processes

Article

Fuzzy Harmony Search Technique for Cyber Risks in Industry 4.0 Wireless Communication Networks

Zhifeng Diao [1] and Fanglei Sun [2,*]

[1] College of Design and Innovation, Tongji University, Shanghai 200092, China
[2] School of Creativity and Art, ShanghaiTech University, Shanghai 201210, China
* Correspondence: sunfl@shanghaitech.edu.cn

Abstract: Industry 4.0 houses diverse technologies including wireless communication and shared networks for internal and external operations. Due to the wireless nature and remote operability, the exposure to security threats is high. Cyber risk detection and mitigation are prominent for secure industrial operations and planned outcomes. In addition, the system faces the threat of intelligence attacks, security standards issues, privacy concerns and scalability problems. The cyber risk related research problems influence overall data transmission in industry wireless communication networks. For augmenting communication security through cyber risk detection, this article introduces an Explicit Risk Detection and Assessment Technique (ERDAT) for cyber threat mitigation in the industrial process. A fuzzy harmony search algorithm powers this technique for identifying the risk and preventing its impact. The harmony search algorithm mimics the adversary impact using production factors such as process interruption or halting and production outcome. The search performs a mimicking operation for a high objective function based on production output for the admitted plan. The fuzzy operation admits the above factors for identifying the cyber impacting risk, either for its impacts or profitable outcome. In this process, the fuzzy optimization identifies the maximum or minimum objective output targeted for either outcome or risk interrupts, respectively. The fuzzy threshold is identified using a mediated acceptable range, computed as the ratio between minimum and maximum, mimicking occurrences between the risk and scheduled production outcomes. Therefore, the mimicking crossing or falling behind the threshold for the interruption/halting or production, respectively, are identified as risks and their source is detected. The detection communication source is disconnected from the industrial process for preventing further adversary impacts. The introduced system achieves 8.52% high-risk detection, 12.5% fewer outcome interrupts, 8.3% fewer halted schedules, 8.08% less interrupt span, and 7.94% less detection time compared to traditional methods.

Keywords: communication networks; cyber security; FHS; industry 4.0; risk detection

check for updates

Citation: Diao, Z.; Sun, F. Fuzzy Harmony Search Technique for Cyber Risks in Industry 4.0 Wireless Communication Networks. *Processes* **2023**, *11*, 951. https://doi.org/10.3390/pr11030951

Academic Editors: Adel Ali Ahmed, AbdulRahman Alsewari, Yousef Fazea and Waleed Ali

Received: 15 February 2023
Revised: 8 March 2023
Accepted: 9 March 2023
Published: 20 March 2023

1. Introduction

Industry 4.0 is the fourth industrial revolution that rapidly contains automated machines and technologies to perform industry-related tasks. Industry 4.0 enhances the efficiency and productivity range of products. Various risks and challenges occurred in industry 4.0, which enormously reduced the production range [1]. Cyber security risks also occur in industries that lead to the loss of a huge amount of data due to attacks. Malware and ransomware are the major cyber-security risks that cause attacks due to malfunctions in software [2]. Insufficient security policies also cause severe damage and attack possibilities in industry 4.0. Cyber security risk prediction and prevention are crucial tasks to perform in industry 4.0. The cyber security analysis-based method is mostly used for risk prediction in industry 4.0 [3]. A reference architecture model is used here to detect threats and risks based on certain functions and operations. A monitoring system is implemented in every industry that gathers information that is relevant to production and risks [4]. The monitoring system reduces the latency in cyber-attack risk prediction, enhancing industries' efficiency ratio. Information and communication technologies (ICT) are used in industry 4.0, providing various services and functionalities during the manufacturing process [5].

Various methods and techniques are used to address cyber-security risks which occurred in industry 4.0. The Artificial Intelligence (AI) technology-based detection method is commonly used for the cyber-security detection processes. The Artificial Neural Network (ANN) algorithm detects the threats which contain abnormal risks in a process [6]. The feature selection method in ANN extracts the important features and patterns relevant to risks and problems [7]. Third-party attacks and risks are predicted by the feature selection method, reducing the early detection latency. ANN also identifies the actual cause of threats and the location of risks, which are presented in industry 4.0 [8]. The Industrial Internet of Things (IIoT) network is used in industries that provide certain services for the product improvement process. The IIoT-based detection method is also used for the risk detection process [9]. IIoT analyzes the datasets which are presented in the database, which produce feasible information for the further risk detection process. IIoT identifies the risks which occur during interaction and communication processes. IIoT improves risk detection accuracy, enhancing industries' performance and production levels [10].

Machine learning (ML) techniques and methods are most commonly used for prediction and detection processes. ML is mainly used to achieve high accuracy in the detection process. ML is used in the cyber risk detection process for industry 4.0 [11]. ML-based methods are used in the cyber-security risk prediction process. Convolutional neural network (CNN) is used as a detection method that detects the malfunctions and risks which occur during interaction and production processes. CNN improves the overall production and feasibility range of industries, enhancing efficiency among other organizations [6,12]. An adaptive deep learning (ADL) algorithm is also used for the cyber risk detection process. The ADL algorithm detects industries' network traffic and data flow that provides relevant data for further processes. ADL reduces both the computation cost and time consumption ratio in the computation process, which increases the accuracy of the detection process [13]. A deep neural network (DNN) model is used for the optimization process. Principle component analysis (PCA) is implemented in the DNN model that analyses the data which is eliminated by certain operations. PCA detects the original data required for the optimization process and provides feasible solutions to solve optimization problems in industries [14,15]. However, these methods are consumed with difficulties while handling the threat intelligence because several intermediate attacks reduce the system efficiency and cause security related issues. The security related cyber risks are overcome by applying the fuzzy harmony search. The contributions of this article are highlighted below:

(1) Designing a risk detection technique for smart industrial communication networks to prevent cyber threats for uninterrupted production outcomes.
(2) Incorporating the fuzzy harmony search process for analyzing, classifying, and detecting mimicking operations for maximizing production-based objectives.
(3) Performing a dataset-based analysis for validating the proposed techniques' process flow based on harmony search optimization.
(4) Performing a comparative analysis using specific methods for proving the proposed techniques' consistency with the other existing methods.

2. Related Works

Pearce et al. [16] proposed a smart input–output module for mitigating cyber–physical attacks. The proposed scheme is mostly used in industrial control systems. The actual goal of the proposed scheme is to identify the dangers which are mitigated in industries. The proposed scheme secures real-time applications from cyber-attacks, enhancing the systems' reliability range. The smart I/O module reduces both complexity and difficulties in connectivity. The proposed scheme improves the efficacy and performance range of industries. Ahmadi-Assalemi et al. [17] designed a super learner ensemble for anomaly detection in the industrial control system (ICS). Artificial intelligence (AI) is used that collects the necessary data, which reduces the latency in the data collection process. The proposed method also identifies the cyber risks which are presented in ICS. Cyber risks reduce the workflow and production rate of industries. Experimental results show that the designed method achieves high accuracy in anomaly detection. Wang et al. [18] developed a lightweight approach for the network intrusion detection process in industrial cyber–physical systems (CPS). A deep learning algorithm named deep convolutional neural network (CNN) is implemented in the proposed approach. CNN is mainly used here to improve performance and to increase the speed of the anomaly detection process. Knowledge distillation (KD) is also used to train the data for the detection process. The proposed approach maximizes the accuracy of intrusion detection, improving CPS's effectiveness. Rosado et al. [19] introduced a new methodology for analyzing risks in information systems using meta-pattern and adaptability (MARISMA). The introduced MARISMA method is commonly used to address the risks in cyber–physical systems (CPS). A risk analysis technique is used here that analyzes the risks based on characteristics and behaviors. The introduced method reduces the latency in detection, which enhances the performance and efficiency level of CPS. When compared with other methods, the introduced MARISMA increases the accuracy of the risk detection process. Traganos et al. [20] proposed a reference architecture named the HORSE framework for cyber–physical systems (CPS) in smart manufacturing industries. Important characteristics and features are detected from the database, producing feasible information for further processes. The reference architecture acts as a safety detection method that identifies the cyber-attacks' risks that occurred during production.

