	VH
F 5	L	L	H	VH	N	L	H	L	H	H
F 6	VL	VL	L	L	H	N	VH	H	L	L
F 7	H	H	H	H	H	VH	N	H	VH	H
F 8	L	L	H	H	H	VH	VH	N	VH	H
F 9	L	L	H	H	H	H	H	H	N	H
F 10	H	H	VH	VH	H	L	H	H	L	N

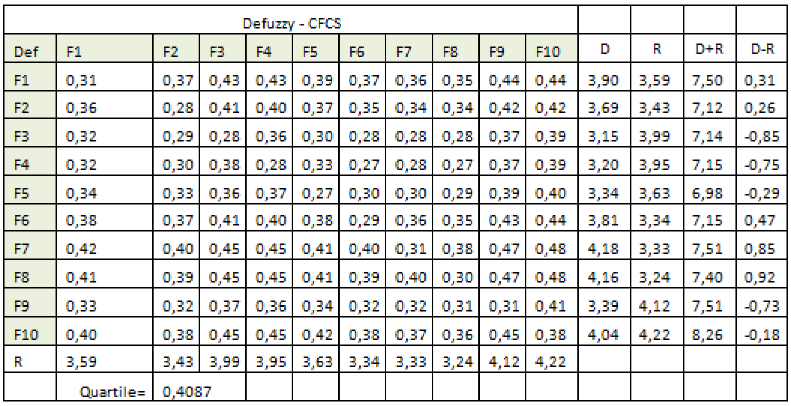
The mean value and R-values of the evaluation results of each decision maker and the total relational fuzzy matrix data given in Table 4. Each element in the matrix represents the sum. The strength of the random effect of premise i on premise j. Using Equation (10) neighbourhood matrix created and showed in Table 4. The row sums showed in Table 5 using Equations (7) and (9) as a categorized "clear cause" premise or "net effect" premise. The "clear cause" antecedents suggest the ordinal values of these factors. Using the information from Table 5, the (D + R) and (D – R) maps were obtained and shown in Figure 4.

Table 4: Total-relation fuzzy matrix



Exp-4	F1			F2			F3			F4			F5			F6			F7			F8			F9			F10		
F 1	0	0	0	0,3	0,5	0,8	0,8	1	1	0,8	1	1	0,5	0,8	1	0,5	0,8	1	0	0,3	0,5	0	0,3	0,5	0,8	1	1	0,8	1	1
F 2	0	0	0,3	0	0	0	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0,3	0,5	0,8	0,3	0,5	0,8	0,8	1	1	0,5	0,8	1
F 3	0	0,3	0,5	0	0	0,3	0	0	0	0,8	1	1	0	0	0,3	0	0	0,3	0	0	0,3	0	0	0,3	0,8	1	1	0,8	1	1
F 4	0	0,3	0,5	0	0	0,3	0,8	1	1	0	0	0	0,3	0,5	0,8	0	0	0,3	0	0	0,3	0	0	0,3	0,8	1	1	0,8	1	1
F 5	0,5	0,8	1	0,5	0,8	1	0,3	0,5	0,8	0,5	0,8	1	0	0	0	0,3	0,5	0,8	0	0,3	0,5	0	0,3	0,5	0,8	1	1	0,8	1	1
F 6	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0	0	0	0,3	0,5	0,8	0,3	0,5	0,8	0,8	1	1	0,8	1	1
F 7	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0	0	0	0,8	1	1	0,8	1	1	0,8	1	1
F 8	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0	0	0	0,8	1	1	0,8	1	1
F 9	0,3	0,5	0,8	0,3	0,5	0,8	0,5	0,8	1	0,5	0,8	1	0,5	0,8	1	0,5	0,8	1	0,3	0,5	0,8	0,3	0,5	0,8	0	0	0	0,8	1	1
F 10	0,5	0,5	0,8	0,3	0,5	0,8	0,8	1	1	0,8	1	1	0,8	1	1	0,8	1	1	0,3	0,5	0,8	0,3	0,5	0,8	0,8	1	1	0	0	0

