Securing Information Management in Collaborative Environments Using Machine Learning

Ahmed Hatip [1], Karla Zayood [2], Rabah Scharif [3]

[1] Gaziantep university, Turkey

[2] Online Islamic University, Department Of Science and Information Technology, Doha, Qatar

[3] Applied Engineering Department, Institute of Applied Technology, UAE

Emails: Kollnaar5@gmail.com; zayyyoood134@gmail.com ; rabah.scharif@aths.ac.ae

Abstract

Recently, there has been a significant increase in the use of collaborative environments for managing and sharing information. However, these environments often present significant security risks due to the potential for unauthorized access, data leakage, and other security breaches. To address these risks, machine learning (ML) techniques have been increasingly used to secure information management in collaborative environments. We propose a novel ML approach to be applied to detect and prevent security threats in collaborative environments. Our approach integrates temporal convolution to detect and prevent security threats by analyzing spatial-temporal patterns in data from various sources, such as network traffic, system logs, and user behavior. Furthermore, we present a case study demonstrating the effectiveness of our model in securing collaborative information management. The case study involves the development of our system for detecting insider threats in a collaborative environment. Extensive experimentation on this case study demonstrates the efficiency and effectiveness of the proposed system for securing information management and promoting further developments.

Keywords: Security Risks; Information Management; Collaborative Environments; Network Traffic; Machine Learning

1. Introduction

Information management in collaborative environments refers to the processes, systems, and tools used to manage and share information among a group of people working together towards a common goal. Collaborative environments can be virtual, such as online platforms or cloud-based software, or physical, such as co-working spaces or team rooms. In collaborative environments, effective information management is critical for achieving success and improving productivity [1]. However, managing, and securing information in these environments can be challenging due to the large volumes of data generated, the need for collaboration across different teams and organizations, and the potential for security breaches. As a result, organizations are increasingly turning to innovative solutions such as machine learning to improve the security and efficiency of information management in collaborative environments [2].

Collaborative environments often present significant security challenges due to the potential for unauthorized access, data leakage, and other security breaches. One of the major security challenges is the risk of insider threats, where individuals who have authorized access to the information in the collaborative environment deliberately or unintentionally misuse or disclose sensitive data. Another challenge is the difficulty of ensuring that all team

Doi : https://doi.org/10.54216/JCIM.110203
Received: November 27, 2022 Revised: January 18, 2023 Accepted: March 09, 2023

members have access to the same level of security measures, which can lead to gaps in security and vulnerabilities [4]. In addition, collaborative environments can be vulnerable to external threats such as hacking, phishing attacks, and malware, which can compromise sensitive information and disrupt team operations. Finally, the need to manage multiple versions of documents and ensure that all team members are working from the most up-to-date information can also pose a security risk, as outdated or incorrect information can lead to errors and miscommunication [5]. Addressing these security challenges requires a comprehensive approach that includes both technical and organizational measures, such as access control, encryption, monitoring, training, and policies and procedures [6].

In line with the above research gaps, this study presents the ML-based system for addressing security challenges in collaborative environments is designed to detect and prevent insider threats. Our system applies a temporal convolutional model to analyze user behavior and identify anomalies that may indicate malicious activity. The system is also capable of monitoring and analyzing network traffic and user access logs to detect and prevent unauthorized access and data leakage. Our system is continuously updated with the latest threat intelligence to ensure that it can effectively detect and prevent emerging threats.

The remaining paper is structured as follows. Related works are reviewed in section 2. Section 3 discusses the methodology of the proposed solution. The experiments and related discussions are given in section 4. The conclusion of our work is presented in section 5.