The proposed HORSE framework improves smart industries' overall production and manufacturing range. Farrugia et al. [21] developed a real-time prescriptive solution for explainable cyber-fraud detection. Machine learning (ML) algorithms are used here to detect the actual cyber-fraud located in an application. The actual behaviors of frauds and intrusions are examined, which provides feasible data for the detection process. The proposed method reduces both the time and energy consumption ratio in the computation process. The proposed method achieves high accuracy in cyber-fraud detection, which maximizes the efficiency and flexibility level of the systems. Leong et al. [22] designed a cyber risk cost management method for Internet of Things (IoT) devices-based health insurance. The proposed method's main aim is to ensure users' safety and security to obtain proper insurance. Cyber risks and problems are detected by this method, which reduces the complexity and difficulties ratio in cost management systems. The proposed method improves the performance and energy-efficiency range of IoT-linked health insurance systems. Pinto et al. [23] proposed a data-driven anomaly detection method for cyber–physical production systems (CPPS). The proposed method detects the attacks which are presented in the edge layer of CPPS. An artificial intelligence-based model is used here to tackle the attacks occurring during manufacturing and production processes. Experimental results show that the proposed method increases the accuracy of anomaly detection, enhancing the systems' effectiveness and performance level. Zängerle et al. [24] developed an enterprise-level cyber risk prediction method. The actual goal of the proposed method is to address the risks and problems which cause severe damage to the production and manufacturing systems. The proposed method predicts the sparse data availability which is required for various processes. Unwanted threats and cyber risks are detected here, reducing the overall complexity of certain tasks. The developed method maximizes the efficiency and feasibility range of the systems. Pantano et al. [25] introduced a human cyber–physical system approach for lean automaton. An industrial 4.0 reference architecture is used here that addresses human integration and operation in a system. The main aim of the introduced approach is to improve flexibility and reduce the complexity ratio of the systems. Human mistakes and malfunctions are detected here, reducing production system errors. Compared with other approaches, the introduced approach enhances the performance and effectiveness level of the systems. Latino et al. [26] proposed a reference framework for cyber-security in the food and beverage industries. A thematic analysis is used here that identifies the important datasets which are required to perform a certain task in industry.

The reference framework detects cyber threats, problems, and challenges. Both time and energy consumption ranges in the computation are reduced. The proposed framework improves both the flexibility and robustness range of the food and beverage industries. Miehle et al. [27] designed a stochastic Petri net approach for smart factories. The designed method is an information network analysis that analyzes the information based on certain conditions. The threats and problems which occur during manufacturing are detected using the Petri net approach. The proposed approach reduces the IT network complexity in smart industries. The proposed approach increases the accuracy of attack detection, enhancing smart factories' performance. Shahin et al. [28] presented a fully convolutional neural network (FCN) approach for cyber-attack detection and classification processes in smart manufacturing systems. Industrial Internet of Things (IIoT) devices are commonly used in manufacturing systems, which leads to various problems. Intelligence tools are used here to detect the threats and attacks from the manufacturing systems. Experimental results show that the proposed FCN approach achieves high accuracy in attack detection, which reduces the latency in further processes. Jbair et al. [29] introduced a structured threat modeling approach for industrial cyber–physical systems (CPS). The main aim of the proposed approach is to identify the threats which occurred due to smart manufacturing systems. The introduced method is end-to-end modeling which detects the threats based on characteristics and functions. The exact impacts and ability of threats are also identified, reducing the computation process's complexity. The introduced method increases the safety and security ratio of CPS from attackers.

The so far discussed methods rely on external data observed from the ground devices and inputs from the previous performance as discussed in [16,19]. The methods in [18,20,21] address the aforementioned issues for handling shortcomings using classification. In classification, the complexity of handling adverse impacts is suppressed in the later methods [24,27]. However, risk assessment relies on predicted and observed outcomes for identifying different halts and their precise reason. The proposed technique relies on this information for reducing the halts due to interrupts coping with the production plan. The adaptability of balancing the performance and risk mitigation to be maintained, is accomplished by the proposed technique.

3. Explicit Risk Detection and Assessment Technique

The proposed ERDA technique is introduced to detect and mitigate cyber risk in industrial operations to improve security. The different technologies in wireless communication networks remotely accessed and regulated through processing units in the industry depend on better accuracy for their operations and planned outcomes. Both data processing and production monitoring integrations comprise security threats due to the remote operability and wireless nature exposed through cyber risk detection. Some common wireless communication networks based on industry 4.0 house technologies that are used for performing external and internal operations which is a prominent factor in which the adversary/risk can be thwarted through a fuzzy harmony search algorithm (FHS). ERDAT is one such technique used for classifying the processing unit. Figure 1 presents the proposed techniques' illustration.

The process of ERDAT in wireless communication networks assisted industry 4.0 in acquiring a prediction plan and adversary detection to prevent its impact. Production monitoring and data processing in the industrial unit through communication networks are processed. The prediction plan is used for classifying the processing between risk and scheduled production. The classification output is used for identifying the process interruption or halting and production outcome by the correlation analysis from the stored industrial data. The process of explicit risk detection and the computation technique is used to prevent adversaries, where the prediction plan is initially processed. The input prediction plan in industry 4.0 is represented in Equations (1) and (2).

$$Ind_n = \frac{1}{N_i}\left|\sum_{t=1}^{N_i} P_O(t) - I_H(t)\right| \tag{1}$$

where,

$$\left.\begin{array}{c} P_O(t) = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{\alpha_M(t)}{N_i * t} dt \\ and \\ I_H(t) = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{\beta_M(t)}{N_i * t} dt \end{array}\right\} \tag{2}$$

where, $P_O(t)$ and $I_H(t)$ means the production outcome and process interruption/halt in the wireless communication networks for the mimicking operations based on α and β. If α_M and β_M are the minimum and maximum profitable outcome and process interruption or halting at different time t intervals. This mimicking operation M is performed through the harmony search algorithm HSA for gaining profitable outcomes and identifying the cyber risks. The variable N_i used to denote the amount of processing performed in a single industrial unit. Then, $\alpha_M \in [0, \infty]$ and $\beta_M \in [-\infty, 0]$, and hence, the harmony search algorithm is a relatively fuzzy optimization inspired by industry 4.0 wireless communication networks. The HSA process Equations (3)–(5) identify cyber risk and prevent its impacts on the search domain.

$$HSA \in [0, 1] \tag{3}$$

$$F(X)_{New} = F(X)_{Old} + \Delta_p \tag{4}$$

$$CR_D = min(P_O) \in max(I_H) \tag{5}$$

Such that,

$$\left.\begin{array}{c} P_O(t) = \frac{1}{N_i}\int_{-\infty}^{\infty} \alpha_M.t \in CR_D dt \\ and \\ I_H(t) = \frac{1}{N_i}\int_{-\infty}^{\infty} \beta_M.t \in CR_D dt \end{array}\right\} \tag{6}$$

Equations (3) and (4) computes the initial cyber security is detected and mitigated for all $P_O(t) + I_H(t)$ instances. This sequence of instances represents a complete industrial data processing and production monitoring based on α_M and β_M operations in different time intervals through a fuzzy harmony search algorithm. Here $\exists$ is the overall industrial data and production analysis. The mimicking operation is illustrated in Figure 2.