Table 5: Defuzzified total-relation matrix and D+R, D-R values



Defuzzy - CFCS														
Def	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	D	R	D+R	D-R
F1	0,31	0,37	0,43	0,43	0,39	0,37	0,36	0,35	0,44	0,44	3,90	3,59	7,50	0,31
F2	0,36	0,28	0,41	0,40	0,37	0,35	0,34	0,34	0,42	0,42	3,69	3,43	7,12	0,26
F3	0,32	0,29	0,28	0,36	0,30	0,28	0,28	0,28	0,37	0,39	3,15	3,99	7,14	-0,85
F4	0,32	0,30	0,38	0,28	0,33	0,27	0,28	0,27	0,37	0,39	3,20	3,95	7,15	-0,75
F5	0,34	0,33	0,36	0,37	0,27	0,30	0,30	0,29	0,39	0,40	3,34	3,63	6,98	-0,29
F6	0,38	0,37	0,41	0,40	0,38	0,29	0,36	0,35	0,43	0,44	3,81	3,34	7,15	0,47
F7	0,42	0,40	0,45	0,45	0,41	0,40	0,31	0,38	0,47	0,48	4,18	3,33	7,51	0,85
F8	0,41	0,39	0,45	0,45	0,41	0,39	0,40	0,30	0,47	0,48	4,16	3,24	7,40	0,92
F9	0,33	0,32	0,37	0,36	0,34	0,32	0,32	0,31	0,31	0,41	3,39	4,12	7,51	-0,73
F10	0,40	0,38	0,45	0,45	0,42	0,38	0,37	0,36	0,45	0,38	4,04	4,22	8,26	-0,18
R	3,59	3,43	3,99	3,95	3,63	3,34	3,33	3,24	4,12	4,22				
	Quartile=	0,4087												

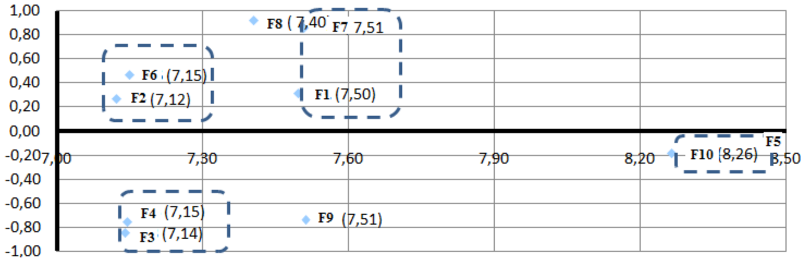


Figure 4: Influential diagram of the dimensions

6. Conclusion

Our aim determine the most effective criteria affecting security within the federated and transfer learning on network management structure. It thought that this study contribute to the literature since the integrated method and application proposed in the study have not been included in the literature before. Fuzzy approach has made it easier to evaluate the verbal expressions of the decision-making experts. Its effective and comprehensive evaluation allow the criteria to analyse effectively in practical. The importance of these criteria taken into account in the federated learning that takes place in the future security-based network management structure.

In this study, the federated learning style examined in order to train the distributed edge data sources with the collaborative training model. The criteria affecting the federated learning and transfer learning structure ranked according to their importance by using the fuzzy DEMATEL method. Because of this ranking, values with the best performance were F6 (Communication), F7 (Integrity) and F3 (Reliability). We can see that F6-F2 is similar, F7-F1 is very close to each other, F4-F3 has very close values, but F9-F10 and F5 have more distant values than other criteria groups and are different in this grouping structure.

References

[1] Rahatulain A. Onori M., A new methodology to analyze the functional and physical architecture of existing products for an assembly oriented product family, Peer-review under responsibility of the scientific committee of the 28th CIRP Design Conference 2018. 28th CIRP Design Conference, May 2018, Nantes, France

[2] Rahatulain A., Onori Viewpoints and views for the architecture description of cyber-physical manufacturing systems, Peer-review under responsibility of the scientific committee of the 28th CIRP Design Conference 2018. 28th CIRP Design Conference, May 2018, Nantes, France, CIRP 00 (2017) 000-0000

[3] Skowronski R., The open blockchain-aided multi agent symbiotic cyber-physical systems, Future Generation Computer Systems 94(2019) 430-443.

[4] Bolbot V., Theotokatos G., Bujorianu L.M., Boulougouris E., Vassalos D., Vulnerabilities and safety assurance

methods in Cyber-Physical Systems: A comprehensive review, Reliability Engineering and System Safety, 182 (2019) 179-193.

[5] Hoffmannn R., Napiorkowski J., Prorasowicki T., Stanik J., Risk based approach in scope of cybersecurity threads and requirements, 1st International Conference on Optimization-Driven Architectural Design (OPTARCH 2019), Procedia Manufacturing 44(2020) 655-662

[6] Marotta A., Martinelli F., Nanni S. Orlando A., Yautsiukhin A, Cyber-insurance survey, Computer Science Review, 24 (2017) 35-61

[7] Ruan K., Introducing cybernomics: A unifying economic framework for measuring cyber risk, Computers&Security (2017), 83, pp.77-89

[8] Su D., Liu J., Wang W., Wang X., Du X., Guizani M., Discovering communities of malapps on Androis-based mobile cyber-physcal systems, Ad Hoc Networks, 80 (2018) 104-118

[9] Akinrolabu O., Nurse J.R.C., Martin A., New S., Cyber risk assessment in cloud provider environments: Current models and future needs, Computers & Security 87(2019) 101600.