2. Related Work

With the continuous advance in collaborative information management, research literature has encountered an increased interest in addressing the security problems of such collaborative systems. The paper [5] presented a framework for secure and collaborative sharing of healthcare data across multiple cloud platforms. They attempted to address the challenges of data security and privacy in cloud-based environments. Their proposed framework employs a multi-layered security approach, which includes encryption, access control, and data classification mechanisms to ensure that healthcare data is securely shared between different healthcare providers. It also integrated collaboration features, such as workflow management and user feedback, to enable effective communication and collaboration among healthcare providers. In [7], the authors provided an in-depth analysis of the security challenges and solutions for cooperative intelligent transport systems (C-ITS). They highlighted the potential security risks associated with C-ITS, such as privacy violations, data tampering, and denial-of-service attacks. They also discussed the various standards and protocols that have been developed to enhance the security of C-ITS, such as secure message dissemination and certificate management. In [12] presented a comprehensive survey of recent advances in vehicular network security, trust, and privacy. They studied the significant security challenges faced by vehicular networks, such as location privacy, data confidentiality, and malicious attacks. In [13], the authors provided a comprehensive survey of emerging security mechanisms for IoT systems based on Software-Defined Networking (SDN) and Network Function Virtualization (NFV). They discussed the various security mechanisms that have been proposed to address these challenges, including traffic classification, access control, and intrusion detection systems. They presented a critical analysis of the existing literature on SDN and NFV security mechanisms for IoT systems, highlighting the gaps in current research and proposing future research directions. In [17], the authors proposed an approach for detecting anomalous insiders in collaborative information systems. They used statistical anomaly detection techniques to identify suspicious behavior patterns and then

Doi : https://doi.org/10.54216/JCIM.110203
Received: November 27, 2022 Revised: January 18, 2023 Accepted: March 09, 2023

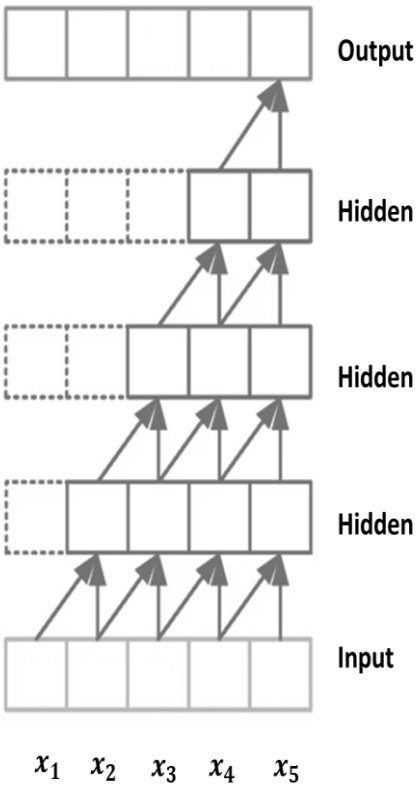

Figure 1: Architecture of the causal convolution

leverage expert knowledge to validate the anomalies and determine whether they are indicative of malicious intent. Their proposed approach also considered the collaboration patterns of insiders, such as their social relationships and communication patterns, to improve the accuracy of the detection. The authors of [18] proposed an ML-based approach for enhancing the security of C-ITS using digital twins, in which the security challenges faced by C-ITS, such as data privacy, message integrity, and availability. They developed a framework that leverages digital twins to generate simulated data that can be used to train deep learning models for intrusion detection and attack attribution. The authors of [19] demonstrated how GAN-based collaborative models can leak sensitive information about the training data and the models themselves. They proposed an attack called the "model inversion attack," which could infer sensitive information about the training data by observing the output of the collaborative model. They also presented a defense mechanism based on differential privacy to mitigate the privacy risks associated with GAN-based collaborative ML.

3. Proposed Methodology

In this section, we present the proposed methodology for addressing the security challenges in collaborative environments using machine learning. The methodology is designed to detect and prevent security threats by analyzing data from various sources, such as network traffic, system logs, and user behavior. In the following subsections, we discuss each step in-detail and explain how our proposed methodology can effectively address the previously mentioned security challenges.