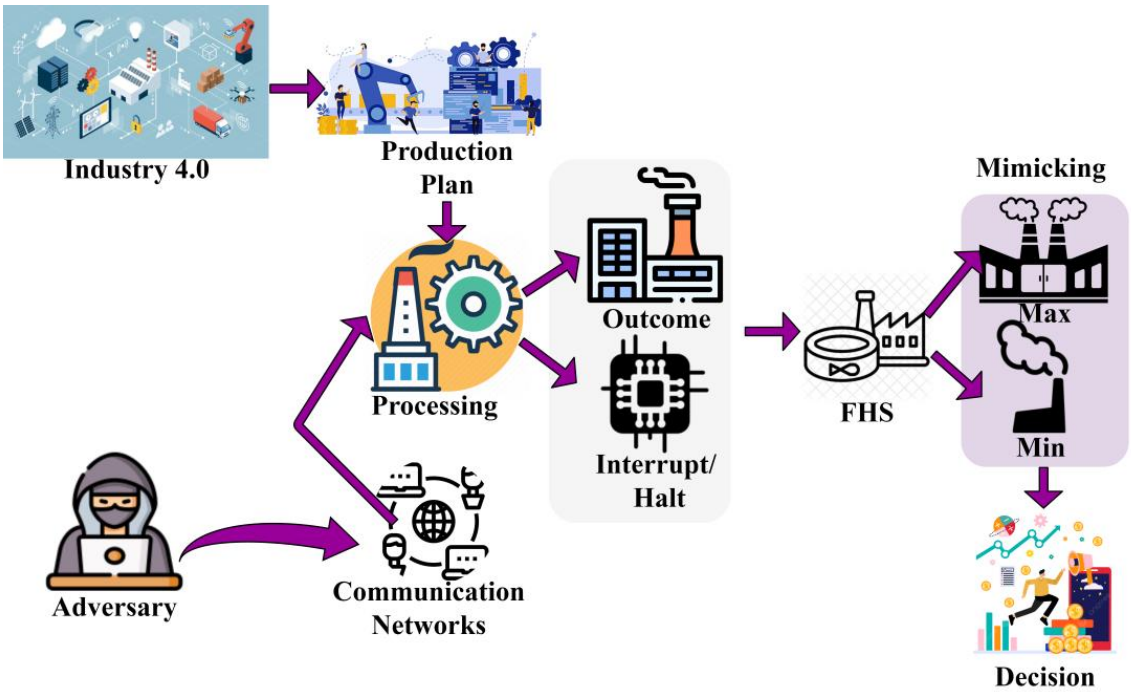


Figure 1. Proposed Technique Illustration.

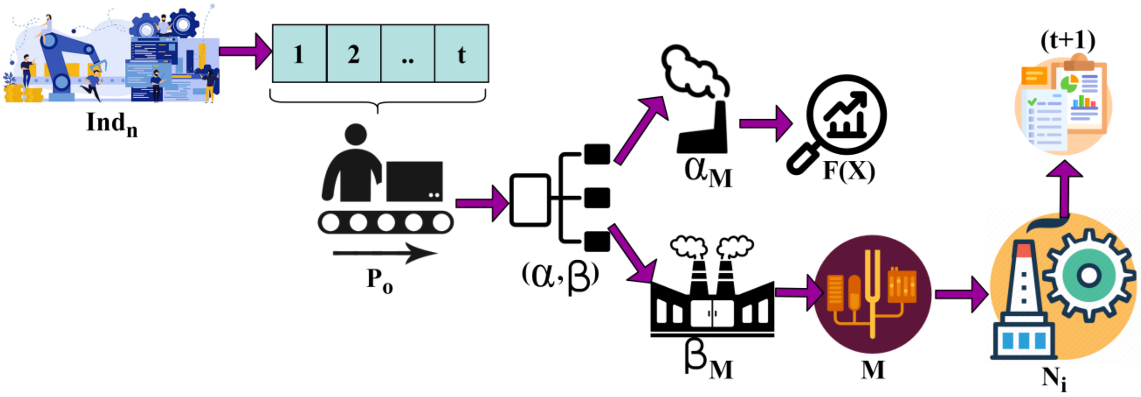


Figure 2. Mimicking Operation.

The production output is classified $\forall(\alpha,\beta)$ such that α_M and β_M are used for assessment. In the α_M, β_M outcomes, β_M is alone mimicked for $N_i + i \in (t+1)$. The α_M, the generated output is pursued $F(X)$ for identifying any risks in the previous t. This analysis is not pursued under M for t whereas $(t+1)$ pursues (α,β) for classification (Figure 2). Processing is classified as production outcome and interruption/halting to reduce the adversary impact present in communication networks. Adversary impact is due to the cyber impacting risk identified in the industrial processing unit while observing production output in any instance. Therefore, the normalization of data processing and production monitoring follows a high-objective function Obj_F and is expressed as

$$\left.\begin{array}{l} P_O(t) = \frac{\alpha_M(t)}{N_i \times t} \times 2^{\frac{A}{2}} fuzzy_{opt_i}\left[\exists \times t - \frac{A}{2}\right] \\ I_H(t) = \frac{\beta_M(t)}{N_i \times t} \times 2^{\frac{A}{2}} fuzzy_{opt_j}\left[\exists \times t - \frac{A}{2}\right] \end{array}\right\} \tag{7}$$

where,

$$\left.\begin{array}{c} fuzzy_{opt_i} = Obj_F(t)\left|\frac{A}{2}\right|F(t)_{l-1} \\ and \\ fuzzy_{opt_j} = Obj_F(t)^{-1}\left|\frac{A}{2}\right|F(t)_{l-1} \end{array}\right\} \tag{8}$$

Based on the Equations (7) and (8), the variable $fuzzy_{opt_i}$ and $fuzzy_{opt_j}$ represents the admitted plan for performing a mimicking operation based on production outcomes and interrupt/halt occurrence identification. The production factors such as process interruption $Obj_F(t)$ and production outcome $Obj_F(t)^{-1}$ relies on the minimum and maximum mimicking occurrences of $fuzzy_{opt_i}$ and $fuzzy_{opt_j}$. From the mimicking occurrence in the industry 4.0, wireless communication networks for the high objective function based on production outcome are computed. The variable A is used to denote the adversary impact in the communication networks and also for the process of cyber risk detection. Now, the source mitigation in industry 4.0 admits the above factors for detecting the cyber impacting risk and is computed as

$$\left.\begin{array}{c} \complement[Obj_F(t)] = \frac{A}{2}\frac{(\exists)-I_H}{t^2}\left[fuzzy_{opt_i} - fuzzy_{opt_j}\right] \\ and \\ \complement\left[Obj_F(t)^{-1}\right] = \frac{2^{\frac{A}{2}}}{t}\left[\int_0^{\infty}\frac{fuzzy_{opt_i}[(\exists)-I_H]}{t}dt - \int_{-\infty}^{0}\frac{fuzzy_{opt_j}[(\exists)-A]}{t}dt\right] \end{array}\right\} \tag{9}$$

The cyber-impacting risks $\complement[Obj_F(t)]$ are detected after performing the harmony search algorithm. From this instance, two factors, production outcome and process interruption/halt, are extracted for further process classification. Equation (10) is used to evaluate the scheduled production outcome (S_{PO}) and risk occurrence (R_{OC}) measure for profitable output and is represented as

$$\left.\begin{array}{c} S_{PO} = \frac{1}{2\pi(\exists\times A)}\left|\sum_{t=1}^{i}(\alpha_M+\beta_M)Thr\right|, \forall i \in A, j = i+1 \\ and \\ R_{OC} = -\sum_{i=min_{out}}^{max_{out}} Thr\log S_{PO_i} \end{array}\right\} \tag{10}$$

where the variable max_{out} and min_{out} are the maximum and minimum objective outputs of S_{PO} as identified. The log normalization of scheduled production outcome identifies the overlapping functions in source mitigation as in Equation (11)

$$R_{OC}[Obj_F(t)] = \frac{R_{OC}}{\log\left[\frac{max_{out}-min_{out}}{t}\right]} \tag{11}$$

This log normalization process is performed for continuing the fuzzy operation and cyber risk occurrence detection along with the various technology and time intervals. The classification process is based on S_{PO} and $R_{OC}[Obj_F(t)]$ using fuzzy optimization. This industrial processing unit classification helps to differentiate the outcome interrupt and halted schedules for all either $P_O(t)$, or $I_H(t)$, or both processes. The risk occurrence estimation from the previous intervals is diagrammatically presented in Figure 3.

