Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 4, pp. 2581–2588, DOI 10.12694/scpe.v25i4.2862

INTELLIGENT ADVANCED ATTACK DETECTION TECHNOLOGY BASED ON MULTI-MODAL DATA FUSION

FEILU HANG[*], LINJIANG XIE[†], ZHENHONG ZHANG[‡], AND JIAN HU [§]

Abstract. This paper proposes an adaptive Wedman intrusion detection algorithm (AID-DFS) for data fusion. Firstly, feature extraction of abnormal text detection is carried out using a BI-gated loop (Bi-GRU). Multi-branch convolutional recurrent neural network (CNN-RNN) extracts hierarchical features from abnormal images. The multi-mode dynamic fusion uses the intermodal and intramodal attention mechanisms. In this way, a joint representation of multiple modes is obtained. The visual perception mechanism is used to realize multichannel integration and strengthen the function of original information in multichannel. The experimental results show that the proposed method has 99.6% accuracy and 94.9% accuracy. Compared with other algorithms, the proposed method can improve the performance of the intrusion system by about 10.2%.

Key words: Wireless sensor network; Information fusion; Intrusion detection; Convolutional neural network; Anomaly information extraction

1. Introduction. In recent years, wireless sensor network (WSN) has been applied increasingly and has become an essential technology in smart grid, rail transit, manufacturing and other major engineering fields. Detecting abnormal services, such as network attacks, is a prerequisite for long-term continuous critical infrastructure monitoring. The popular methods currently include data mining, game theory, traffic prediction, and computational intelligence technology. Literature [1] uses a negative selection algorithm in immunology to monitor the behavior of wireless sensor networks. Literature [2] uses the K-means method to learn and classify massive network information collected in wireless sensor networks to detect various types of network attacks. In reference [3], a game theory intrusion detection algorithm is designed to solve the abnormal phenomena in wireless sensor networks. A cluster-structured hybrid intrusion detection method (CHH-IDS) is studied in reference [4]. This method can detect both existing and non-existing attacks at the same time. Literature [5] combines kernel self-grouping mapping technology and PSO algorithm (KSOM-PSO). It can effectively improve the recognition accuracy of wireless sensor networks. Literature [6] constructs a WSN network intrusion detection model based on multiple stages. This algorithm updates the posterior information of subsequent nodes based on the Bayes criterion, thus significantly improving the detection accuracy of clustered WSNs. Given the problems of high and low false alarm rates in network security, most of the existing intrusion detection methods are based on data mining. Although these methods can ensure the regular operation of the network, they are still vulnerable to various types of network intrusion attacks. Therefore, how to use the abnormal behavior in the network to improve the security of sensor networks is the core goal of wireless sensor networks. Literature [7] proposes a multi-protocol hierarchical IDS (T-MPNID) algorithm based on the fusion of trust and noise detection. An intrusion detection model based on a neural network is proposed, aiming at the abnormal behavior in wireless sensor networks. Intrusion detection is a security protection technology with positive significance. It distinguishes common from intrusion in a binary way. The core of the attack is the information fusion processing of each subsystem.

[*]Information security operation and maintenance center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, 650106, China (Corresponding author, hangfeilu2021@163.com)
[†]Information security operation and maintenance center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, 650106, China
[‡]Network Security Management Center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, 650106, China
[§]Network Security Management Center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, 650106, China