Temporal convolutional network (TCN) is applied as a popular learning model that is well-suited for analyzing sequential data, such as time series or signals. In our proposed methodology, we use TCNs to extract features from the preprocessed data, which are then fed into a supervised learning model for training [20-21]. The design of TCN is based on causal convolutions, in which the input at time t can only rely on the inputs that are not after time t, as depicted in Fig. 1. Nevertheless, the inadequate receptive of the causal convolution has a constrained capacity to acquire global information. Thus, to tackle this issue, we apply the dilation strategy based on obtaining larger

Doi : https://doi.org/10.54216/JCIM.110203
Received: November 27, 2022 Revised: January 18, 2023 Accepted: March 09, 2023

performance. In mathematical term, provided 1-D dimension input x, the feature map generated by dilation convolution at step t is defined as:

$$s_t = (x *_d f)(t) = \sum_{i=0}^{k-1} f(i) \cdot x_{t-d} \cdot i \quad (1)$$

With s denoting the output map and f is a 1-D filter with size $k \times 1$. The symbol $*$ designate convolution operation, d denote the dilation factor. The dilation factor d and the filter size k in the TCN can flexibly adjust the size of the receptive filed to obtain features of the input sequence with different time scales. Fig. 1 shows an instance of dilation strategy, in which the kernel size is 2 and the space sampling point is $d = 1, 2$.

In our model, we use two of the above layers to build a residual block, where each of them is tailed with nonlinearity. The design of residual block generates the output as combination of the output of the above layers, and input of the block itself. This can be expressed as follows:

$$LeakyReLU(x) = max(0, x) + negative\_slope * min(0, x) \quad (2)$$

$$h_{1k} = LeakyReLU(W_k * X + b_k), \quad (3)$$

$$h_{2k} = LeakyReLU(W_k * h_{1k} + b_k), \quad (4)$$

$$o = (\mathbf{x} + \mathcal{F}(\boldsymbol{h}_{2k})). \quad (5)$$

The TCN architecture consists of a series of the above residual blocks. The convolutional layers are designed to learn temporal patterns in the input data, with the depth of the network determining the size of the temporal receptive field. By increasing the depth of the network, we can capture longer-term temporal dependencies in the data. The output of convolutional layers is later passed to linear layer with SoftMax activation, where the final classification decision is computed:

$$p(y^{(i)} = j | x^{(i)}; \theta) = \frac{exp(\theta_j^T x^{(i)})}{\sum_{l=1}^{k} exp(\theta_l^T x^{(i)})} \quad (6)$$

$$y = argmax_j \, p\left(y^{(i)} = j \middle| x^{(i)}; \theta\right), \quad (7)$$

During the training process, the cross-entropy objectives are used to calculate the learning loss.

$$C = \frac{-1}{n} \sum_{c=1N}^{N} ([y_c * log\,(a_c) + (1 - y_c) log\,(1 - a_c)]) \quad (8)$$

In the above formula, the term C denote the loss value that need to be minimized. The y_c denote the target value, c designate the attack label. N is integer referring to the total number of classes. The training process has a learning rate of 0.001.

4. Experimental Discussions.

Doi : https://doi.org/10.54216/JCIM.110203
Received: November 27, 2022 Revised: January 18, 2023 Accepted: March 09, 2023

The UNSW dataset is a valuable case study for our proposed work on securing information management in collaborative environments using machine learning. The dataset consists of real-world network traffic data collected from an Australian university campus network. The dataset contains a wide range of network activities, including normal user behaviors and various types of attacks, such as port scans, buffer overflow attacks, and denial-of-service attacks. The data contains a total of 2,540,044 samples, each consisting of 49 features. Our proposed framework is trained on the UNSW dataset to detect and prevent insider threats and other malicious activities. It also can be used to evaluate the effectiveness of the framework in detecting and preventing insider threats in collaborative environments. Moreover, the UNSW dataset is considered a suitable choice as it can be used to simulate collaborative environments, where multiple users have access to sensitive information and need to collaborate to complete their tasks. This simulation can provide insights into the effectiveness of the proposed framework in detecting and preventing insider threats in real-world collaborative environments. The above case study is sampled to build a non-intersecting training set and testing set containing a total of 175,341 records and 82,332 records, respectively.