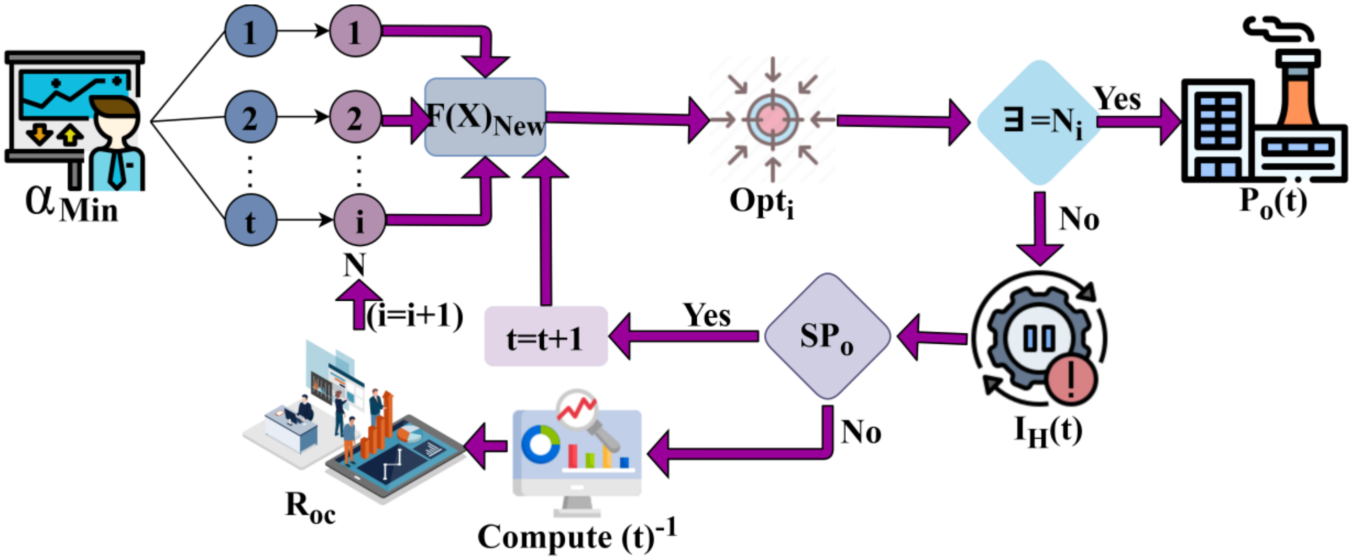


Figure 3. Risk Occurrence Estimation.

The risk occurrence estimation is performed by mapping t and N_i for evaluating $F(X)_{New}$. This is different from the previous occurrences, $\forall \exists = N_i$ analysis. If the case fails, then I_H in the specific t is estimated. This requires S_{P_o} checking under t and $(t)^{-1}$ constraints from which R_{oc} is identified. If R_{oc} is identified under any i, then the process is halted and is considered a risk (Refer to Figure 3). In this processing classification, the threshold is identified at each processing level followed by has. The prediction plan and communication networks are determined as per Equations (12) and (13), either satisfying production outcomes or risk interrupts, respectively.

$$\left.\begin{array}{c} M^O[S_{PO}, Obj_F(t)] = \sum_{i=1}^{\exists} P_O + \sum_{j=1}^{t} I_H - \sum_{i=1}^{\exists}\sum_{j=1}^{t} N_i Obj_F \\ and \\ \mu[S_{PO}, t] = \frac{A^{-M^O[S_{PO}, Obj_F(t)]}}{\sum_{i=1}^{\exists\times t} A^{-M^O[S_{PO}, Obj_F(t)]_{ij}}} \end{array}\right\} \tag{12}$$

In Equation (12), assume the mimicking operation set $M^O[.]$ is sequentially analyzed using the objective function based on scheduled production outcomes. The variable $\mu[.]$ is the initial training set identifying its impact at a different time interval. Similarly, the first production outcome and training sets are given as

$$M^O[R_{OC}(Obj_F(t))], S_{PO} = \begin{cases} \sum_{i=1}^{\exists} N_i - I_H \frac{1}{fuzzy_{opt_i}}, if\ \alpha_M(t) \in [0, \infty] \\ \sum_{i=1}^{\exists} N_i - I_H fuzzy_{opt_j}, if\ \beta_M(t) \notin [0, \infty] \end{cases} \tag{13}$$

And,

$$\mu[R_{OC}(Obj_F(t))] = \frac{(I_H)^{-M^O[S_{PO}, Obj_F(t)]}}{\sum_{i=1}^{\exists \times t} (I_H)^{-M^O[S_{PO}, Obj_F(t)]_{ij}}} \tag{14}$$

In Equation (14), the fuzzy optimization detects the maximum or minimum objective output of the processing and is performed such that $M^O[S_{PO}, Obj_F(t)]$ is evaluated for the mimics operation $\in R_{OC}(Obj_F(t))$. The minimum interruption moves to maximum interruption, whereas the maximum production outcome moves to a minimum, and a fuzzy threshold is identified. This mimicking operation output helps to distinguish the overlapping processes in an industry based on t instance to perform possible classification. Based on Equations (13) and (14), the differences between both the scheduled production outcome and process interruption/halt vary at each time of processing because the objective of the proposed technique lies between these two factors. In this process, these two factors are constant for improving risk detection in industry 4.0. Due to the importance of the two factors, the available processing is converted into fuzzy factors in this condition. Therefore, the fuzzy operation is performed, which functionally adjusts the outcome and risk factors, and the number of processing iterations is considered as the input for FHS. In this case, this consideration is used for performing fuzzy operations because the mimicking values differ when the FHS starts functioning. The fuzzy operation based on two factors is defined by Equations (15) and (16), where the final production outcome and process interruption/halt change their measures in the range [0,1].

$$Z(P_O) = \frac{\sum_{i=1}^{R_{HSA}} \theta_i^{Hmp} \left(Hmp_i^1 \right)}{\sum_{i=1}^{R_{Hmp}} \theta_i^{Hmp}} \tag{15}$$

where Hmp is the harmony search performing mimicking operations and R_{HSA} is the rules and regulations of fuzzy optimization corresponding to targeted objective output. The variable Hmp_i^1 is the first output based on rule 1 corresponds to the harmony search algorithm. The variable θ_i^{Hmp} is the disconnected risk-identified communication source for rules and regulations corresponding to HSA.

$$Z(I_H) = \frac{\sum_{i=1}^{R_{Th_{rat}}} \theta_i^{Th_{rat}} \left(Th_{rat}{}_i^1 \right)}{\sum_{i=1}^{R_{Th_{rat}}} \theta_i^{Th_{rat}}} \tag{16}$$

In Equation (15), Th_{rat} is the threshold ratio identified from the processing and $R_{Th_{rat}}$ is the number of rules and regulations followed by the fuzzy operation corresponding to risk detection. Therefore, $Th_{rat}{}_i^1$ is the first threshold identified network along with rules corresponding to mediate acceptable range. The variable $\theta_i^{Th_{rat}}$ is the disconnected communication source network in industry 4.0 corresponding to risk detection. The harmony search process is represented in Figure 4.

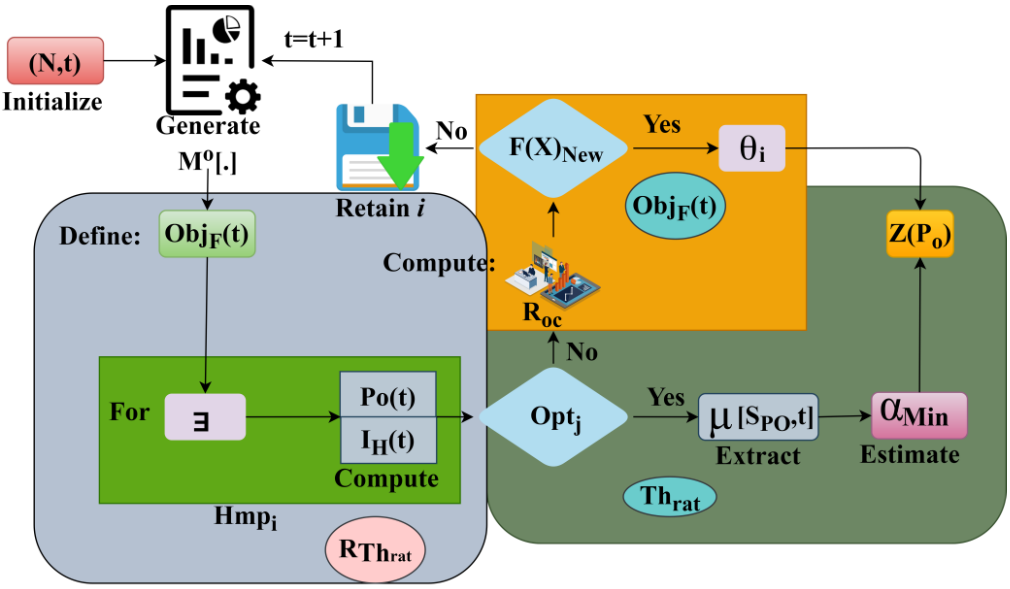


Figure 4. Harmony Search Process.