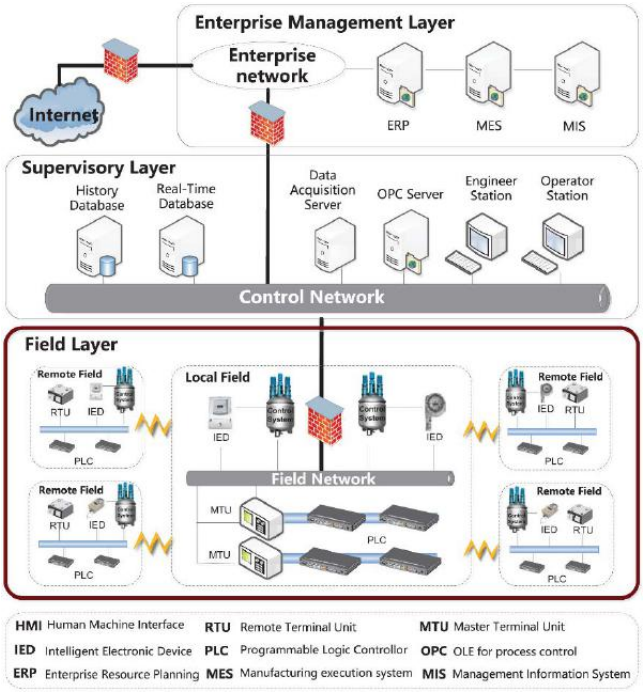

Fig. 2.1: System intrusion detection system architecture based on attention mechanism.

2. Multi-modal data fusion algorithm. Call $O = \{o_1, o_2, \mathrm{L}, o_n\}$ a pseudo data set. Where o_i is the i post. n represents the number of articles published in the data set. The K and S in any post $o = \{K, S\}$ represent its corresponding text and picture, respectively. The error message detection problem can be represented by the function $f(K, S) \rightarrow y$. The number $y \in \{0, 1\}, 0$ marked here represents the actual information. 1 indicates a system intrusion [9]. The method includes four parts: text feature extraction, image feature extraction, multi-modal fusion and error detection (Figure 2.1 cited in International Journal of Distributed Sensor Networks, 2018, 14(8): 1550147718794615).

2.1. Abnormal text feature extractor. The method takes Bi-GRU as the primary research object. It describes long-term sentence dependencies and contextual information between words [10]. Each word vector is pre-trained and word embedding is carried out in Word2vec. The BTH word of text K initializes the vector $K_i \in R^t$. t represents the algorithm dimension. i text with m words is represented as $K = \{K_1, K_2, \mathrm{L}, K_m\}$. Bi-GRU is calculated as follows:

$$\vec{g}_i = \overrightarrow{GRU}\left(K_i\right); i \in [1, m]$$
$$\overleftarrow{g}_i = \overleftarrow{GRU}\left(K_i\right); i \in [1, m]$$

At time i $\vec{g}_i \in R^t$ represents the implied feature of K_i acquired by the positive GRU. $\overleftarrow{g}_i \in R^t$ represents the implicit characterization of K_i obtained by the reverse GRU. The implicit representation $g_i, g_i = [\vec{g}_i, \vec{g}_i], g_i \in R^{2t}$ is constructed by the connection of $\vec{g}_i$ and $\overleftarrow{g}_i$. The feature matrix $K_n \in R^{m \times 2t}$ of the abnormal text is obtained by the implicit representation superposition of m time steps in turn [11]. The most recent hidden layer vector $\vec{g}_m$ on the current GRU and the first hidden layer vector on the backward GRU are used to characterize the result of $\overleftarrow{g}_1$ bar concatenation, and a complete data set $K_f \in R^{2t}, K_f = [\vec{g}_m, \vec{g}_1]$ is obtained.

2.2. Abnormal image feature extractor. The anomaly image feature extractor method is centered on multiple branches of CNN-RNNs (Figure 2.2 cited in Sensors 2020, 20(22), 6592). The algorithm comprises 5CNN branches, each corresponding to VGG19, and the feature vector $s_t \in R^t (t \in [1, 5])$ can be obtained