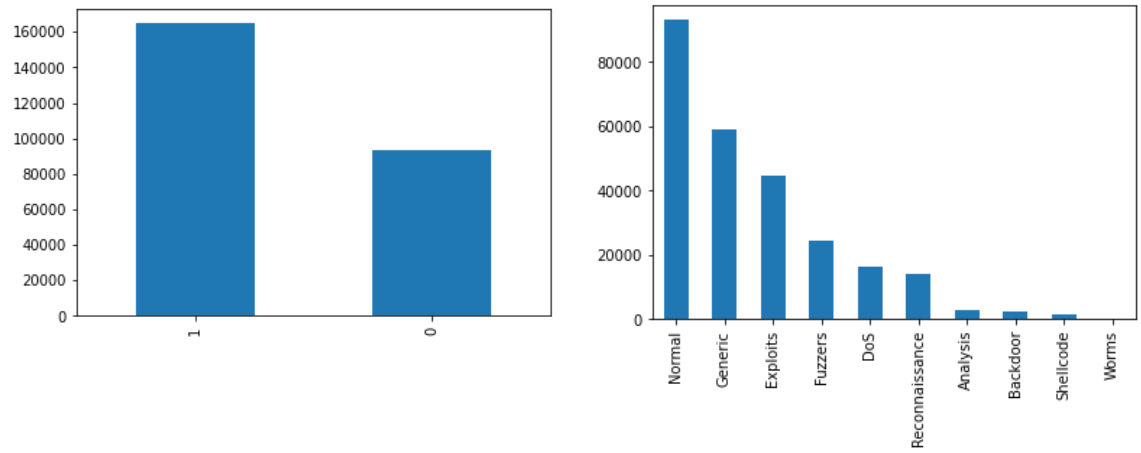

Figure 2: Frequency analysis for the different classes of samples in our case study.

Exploratory analytics is applied on our proposed work for securing information management in collaborative environments. This involves analyzing and visualizing the data to identify patterns, anomalies, and relationships that can help in effective training of our model. For our work, class frequency analysis is conducted in Fig. 2 to visualize the number of samples per each class. In binary case scenario (left part of Fig.2), we can observe that the number normal samples (1) are much higher than the number of malicious samples. In the right part of Fig.2, the class distribution is given at attack level, and it could be noted that our data is encountering a high-class imbalance, which may affect the accuracy of our algorithm.

Doi : https://doi.org/10.54216/JCIM.110203
Received: November 27, 2022 Revised: January 18, 2023 Accepted: March 09, 2023

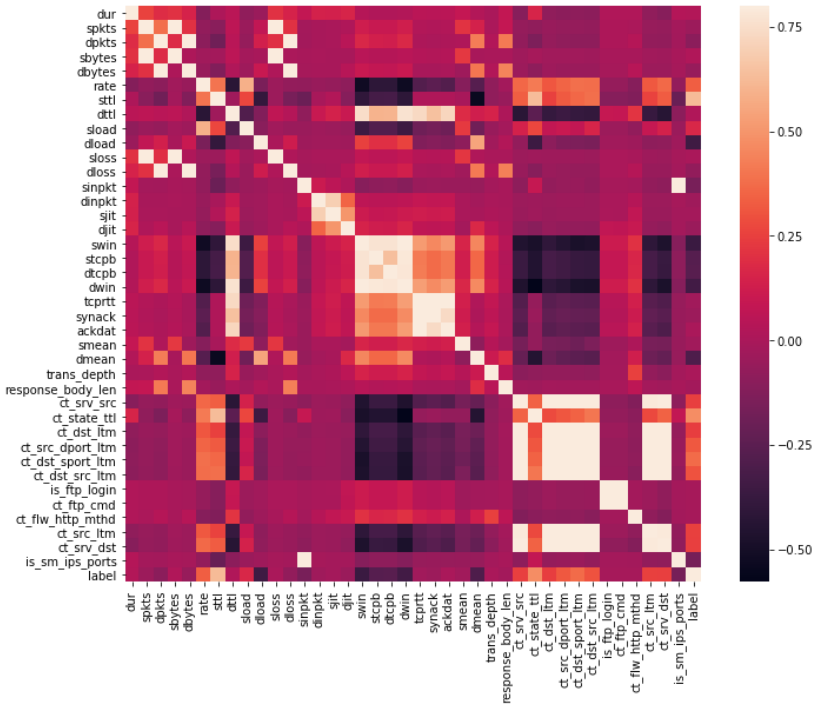

Figure 3: Visualization of Pearson correlation on our case study for securing collaborative environment.