The initialization is performed using (N, t) for retaining i and $I_H(t)$ estimation. It is to be noted that the above is performed under Hmp_i for the R_{HSA} used. Considering the Opt_j under Th_{rat} the $\mu\left[S_{po}, t\right]$ is used for training $\alpha_{Min}\forall t$. Depending on the $F(X)_{New}$ requirement the θ_i is computed $\forall Obj_F(t)$. This is required for $P_{Th_{rat}}$ pursued out of which the least is used for N_i (Figure 4). Fuzzy optimization is performed based on the mimicking operation, which helps to easily identify the processing interruption and halt occurrence. The factors of process interruption and production outcome are calculated to be changed using fuzzy optimization since these factors address controlling the exploitation and exploration of the harmony search domain. The min and max changes in outcome and risk in industry 4.0 are identified using the HSA algorithm, and this process is important to tune the fuzzy optimized solution. The FHS can be useful in adjusting the mimicking crossing/failing rate behind the threshold for identifying risk and disconnecting that source by the algorithm to find the optimal output. Therefore, the variations in these factors are identified to achieve a better decision. The improved harmony search algorithm (IHS) is generated to gain new production outcomes that enhance the precision and convergence rate of the fuzzy harmony search algorithm. To compute the control performances of security threats in wireless communication networks, a new source is generated with the mediated acceptable limit that ranges from $Hmp_i(0 < Hmp_i < 1)$. Each fuzzy threshold consists of minimum and maximum mimicking occurrence for respective production outcome and risk.

This defines the possible objective output; the riskless and profitable outcome was successfully decided on to join them for generating various fuzzy operations for the mimicking of occurrences of outcome and risk. Based on the article, the recommended values for the available factors from 0 to infinity, in this condition, the range 0 to ∞ and $-\infty$ to 0, were used for better outputs using the fuzzy optimization. The fuzzy harmony search for performing mimicking operations relies on $R_{OC}(Obj_F(t)) \in [-\infty, \infty]$ and $\alpha_M \in [0, \infty]$ or $\alpha_M \notin [0, \infty]$ for a better decision. The case of $\alpha_M \in [0, \infty]$ satisfies riskless industrial processing. From the above, $\alpha_M \notin [0, \infty]$ is identified as the threshold occurring instances. With the use of the fuzzy harmony search technique and ERDAT, the high objective function is required to detect and mitigate cyber risk detection. This process classification helps the wireless communication industry 4.0 to reduce data analysis time and production monitoring time while increasing cyber risk detection and profitable outcome in the industries. Based on the prediction plan and rules, the fuzzy threshold occurrence is identified to improve for FHS with a large number of profitable outcomes. This proposed technique reduces maximum interrupt span and halted schedules. Therefore, the stored industry information is handled for further prediction planning for the next source processing. In this case, $M \in [\infty, -\infty]$ is considered for identifying the cyber risk and preventing its impact on the industry. The mimicking crossing and failing behind the threshold is identified for minimizing overlapping processes based on accumulated and extracted factors from industry 4.0. The dataset from [30] is used for assessing the proposed techniques' performance. Precisely, the operations of a gas turbine control system are recorded and presented for analysis using a hardware-in-the-loop emulator. Figure 5 presents the overview of the control system process with the rules associated.

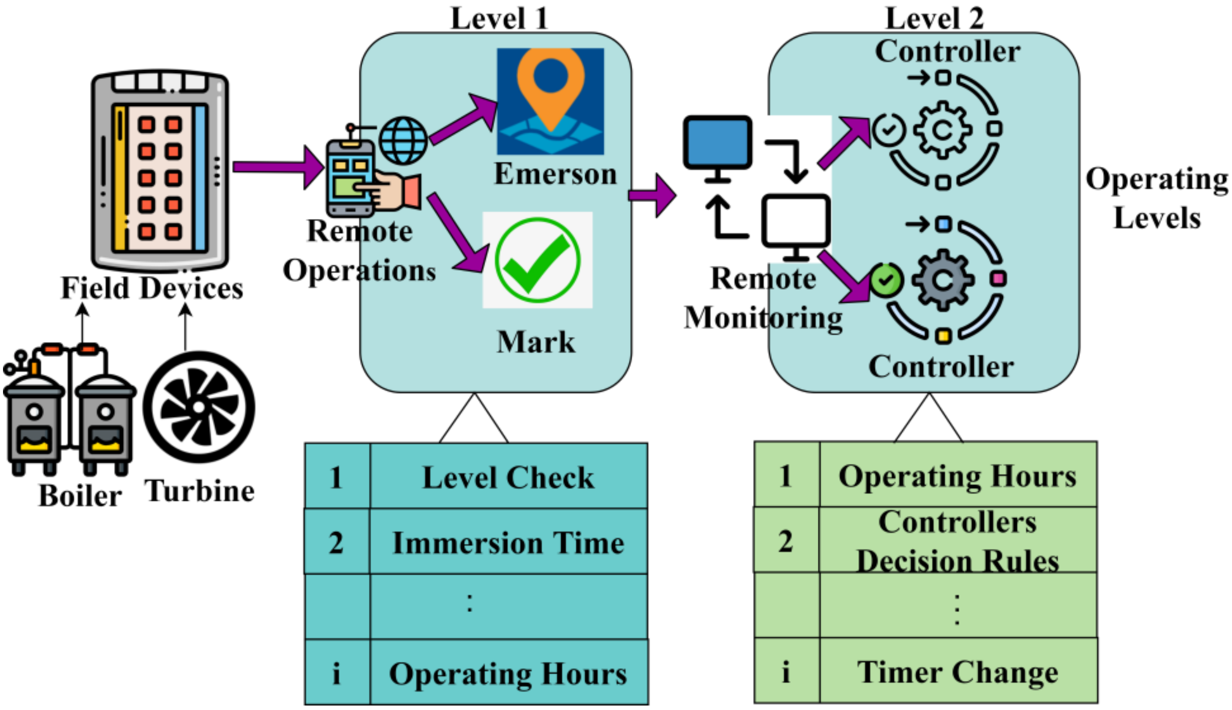


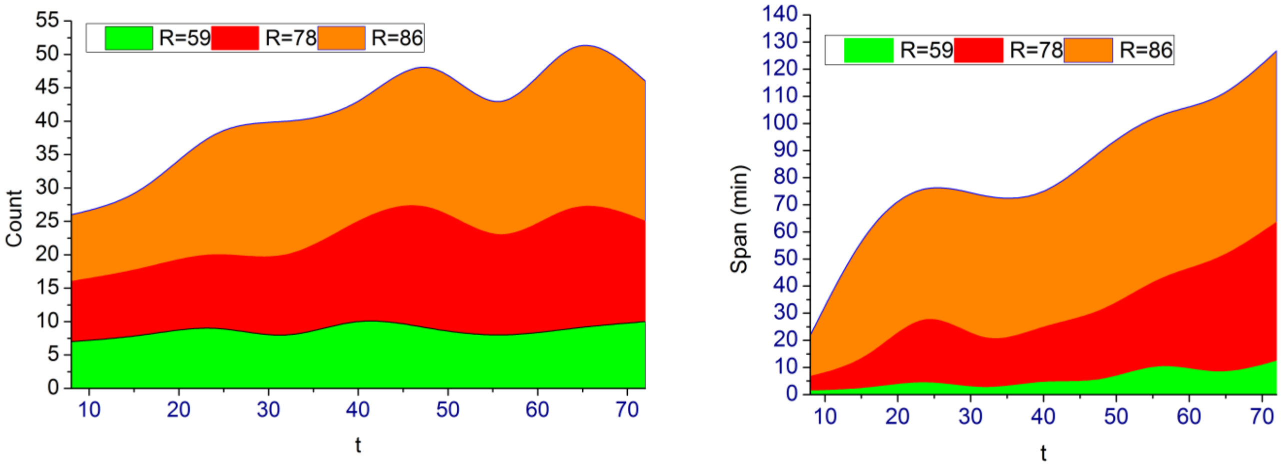
Figure 5. Overview of the Control System Process.