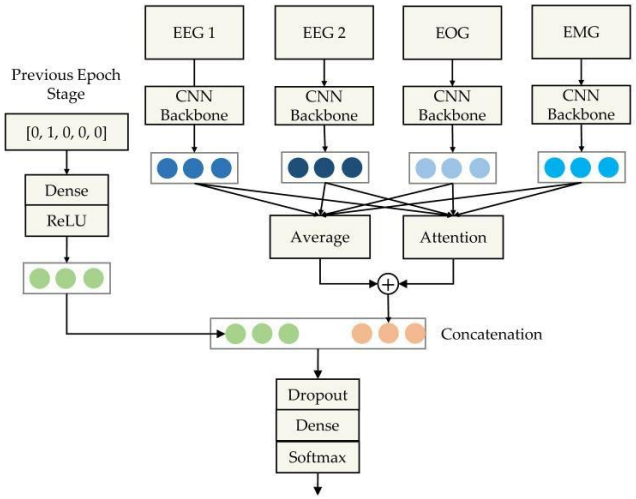

Fig. 2.2: Multi-branch CNN-RNN structure.

by three methods: convolution layer, planarization and complete connectivity [12]. There is a significant dependency relationship between the functions of each level. For example, the texture of a mid-level structure is hierarchical, with low-level feature lines and high-level structural goals. The Bi-GRU model is used to model the sequential dependence between features:

$$\vec{d}_t = \overrightarrow{GRU}\left(s_t\right); t \in [1,5]$$
$$\overleftarrow{d}_t = \overleftarrow{GRU}\left(s_t\right); t \in [1,5]$$

Using A method similar to the text anomaly feature extraction algorithm, the anomaly image feature matrix $S_n \in R^{5\times 2t}$ and the original anomaly image representation $S_f \in R^{2t}, S_f = \left[\vec{d}_5, \overleftarrow{d}_1\right]$ are obtained.

2.3. Multichannel Fusion.

2.3.1. Attention patterns between models. This paper will use the attention mechanism to analyze the degree of correlation between the modes [13]. The purpose is to capture the interaction between the abnormal text and image and realize the correction of the text and image correlation. The attention mechanism is as follows:

$$\text{Attention}(W,T,S) = \text{soft max}\left(\frac{WT^K}{\sqrt{h}}\right)S$$

Attention $(\cdot)$ is the operating function of the attention module. W,T,S is the query matrix, the critical matrix, and the numerical matrix respectively. h is the scaling factor used to avoid excessive molecular dot multiplication, and its value is the dimension of the input property. The abnormal text update matrix K_{update} and image correction matrix S_{update} are obtained by paying attention between models.

$$K_{\text{update}} = \text{Attention}\left(K_n E_{q1}, S_n E_{t1}, S_n E_{s1}\right)$$
$$S_{\text{update}} = \text{Attention}\left(K_n E_{q2}, S_n E_{t2}, S_n E_{s2}\right)$$

Where $K_{\text{update}} \in R^{m\times 2t}; S_{\text{update}} \in R^{5\times 2t}; E_{q1}, E_{t1}, E_{s1}, E_{q2}, E_{t2}, E_{s2} \in R^{2t\times 2t}$. Concatenate K_n and K_{update} into the exception literal property matrix $K_{n1} \in R^{m\times 4t}$:

$$K_{n1} = [K_n, K_{\text{update}}]$$

Similarly, the anomaly image property matrix $S_{n1} \in R^{5\times 4t}$ can be obtained:

$$S_{n1} = [S_n, S_{\text{update}}]$$

2.3.2. In-mode attention module. The internal connection of a single model is a kind of complement to the interaction between various models. The internal attention model establishes the internal relationship between single patterns. The calculation process is as follows:

$$K_{n2} = \text{Attention}\left(K_{n1}E_{q11}, K_{n1}E_{t11}, K_{n1}E_{s11}\right)$$
$$S_{n2} = \text{Attention}\left(S_{n1}E_{q21}, S_{n1}E_{t21}, S_{n1}E_{s21}\right)$$

$K_{n2}R^{m\times 4t}$ and $S_{n2} \in R^{5\times 4t}$ are the feature matrices of the final intrusion system exception text and exception picture respectively. $E_{q11}, E_{t11}, E_{s11}, E_{q21}, E_{t21}, E_{s21} \in R^{4t\times 4t}$. 2.3.3 Fusion Module. Average pooling of the above obtained K_{n2} and S_{n2} to obtain the final feature description $R_K, R_S \in R^{4t}$ of the abnormal text and image:

$$R_K = \text{AvgPool}\left(K_{n2}\right)$$
$$R_S = \text{AvgPool}\left(S_{n2}\right)$$

AvgPool$(\cdot)$ is average pooling. The text representation R_K and image representation R_S are joined to form abnormal text and image to represent $R'_f \in R^{8t}$ and $R'_f = [R_K, R_S]$ together. Through the linear transformation of the model, the joint representation $R_f \in R^{2t}$ of the multiple modes is obtained.