In addition, we perform Pearson correlation analysis to explore the most relevant features in the data that can be used as inputs to our case study, as shown in Fig. 3. It could be noted that the highest correlation occurs between the following sets of features (spkts, sbytes, sloss), and (dpkts, dbytes, dloss). This can be further validated in Fig. 4, where the pair plots are displayed between the above-mentioned pair plots. Feature importance analysis is applied based on univariate statistical test, to identify the most predictive features for a target feature. In particular, the chi-squared test is applied to test the independence of two categorical variables. We apply a chi-squared test to examine the relationship between different attacking features and the label in our case study. If the chi-squared test shows a statistically significant relationship, we can conclude that the user attribute is predictive of the target feature. Fig. 5 shows the feature importance based on chi-squared test.

A comparative analysis of our proposed approach against state-of-the-art ML algorithms can help evaluate its effectiveness in addressing security challenges in collaborative environments. We can compare the performance of our approach with other existing ML algorithms such as Decision Trees, Gradient Boosting

Doi : https://doi.org/10.54216/JCIM.110203
Received: November 27, 2022 Revised: January 18, 2023 Accepted: March 09, 2023

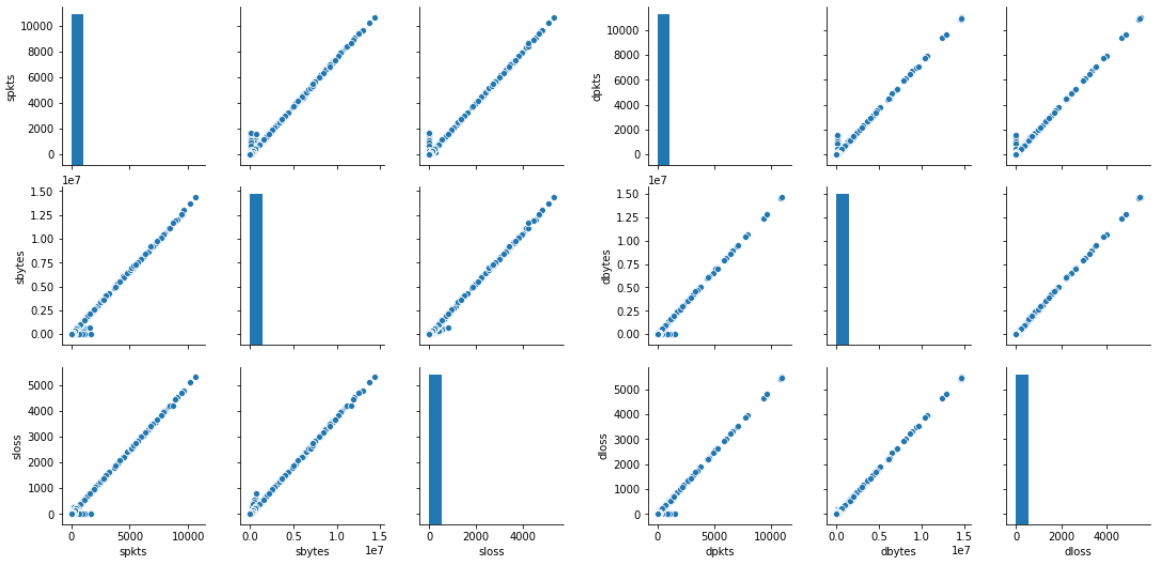

Figure 4: visualization of pair plots between highly related variables in our case study.