The component overview is presented in Figure 5 from the given dataset, along with the rules and operations. It includes Io devices, PLC controller's emersions marks level indicators, etc. The rules associated with different levels that are associated with the operations are presented. The rules are modified based on the operations and their outcome. In this process, 114 rules are used for operating the gas turbine for a continuous 2 h (Figure 5). The production outcome and risk mitigation are computed for improving the wireless communication industry processing accuracy at different time intervals. The fuzzy threshold is identified at the time of mimicking operation based on data processing and production monitoring instances in industry 4.0. Therefore, the accumulated industrial data processing is not prolonged for risk detection and mitigation. Further prediction planning is used to forecast risk occurrence and mediate an acceptable range of mimicking occurrences between the risk and scheduled production outcomes at t. Cyber risk detection is maximized for optimal decisions without increasing the halted schedules and detection time. The remaining processes maximize interrupt span based on outcome and risk for preventing overlapping sources in smart industries. The changes in particular communication production and risk are moved to new communication using FSA. Hence, the maximum production outcome and minimum interruption are achieved for better decisions, thereby reducing risk detection. Then the overall working process of the fuzzy harmony search based cyber risk identification processing steps are described in Table 1.

Table 1. Fuzzy harmony search based risk identification.

Step 1: Initialize the parameters of the fuzzy harmony search technique, such as the number of solutions, number of iterations, and harmony memory size.
Step 2: Initialize the fuzzy sets for the input variables, such as the security level, threat level, and network performance.
Step 3: Conduct a risk analysis and identification to identify potential cyber risks in industry based communication process.
Step 4: Generate an initial harmony memory by randomly selecting solutions within the search space.
Step 5: Evaluate the fitness of each solution in the harmony memory using the fuzzy logic rules and objective function.
Step 6: Update the harmony memory by replacing the worst solutions with new solutions generated through the fuzzy logic rules and improvisation strategies.
Step 7: Update the fuzzy sets based on the performance of the solutions in the harmony memory.
Step 8: Repeat steps 5–7 until the termination criteria, such as the maximum number of iterations or a threshold fitness value, is reached.
Step 9: Conduct a risk analysis and identification of the solutions in the final harmony memory to identify potential cyber risks and their likelihoods.
Step 10: Select the best solution in the final harmony memory as the optimal solution for the risk identified in the industrial IoT applications.

The first analysis is for the actual risk counts detected and the rule estimation, as given in Figure 6.

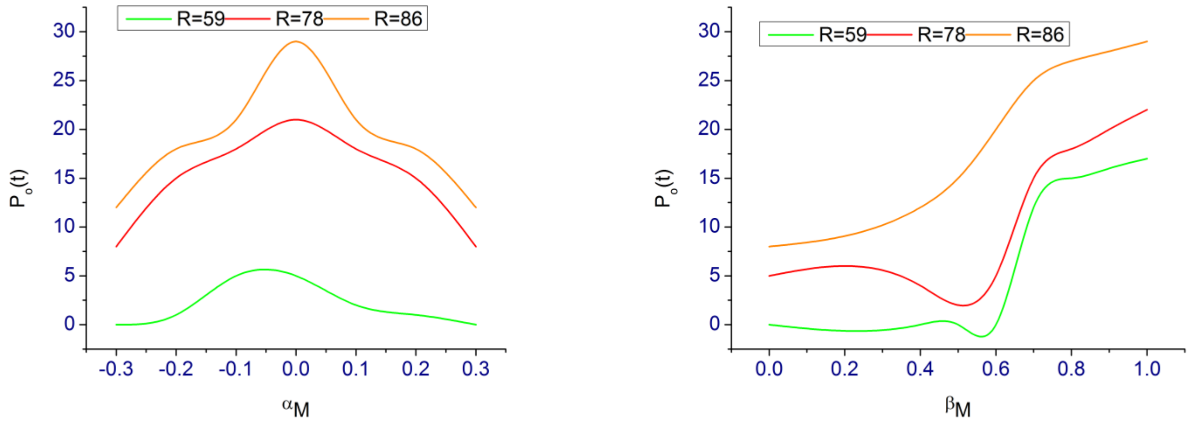


(**a**) (**b**)

Figure 6. Count and Span Analysis. (**a**) Count. (**b**) Span Analysis.

Based on the provided data, the $R_{MSA} = 59, 78, 86$ is varied for estimating the count and span. As the R_{MSA} increases, Th_{rat} and $P_{Th_{rat}}$ varies for which the detection is performed. Therefore the $\exists$ is performed for maximum halts under varying t. In the HS process the $P_o(t)$ for the varying α_M and β_M is analyzed in Figure 7.

The analysis is performed for $P_o(t)$ under the varying α_M (Range: -0.4 to +0.3) and F_M (Range: -0.4 to 1) in Figure 7. This is determined using the $fuzzy_{opt_{i,j}}$ wherein (i, j) classifications are performed using Hmp_i. In the varying processes (level 1 and level 2), if $Th_{rat} > \theta_i^{Th_{rat}}$ then $F(X)$ is retained and therefore the $P_o(t)$ and $I_H(t)$ as in Equation (7) is obtained. It satisfies the maximum conditions in the HAS due to which risks are thwarted (Figure 7). In the final analyses, the High $P_o(t)$ and $Obj_p(t)$ are analyzed for different risk factors, as presented in Table 2.



(**a**) (**b**)

Figure 7. $P_o(t)$ Analyses. (**a**) $P_o(t)$ for the varying α_M. (**b**) $P_o(t)$ for the varying β_M.

Table 2. $P_o(t)$ and $Obj_F(t)$ Analyses.

Operation	Device	Risk Factor	M^o[.]	High$P_o(t)$	$Obj_F(t)^{-1}$	$Obj_F(t)$
1	C	Long term attack decreases	3		No	
2	IO	Attempt to maintain previous sensor value	8	✓	No	
3	C	A long-term attack that decreases the SP value	98		Yes	No
4	MS	Decreases or increases the CV value. Restore normal	5	✓	No	
5	IO	Decreases or increases the CV restore as a form of the trapezoidal profile while hiding SP changes of HMI	45		No	
6	MS	Decreases or increases the CV restore as a form of the trapezoidal profile while hiding SP changes of HMI	61		No	
7	MS	A long-term attack that decreases the SP value	78	✓	No	
8	IO	Attempt to maintain previous sensor value	78	✓	Yes	No
9	MS	A short-term attack that decreases the CV value	65		No	No
10	C	A long-term attack that decreases the SP value	28	✓	No	
11	IO	Attempt to maintain previous sensor value	94		Yes	No
12	MS	A long-term attack that decreases the SP value	103	✓	Yes	
13	C	Attempt to maintain previous sensor value	82		No	No
14	IO	A short-term attack that decreases the CV value	8		No	
15	IO	Attempt to maintain previous sensor value	29	✓	No	No
16	C	A long-term attack that decreases the SP value	64		No	
17	MS	Attempt to maintain previous sensor value	98	✓	Yes	No
18	IO	A short-term attack that decreases the CV value	78		No	
19	MS		91		Yes	No
20	C		89	✓	Yes	No

Note: ✓ means it has **High $P_o(t)$**.

The risk is focused on Io devices or controllers (c) or the monitoring systems (MS). Based on the risk factor, M^o is initialized that is handled under M and $N_i \forall t$. If the S_{po} is high then R_{oc} is less, however, the variations are less for different operation levels. Therefore $objp(t)^{-1}$ maximum is achieved as high compared to $Objp(t)$. At some time instance such as $Th_{rat} > \theta_i^{Th_{rat}}$ the n $Objp(t)^{-1}$ is also high. This indicates fewer outages for the varying processes. Based on the M, the interrupt analyses are presented in Figure 8.