2.4. System Intrusion Detector. The information between the original text and the original image is always missing when merged. The attention mechanism is constructed to represent the K_f of each channel. S_f and multichannel commonfeature R_f are reintegrated to strengthen the original signal. The calculation process is as follows:

$$c_t = \tanh\left(E_w g_t + b_w\right); t \in [1, 3]$$
$$\beta_t = \frac{\exp\left(c_t^T c_w\right)}{\sum_t \exp\left(c_t^T c_w\right)}$$
$$f = \sum_t \beta_t g_t$$

E_w stands for weighting matrix. b_w refers to a biased term. g_1, g_2, g_3 stands for $R_f, S_f, K_f \cdot c_1, c_2, c_3$ is a nonlinear transformation of g_1, g_2, g_3. In the training phase, the situation vector c_w is randomly initialized and co-learned. Where β_t is the normalized weighting of the t eigenvalue. f is an indication of a higher level of entry into a position [14]. The probability distribution is obtained by projecting the advanced representation f into a binary target space using a fully connected layer with softmax activation:

$$o = \text{soft}\max\left(E_c f + b_c\right)$$

E_c stands for the weighted parameter. b_c refers to a biased term. The mutual entropy difference between the predicted probability distribution and the actual label defines the loss function:

$$D = -\sum_{i=1}^{n} \left[y_i \log o_i + (1 - y_i) \log\left(1 - o_i\right)\right]$$

n indicates the number of abnormal texts. $y_i \in \{0, 1\}$ is the value of the actual flag. 1 is system intrusion, o is accurate information. o_i stands for the probability of being predicted to be attacked by the system.

3. Performance analysis. NS_3 simulator was used to simulate AID-DFS. The simulated WSN has 25 nodes. It is distributed in the range of 100 mx100m.This paper divides it into four clusters and is communicated through the hierarchical dynamic source routing mechanism [15]. The algorithm's performance is compared and analyzed using the KDDCUP 1999 database. Other parameters of the simulated WSN are listed in Table 3.1.

Table 3.1: Simulation parameters.

Parameter	Value
Simulation time/s	660
Communication radius /m	100
Packet size /B	250
Scope of trust score	[0,1]
Weight parameter	0.7
Types of intrusion attack	DoS/Probing/U2R/R2L

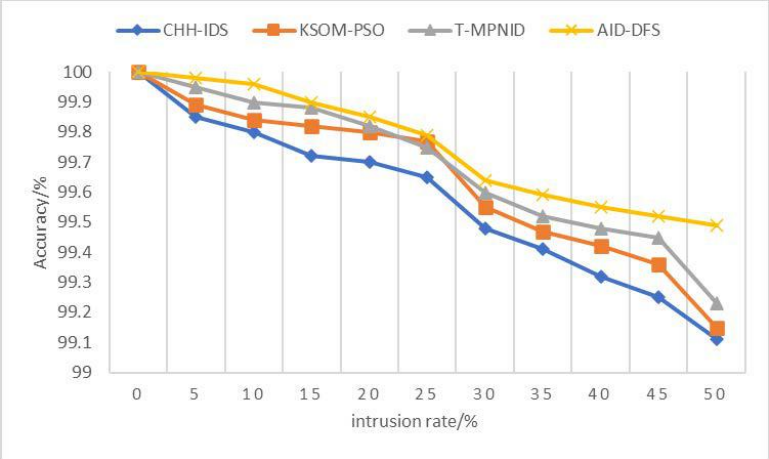

Fig. 3.1: Comparison of the accuracy rates of intrusion detection of four schemes.