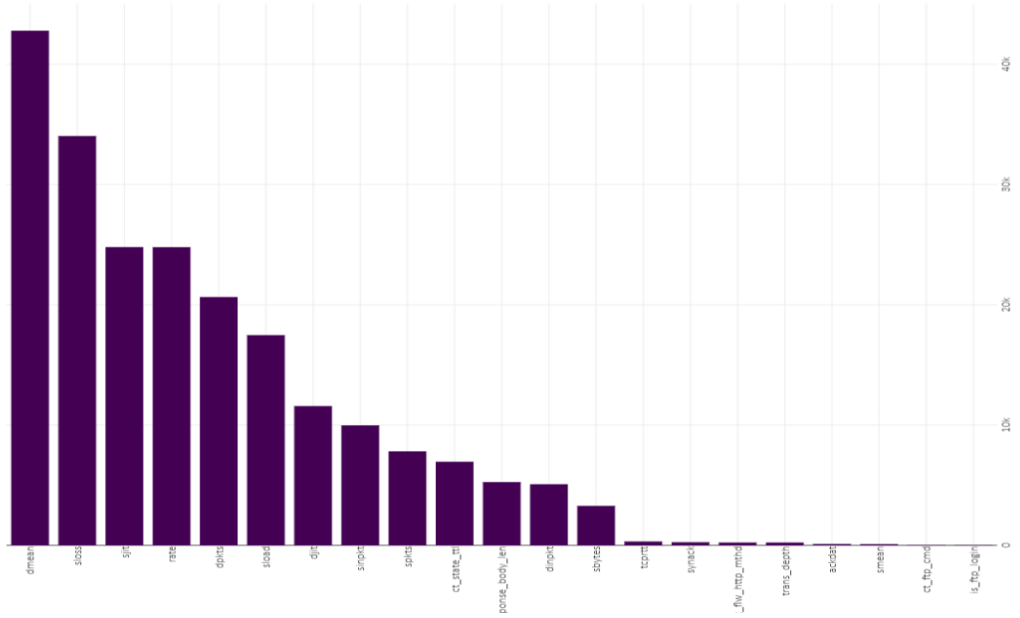

Figure 5: Feature importance in our case study

Classifier, Naïve Bayes, and Support Vector Machines. We can evaluate the performance of each algorithm on various metrics such as accuracy, precision, recall, and F1 score. These metrics can provide an insight into how well the algorithm performs in detecting malicious activities and predicting security threats in collaborative environments. Table 1 shows the numerical results of comparative analysis. The results demonstrate that logistic regression has the lowest detection performance. Deep neural networks (like MLP, GRU, LSTM) are achieving a good detection performance, however they consume more time than traditional ML methods. More importantly, the proposed approach shows great competitive capability over the competing methods and achieves lower execution time than the competing deep networks.

Doi : https://doi.org/10.54216/JCIM.110203
Received: November 27, 2022 Revised: January 18, 2023 Accepted: March 09, 2023

Table 1: numerical results of comparing the performance of the proposed model against competing ones.

Methods	Accuracy	Recall	Precision	F1-Score	Execution Time
Logistic	92.99	92.96	92.86	92.93	1.81
kNN	95.05	95.31	95.30	95.26	20.39
Decision Tree	96.54	96.46	96.41	96.56	1.80
Extra Trees	97.83	97.84	97.55	97.61	5.16
MLP	96.24	96.20	96.37	96.11	43.36
GRU	96.40	96.57	96.38	96.58	86.72
LSTM	96.74	96.71	96.65	96.51	89.05
Ours	98.55	98.41	97.57	98.07	33.43

5. Conclusion

This research proposes an ML approach for securing information management in collaborative environments through detecting the security risks and threats that these environments face. Our proposed solution leverages an intelligent temporal convolution approach to detect and prevent unauthorized access to sensitive information and detect anomalous behaviors. The framework also considers the collaboration patterns of insiders to improve the accuracy of the detection. Our proposed approach provides a valuable tool for organizations to protect against insider threats and ensure the security of their collaborative environments. Future work may involve testing the proposed framework on real-world collaborative environments and optimizing the algorithms to achieve better performance.

References

[1] Del Giudice, M. and Della Peruta, M.R., 2016. The impact of IT-based knowledge management systems on internal venturing and innovation: a structural equation modeling approach to corporate performance. *Journal of Knowledge Management*.

[2] Santoro, G., Vrontis, D., Thrassou, A. and Dezi, L., 2018. The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity. *Technological forecasting and social change*, *136*, pp.347-354.

[3] Salmon, P.M., Stanton, N.A. and Jenkins, D.P., 2017. Distributed situation awareness: Theory, measurement and application to teamwork.