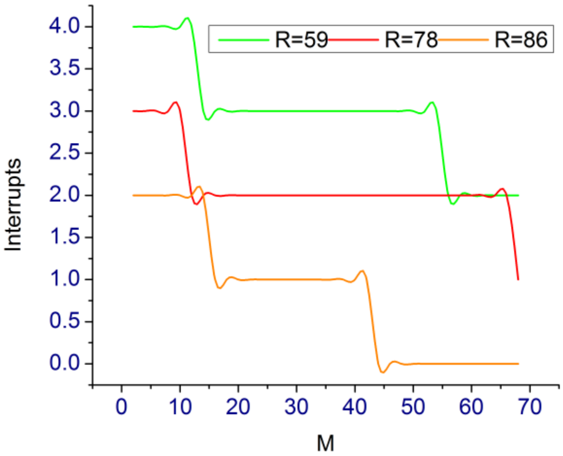


Figure 8. Interrupt Analysis.

The interrupt reduces as the M increases; out of 114, 68 are mimic classifying α_M and β_M. This classification provides Hmp_i for further interval analysis such that $F(X)_{New}$ identifies the risks (Figure 8). According to the discussions, the steps for conducting the T-test is given as follows.

t-Test Analysis

Initially, industrial processes are analyzed with the help of the industrial wireless communication process. The cyber risk related data is collected with the help of the communication process. During the analysis, the fuzzy harmonic approach is utilized to evaluate the industrial performance to detect the risk factor. The collected risk related information is prepared and analyzed using statistical methods. Define Hypotheses: Define the null hypothesis and alternative hypothesis. The null hypothesis is that there is no significant difference in the effectiveness of the fuzzy harmonic approach and existing risk detection methods. The alternative hypothesis is that the fuzzy harmonic approach is significantly better than existing risk detection methods.

Calculate T-value: Calculate the T-value using the following formula:

$$\text{T} = (\text{X1} - \text{X2})/(\text{sqrt}((\text{S1}^2/\text{n1}) + (\text{S2}^2/\text{n2}))) \tag{17}$$

In Equation (16) X1 and X2 are the means of the two groups being compared, S1 and S2 are the standard deviations of the two groups, and n1 and n2 are the sample sizes of the two groups. Then degrees of freedom have been determined (df) using the following formula:

$$\text{df} = \text{n1} + \text{n2} - 2 \tag{18}$$

Determine the critical value of T using a T-table or statistical software. This is based on the desired significance level (usually 0.05 or 0.01) and the degrees of freedom. Compare T-value and Critical Value: Compare the calculated T-value with the critical value. If the calculated T-value is greater than the critical value, then the null hypothesis can be rejected, and the alternative hypothesis is accepted. This means that the fuzzy harmonic approach is significantly better than existing risk detection methods.

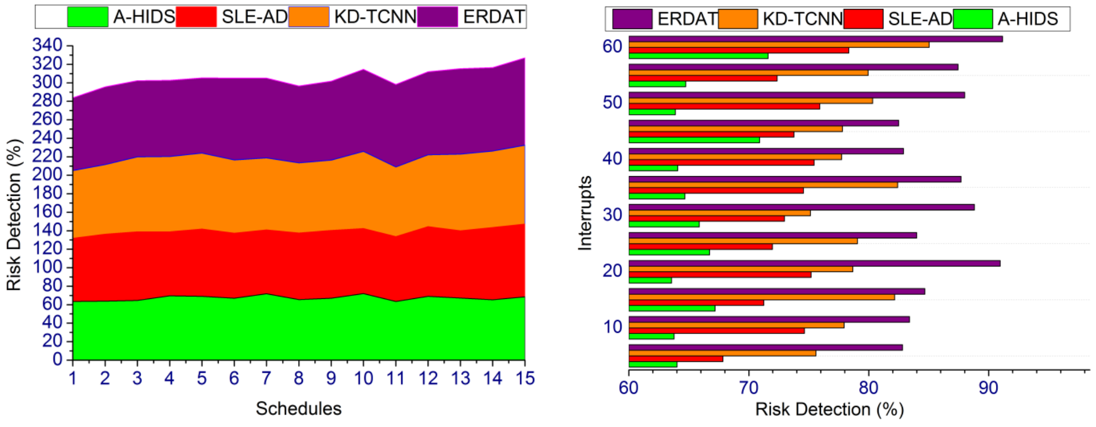
Interpret Results: Interpret the results and draw conclusions about the effectiveness of the fuzzy harmonic approach for cyber risk detection in industrial wireless communication.

4. Discussion

The discussion is presented using the metrics risk detection, outcome interrupt, halted schedules, max. interrupt span and detection time. The variants are schedules (up to 15) and interrupt (up to 60). The comparative methods are A-HIDS [23], SLE-AD [17], and KD-TCNN [18]. Compared to these methods, the introduced approach uses the fuzzy set and harmony optimization algorithm function which improves the overall risk identification and detection rate. In addition, fuzzy set and optimization problem solves the optimization problem and minimizes the detection rate.

4.1. Risk Detection

This proposed technique achieves high cyber risk detection in different wireless communication-based technologies and relies on production outcome and risk for improving profitable outcomes (Refer to Figure 9). The prediction plan for internal and external operations is made as security threats are high in industry 4.0; the cyber risk is mitigated due to the wireless nature and remote operability. The overlapping sources and cyber security mitigation is identified in processing units through a fuzzy harmony search algorithm. Based on the cyber threat mitigation in different technologies analyzed with the already stored industrial data, this assessment is performed for better decisions in the particular communication processing. Therefore, the identification of security threats in processing units of industry 4.0 improves the profitable outcome for preventing risks based on accumulated data, and hence fuzzy optimal operation is achieved. The varying threshold value is identified for further prediction plans for sequential production achieved. In the proposed technique, the harmony search algorithm mimics the adversary impacts based on production outcome and process interruption identification maximizing cyber risk detection.



(a) (b)

Figure 9. Risk Detection. (**a**) Risk Detection. (**b**) Interupts.

4.2. Outcome Interrupt

The classification of production outcome and process interruption/halt is performed for all the secure industrial operations and planned outcomes are observed from industry 4.0 for improving communication security. This proposed technique is aided for satisfying maximum interrupt span with fewer risk mitigation admits using the fuzzy operation. With the use of fuzzy harmony search and ERDAT, a high objective function is achieved to detect and mitigate cyber risk detection. Using this mimicking operation, the fuzzy threshold varies, each source mitigation instance is identified through fuzzy harmony search. If any risk occurrence is identified, a new communication network is processed for identifying adversary impact. In this article, the outcome interrupt is less for either production outcome or risk interrupts. In this manuscript, this process classification helps the wireless communication industry 4.0 to reduce data analysis time and detection time for increasing cyber risk mitigation and profitable outcome in the industries. For high data processing and profitable outcome, fuzzy optimization is performed to identify the risk in communication networks and prevent its impact. The fuzzy threshold occurred production is discontinued; the new source is generated for processing in which the mimic operation achieves less outcome interrupts, as represented in Figure 10.

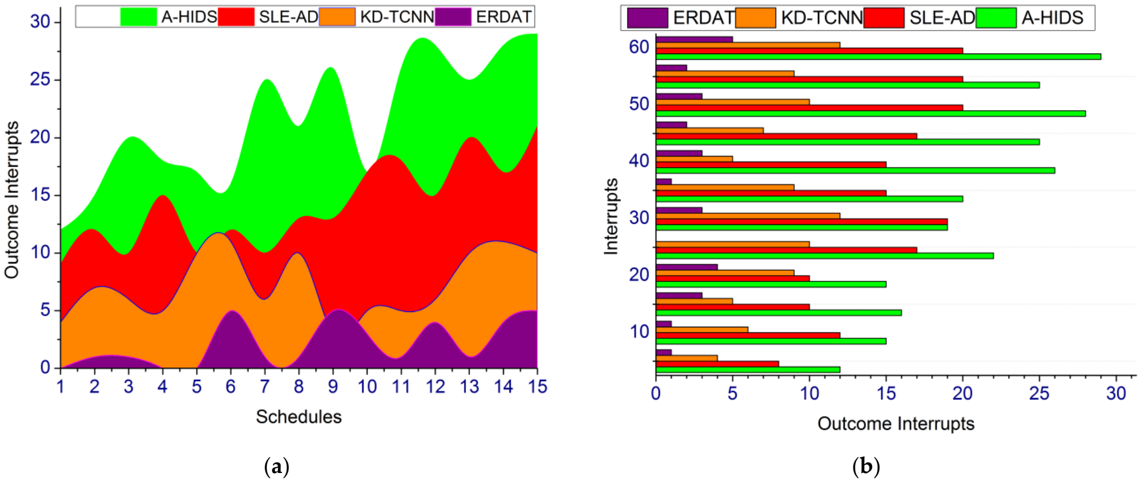


Figure 10. Outcome Interrupt. (**a**) Outcome Interupts. (**b**) Interupts.