3.1. Accuracy. Accuracy rate (AR) is the probability of accurately distinguishing between intrusion attacks.

$$R_A = \frac{P_T + N_T}{P_T + N_T + P_F + N_F}$$

N_F is the false negative ratio. Where N_T is the actual negative ratio. Figure 3.1 shows the change of recognition accuracy of AID-DFS, CHH-IDS (reference [4]), KSOM-PSO (reference [5]), and T-MPNID (reference [7]) algorithms for different attack modes, where $\Delta R = 0.25$. It can be seen from Figure 3.1 that the recognition accuracy of the four methods for different attack modes is reduced to different degrees, among which the recognition accuracy of CHH-IDS is the largest. The identification accuracy of CHH-IDS, KSOM-PSO, T-MPNID and other intrusion methods reaches $99.80\%, 99.86\%$ and 99.93%, respectively, when the intrusion speed is 20%. When the intrusion rate is 50%, the identification accuracy of CHHIDS reaches $99.20\%, 99.33\%$ and 99.52%, respectively. AID-DFS has a recognition accuracy of 99.33% and 99.70% for different species, respectively.

3.2. Detection rate. Detection rate (DR) is the probability that an intrusion can be correctly detected:

$$R_D = \frac{P_T}{P_T + P_F}$$

Figure 3.2 shows the difference in detection rates of AID-DFS, CHH-IDS, SOMPSO and T-MPNID algorithms under different attacks. As shown in Figure 3.2, the detection speed of the four methods decreases with the increase in the intrusion rate, significantly decreasing the detection speed of CHH-IDS. The detection rates of the AID-DFS method were $93.69\%, 94.49\%$ and 96.60% at $31.25\%, 97.92\%$ and 99.27%, respectively. In $50.05\%, 88.99\%$ and 91.59% cases, the AID-DFS method can achieve a 98.85% detection rate.

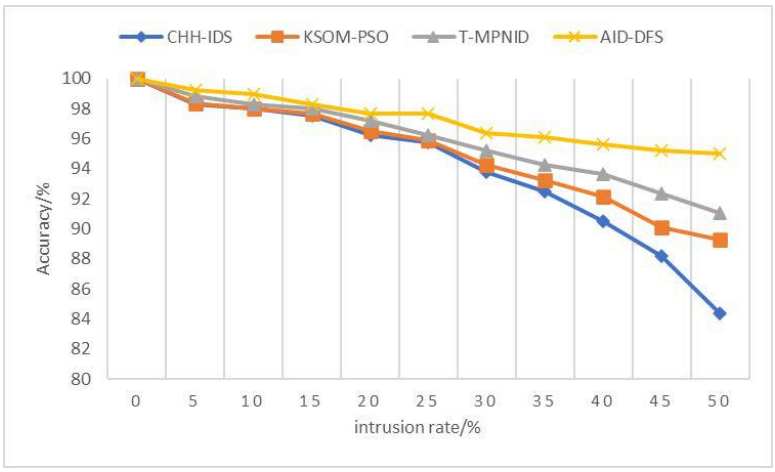

Fig. 3.2: Comparison of intrusion detection rates of the four schemes.

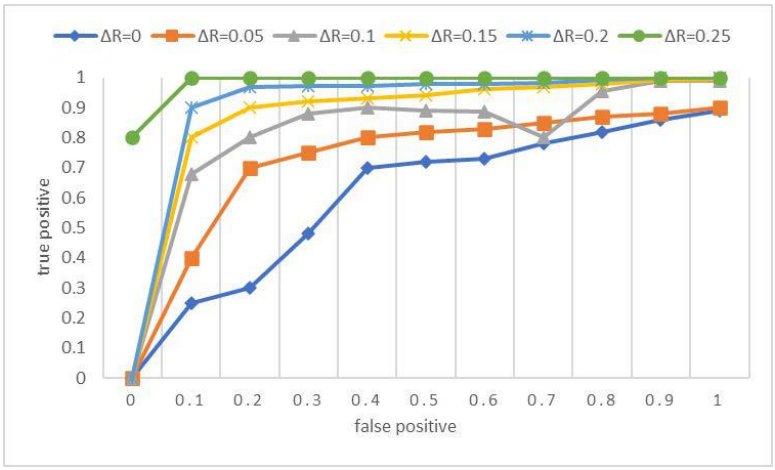

Fig. 3.3: ROC characteristics under different ΔR.