[4] Estrada, I., Faems, D. and de Faria, P., 2016. Coopetition and product innovation performance: The role of internal knowledge sharing mechanisms and formal knowledge protection mechanisms. Industrial Marketing Management, 53, pp.56-65.

[5] Yazdani, M., Chatterjee, P., Zavadskas, E.K., & Hashemkhani Zolfani, S. (2019). A novel integrated decision-making approach for the evaluation and selection of sustainable construction materials with unknown weights under neutrosophic environment. Sustainability, 11(5), 1317.

[6] Zafar, R., Mahmood, A., Razzaq, S., Ali, W., Naeem, U. and Shehzad, K., 2018. Prosumer based energy management and sharing in smart grid. *Renewable and Sustainable Energy Reviews*, *82*, pp.1675-1684.

[7] Ben Hamida, E., Noura, H. and Znaidi, W., 2015. Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics*, *4*(3), pp.380-423.

[8] Soltani, Z. and Navimipour, N.J., 2016. Customer relationship management mechanisms: A systematic review of the state-of-the-art literature and recommendations for future research. *Computers in Human Behavior*, *61*, pp.667-688.

[9] Meng, W., Tischhauser, E.W., Wang, Q., Wang, Y. and Han, J., 2018. When intrusion detection meets blockchain technology: a review. *Ieee Access*, *6*, pp.10179-10188.

Doi : https://doi.org/10.54216/JCIM.110203
Received: November 27, 2022 Revised: January 18, 2023 Accepted: March 09, 2023

[10] Guerrero-Ibáñez, J., Zeadally, S. and Contreras-Castillo, J., 2018. Sensor technologies for intelligent transportation systems. *Sensors*, *18*(4), p.1212.

[11] Lim, M.K., Tseng, M.L., Tan, K.H. and Bui, T.D., 2017. Knowledge management in sustainable supply chain management: Improving performance through an interpretive structural modelling approach. *Journal of cleaner production*, *162*, pp.806-816.

[12] Lu, Z., Qu, G. and Liu, Z., 2018. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Transactions on Intelligent Transportation Systems*, *20*(2), pp.760-776.

[13] Farris, I., Taleb, T., Khettab, Y. and Song, J., 2018. A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Communications Surveys & Tutorials*, *21*(1), pp.812-837.

[14] Hislop, D., Bosua, R. and Helms, R., 2018. *Knowledge management in organizations: A critical introduction*. Oxford university press.

[15] Vasilomanolakis, E., Karuppayah, S., Mühlhäuser, M. and Fischer, M., 2015. Taxonomy and survey of collaborative intrusion detection. *ACM Computing Surveys (CSUR)*, *47*(4), pp.1-33.

[16] Zhang, P., Zhou, M. and Fortino, G., 2018. Security and trust issues in fog computing: A survey. *Future Generation Computer Systems*, *88*, pp.16-27.

[17] Nayeri, M.D., Torabi, S.A., & Tavakkoli-Moghaddam, R. (2021). A goal programming-based fuzzy best–worst method for the viable supply chain of perishable products. Soft Computing, 26, 1235–1255.

[18] Lv, Z., Li, Y., Feng, H. and Lv, H., 2021. Deep learning for security in digital twins of cooperative intelligent transportation systems. IEEE transactions on intelligent transportation systems, 23(9), pp.16666-16675.

[19] Hitaj, B., Ateniese, G. and Perez-Cruz, F., 2017, October. Deep models under the GAN: information leakage from collaborative deep learning. In Proceedings of the 2017 ACM SIGSAC conference on computer and communications security (pp. 603-618).

[20] Sarkar, A., & Srivastava, P. (2021). Recent development and applications of neutrosophic fuzzy sets: a review. Journal of Ambient Intelligence and Humanized Computing, 12, 865–888.

[21] Zhang, Q., Zhong, H., Shi, W. and Liu, L., 2021. A trusted and collaborative framework for deep learning in IoT. *Computer Networks*, *193*, p.108055.

Doi : https://doi.org/10.54216/JCIM.110203
Received: November 27, 2022 Revised: January 18, 2023 Accepted: March 09, 2023