[10] Mukhopadhyay A., Chatterjee S., Saha D., Mahanti A., Sadhukhan S.K., Cyber-risk decisison models: To insure IT or not, Decision Support Systems, 56 (2013), 11-26.

[11] Cardin O., Classification of cyber-physical production systems applications: Proposition of an analysis framework, Computers in Industry, 104(2019) 11-21

[12] Barrere M., Hankin C., Nicolaou N., Eliades D.G., Parisini T., Measuring cybephysical security in industrial control via minimum-effort attack strategies, Journal of Information Security and Applications, 52(2020), 102471

[13] Yaacoub J.P.A., Salman O., Noura H.N., Kaaniche N., Chehab A., Malli M., Cyber-physical systems security: Limitations, issues and future trends, Microprocessors and Microsystems, (2020), 77, 103201

[14] Bendiab G., Shiaeles S., Boucherkha S., FCMDT: A novel fuzzy cognitive mapsa dynamic trust model for cloud federated identity management, computer & security 86 (2019) 270-290.

[15] Tchoffa D., Figay N., Ghodous P., Panetto H., El Mhamed A., Alignment of the product lifecycle management federated framework with Internet of things and virtual manufacturing, Computers in Industry 130 (2021) 103466

[16] Polap D., Srivastava G., Yu K., Agent architecture of an intelligent medical system based on federated learning and blockchain technology, Journal of Information Security and Applications 58 (2021) 102748

[17] Xia Q., Ye W., Tao Z., Wu J., Li Q., A survey of federated learning for edge computing: Research problems and solutions, High-Confidence Computing 1 (2021) 100008

[18] Ali M., Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges, Computers&Security 108(2021) 102355

[19] Bianco-Justicia A., Domingo-Ferrer J., Martinez S., Snchez D., Flanagan A., Tan K.E., A., Achieving security and privacy in federated learning systems: Survey, research challenges and future directions, Engineering Applications of Artificial Intelligence Volume 106, November 2021, 104468

[20] Mothukuri V., Parizi R.M., Pouriyeh S., Huang Y., Dehghantanha A., Srivastava G., A survey on security and privacy of federated learning, Future Generation Computer Systems, Volume 115, February 2021, Pages 619-640.

[21] Chen M., Shlezinger N., Poor H.V., Eldar Y.C., Cui S., Communication-efficient federated learning, PNAS April 27, 2021 118 (17) e2024789118; https://doi.org/10.1073/pnas.2024789118

[22] Chen Y., Luo F., Li F., Xiang T., Liu Z., Li J.,A trsining-integrity privacy-preserving federated learning scheme with trusted execution environment, Information Sciences, Vol. 522, June 2020, pp. 69-79

[23] Gabus A., Fontela E. (1972). World Problems. An Invitation to Further Thought Within The Framework of DEMATEL. Battelle Geneva Research Centre, Geneva.

[24] Lin Chijen, Wu Weiwen (2004). A fuzzy extension of the DEMATEL method for group decision making. European Journal of Operational Research, 156, 445-455.

[25] Lin Chijen, Wu Weiwen (2008). A causal analytical method for group decision making under fuzzy environment. Expert Systems with Applications, 34, 205-213.

[26] Muhammad M.N., Cavus N., Fuzzy DEMATEL method for identifying LMS evaluation criteria, Procedia Computer Science, Volume 120, 2017, pp. 742-749

[27] Stief P., Dantan J.Y., Etienne A., Siadat A., A new methodology to analyze the functional and physical architecture of existing products for an assembly oriented product family identification, Peer-review under responsibility of the scientific committee of the 51st CIRP Conference on Manufacturing Systems. 10.1016/j.procir.2018.03.116, 51st CIRP Conference on Manufacturing Systems

[28] Uygun Ö., Turgay S. Healthcare Management Evaluatıon Wıth Fuzzy Dematel And Fuzzy Anp Approach, Proceedings of 8th International Symposium on Intelligent and Manufacturing Systems (IMS 2012) , Sakarya University Department of Industrial Engineering, Adrasan, Antalya, Turkey, September 27-28, 2012: 567-582

[29] Yager R.R., Filev D.P. (1994). Essentials of fuzzy modeling and control. New York: John Wiley & Sons.

[30] Opricovic S., Tzeng G.H. (2003). Defuzzification within a multicriteria decision nıdel, International Journal of Uncertainty. Fuzziness and Knowledge-Based Systems, 11(5), 635-652.