3.3. ROC Characteristics. FIG. 5 shows that the total transmission time of the AID-DFS system changes with the change of FP under different transmission regulation ratios ΔR. This performance is mainly used to analyze the ROC characteristics of the AID-DFS intrusion detection scheme [16]. With the increase of FP, the total attack rate of the AID-DFS system increases with time (Figure 3.3). When the time delay coefficient is 0, the time delay of the AID-DFS system is the lowest. The intrusion algorithm using AID-DFS has the maximum TP value when ΔR=0.25. The AID-DFS system has the best ROC characteristic at ΔR=0.25.

3.4. Precision rate curve. As the recall rate changes, the accuracy of the system changes. The higher the correct rate, the better the performance. This strategy has the best performance when the correct rate tends to 1 . The recall rate here is defined as $P_T/(P_T + N_F)$. Figure 3.4 shows the change in the precision rate curve of AIDDFS at different transfer adjustment ratios ΔR. The DFS algorithm has the lowest accuracy when $\Delta R = 0$; the DFS intrusion detection algorithm has a high accuracy rate when $\Delta R = 0.25$. In the case of $\Delta R = 0.25$, the intrusion detection algorithm using AIDDFS can obtain the best performance. The recall rate and accuracy of the AID-DFS intrusion detection scheme reached 99.98% and 90.19%, respectively.

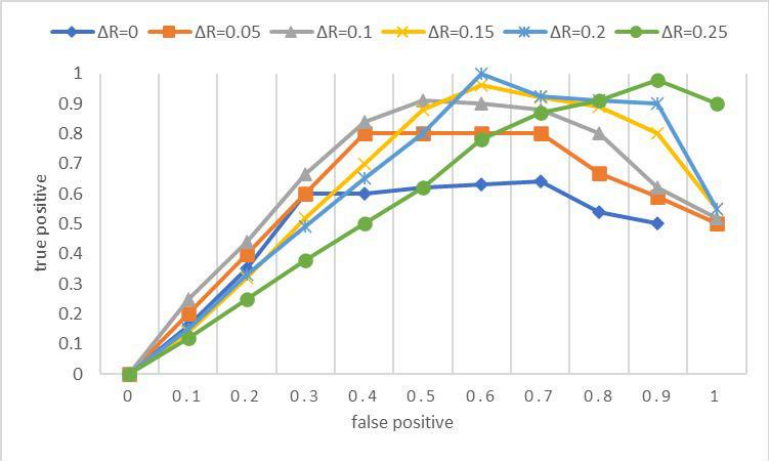

Fig. 3.4: Accurate rate curves under different ΔR.

4. Conclusion. Wireless sensor network (WSN) is the most essential infrastructure monitoring technology currently used. This paper presents an adaptive intrusion detection scheme in the data fusion phase of wireless sensor networks. The interrater-based attention mechanism is proposed to reintegrate the multichannel common expression in different modes and strengthen the original information. Through simulation tests, the algorithm proposed in this project has strong robustness in practical application, with an accuracy of 99.69% and a detection rate greater than 94.99%, which is about 0.5% higher than other traditional methods. In the case of ΔR=0.25, the algorithm proposed has the best reception and operation characteristics, and the recall rate and accuracy rate can reach 99.90 and 90.20%.

REFERENCES

[1] Kumar, S., Chaube, M. K., Nenavath, S. N., Gupta, S. K., & Tetarave, S. K. (2022). Privacy preservation and security challenges: a new frontier multimodal machine learning research. International Journal of Sensor Networks, 39(4), 227-245.

[2] Meng, W., Cai, Y., Yang, L. T., & Chiu, W. Y. (2021). Hybrid emotion-aware monitoring system based on brainwaves for internet of medical things. IEEE Internet of Things Journal, 8(21), 16014-16022.

[3] Wagan, S. A., Koo, J., Siddiqui, I. F., Qureshi, N. M. F., Attique, M., & Shin, D. R. (2023). A fuzzy-based duo-secure multi-modal framework for IoMT anomaly detection. Journal of King Saud University-Computer and Information Sciences, 35(1), 131-144.

[4] Rasheed, A., Mahapatra, R. N., Varol, C., & Narashimha, K. (2021). Exploiting zero knowledge proof and blockchains towards the enforcement of anonymity, data integrity and privacy (adip) in the iot. IEEE Transactions on Emerging Topics in Computing, 10(3), 1476-1491.

[5] Liu, W., Wei, X., Lei, T., Wang, X., Meng, H., & Nandi, A. K. (2021). Data-fusion-based two-stage cascade framework for multimodality face anti-spoofing. IEEE Transactions on Cognitive and Developmental Systems, 14(2), 672-683.

[6] Abate, A. F., Cimmino, L., Cuomo, I., Di Nardo, M., & Murino, T. (2022). On the impact of multimodal and multisensor biometrics in smart factories. IEEE Transactions on Industrial Informatics, 18(12), 9092-9100.

[7] Hussain, M., Fidge, C., Foo, E., & Jadidi, Z. (2021). Discovering data-aware mode-switching constraints to monitor mode-switching decisions in supervisory control. IEEE Transactions on Industrial Informatics, 18(6), 3734-3743.

[8] Luo, F., Khan, S., Huang, Y., & Wu, K. (2022). Activity-based person identification using multimodal wearable sensor data. IEEE Internet of Things Journal, 10(2), 1711-1723.

[9] Khamis, M., Marky, K., Bulling, A., & Alt, F. (2022). User-centred multimodal authentication: securing handheld mobile devices using gaze and touch input. Behaviour & Information Technology, 41(10), 2061-2083.

[10] Panagiotou, P., Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2021). Host-based intrusion detection using signature-based and ai-driven anomaly detection methods. Information & Security, 50(1), 37-48.

[11] Kordestani, M., & Saif, M. (2021). Observer-based attack detection and mitigation for cyberphysical systems: A review. IEEE Systems, Man, and Cybernetics Magazine, 7(2), 35-60.

[12] Jha, R. K. (2023). Strengthening Smart Grid Cybersecurity: An In-Depth Investigation into the Fusion of Machine Learning and Natural Language Processing. Journal of Trends in Computer Science and Smart Technology, 5(3), 284-301.

[13] Huang, K., Wu, Y., Wang, C., Xie, Y., Yang, C., & Gui, W. (2020). A projective and discriminative dictionary learning for high-dimensional process monitoring with industrial applications. IEEE Transactions on Industrial Informatics, 17(1), 558-568.
[14] Hu, C., Yin, M., Liu, B., Li, X., & Ye, Y. (2021). Identifying illicit drug dealers on instagram with large-scale multimodal data fusion. ACM Transactions on Intelligent Systems and Technology (TIST), 12(5), 1-23.
[15] Sun, J., Khan, F., Li, J., Alshehri, M. D., Alturki, R., & Wedyan, M. (2021). Mutual authentication scheme for the device-to-server communication in the Internet of medical things. IEEE Internet of Things Journal, 8(21), 15663-15671.
[16] Hang, F., Xie, L., Zhang, Z., Guo, W., & Li, H. (2023). RETRACTED ARTICLE: Artificial intelligence enabled fuzzy multi-mode decision support system for cyber threat security defense automation. Journal of Computer Virology and Hacking Techniques, 19(2), 257-269.

Edited by: Zhigao Zheng
Special issue on: Graph Powered Big Aerospace Data Processing
Received: Nov 16, 2023
Accepted: Nov 29, 2023