4.3. Halted Schedules

In Figure 11, the production outcome and process interruption/halting changes for each communication network is computed to prevent further adversary impacts. Fuzzy optimization is performed based on mimicking operations and helps identify the processing interruption and halt occurrence in industries. If any disconnection takes place, the harmony search algorithm generates a new source for products that enhance the accuracy and convergence rate of data processing and production monitoring observed from the industry. In this process, the overlapping takes place and the search performs mimics operations for high objective functions identified through FHS. Improving communication security using cyber risk detection is observed from industry 4.0 for updating the previous security with current cyber threat mitigations. The fuzzy optimization used for achieving maximum or minimum objective output based on admit of the above factors is computed continuously. In this process, classification is performed to prevent risks with high security in industry 4.0.

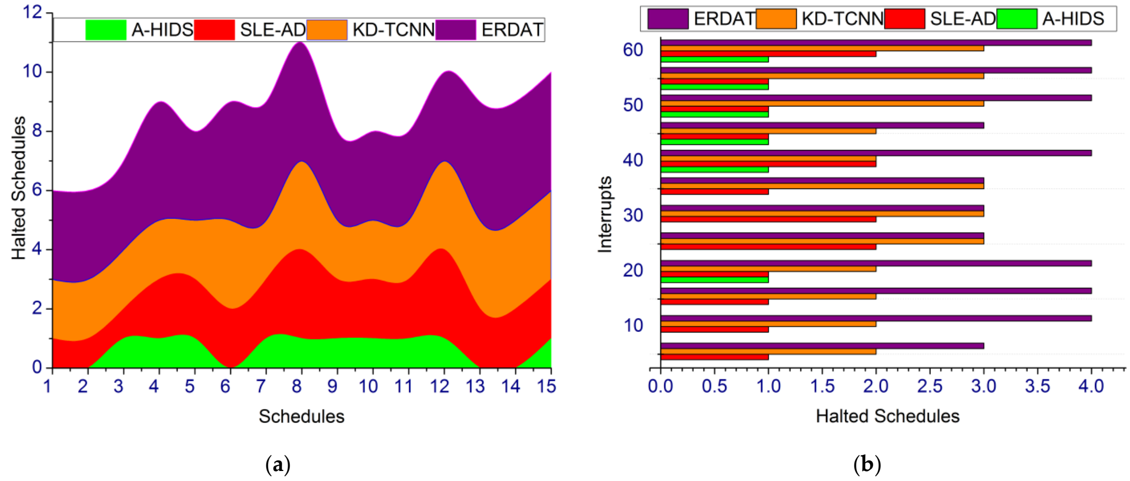
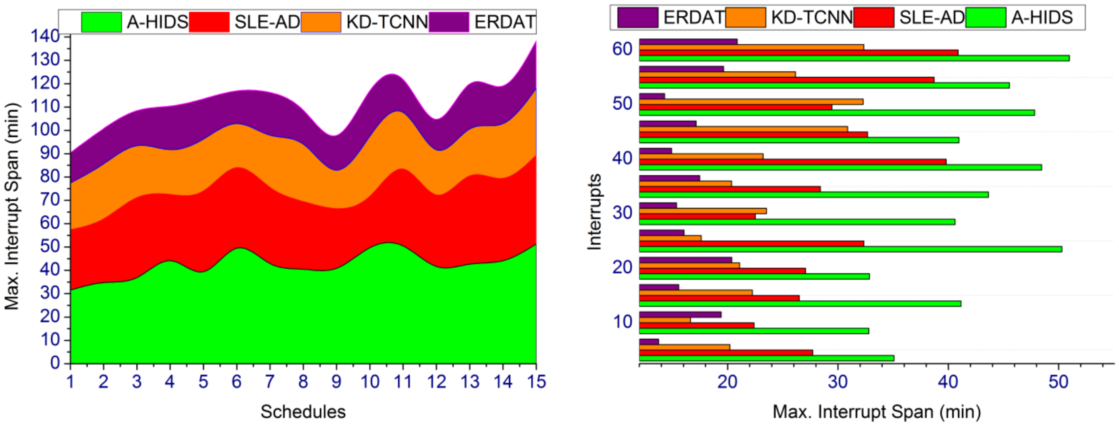


Figure 11. Halted Schedules. (**a**) Halted Schedules. (**b**) Iterupts.

4.4. Maximum Interrupt Span

The maximum interrupt span across different communication technologies is identified for ease of computing production outcome and risk routinely for improving communication security as illustrated in Figure 12. In this proposed cyber risk detection method, satisfying less maximum interrupt span in production outcome processing is identified using mediate acceptable range through mimicking operation at different communication networks. For instance, production outcome and risk occurrence are addressed to prevent fuzzy threshold, which mimics the adversary impact using production factors such as process interruption/halt and production outcome. Cyber risk mitigation is due to identifying adversary impacts and maximum interrupt span in the production process, whereas the optimal decision is made for the admitted plan is preceded using the above Equations (6)–(11). In this proposed technique, the mimicking operation is computed to enhance the fuzzy harmony search algorithm. Instead, the accumulated data processing for profitable outcomes in industry 4.0 prevents risks through the fuzzy operation. Based on the prediction plan, the maximum and minimum objective function is achieved.

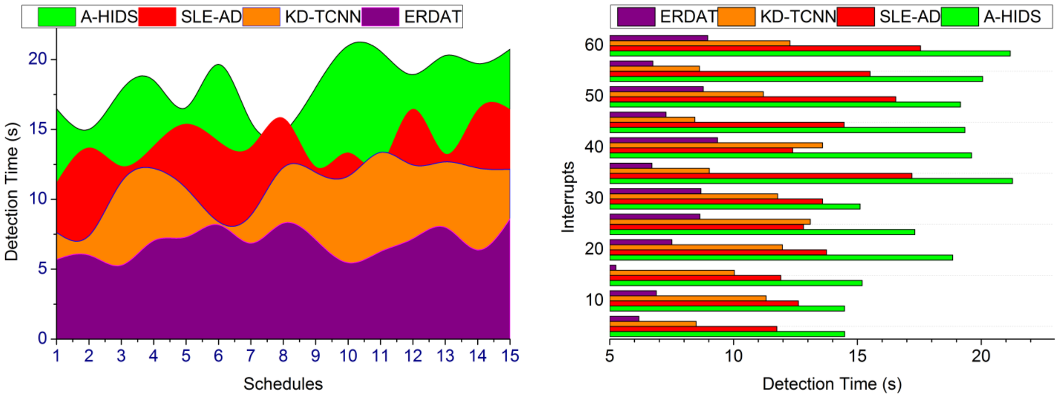


(**a**) (**b**)

Figure 12. Max. Interrupt Span. (**a**) Max. Interrupt Span. (**b**) Interupts.

4.5. Detection Time

In Figure 13, the fuzzy harmony search extracts data observed from the industry and then processes it to gain better decisions to identify security threats in communication networks. The FHS can be useful in adjusting the mimicking crossing/failing rate behind the fuzzy threshold for identifying risk and then disconnecting the risk occurred processing in that source, using the algorithm to find the optimal outcome. The data processing and production monitoring are the two main factors performed through fuzzy operation for improving communication security and risk detection, as it does not require interruption/halting, the source is detected. The fuzzy harmony search algorithm is used for performing a mimicking operation based on the condition $R_{OC}(Obj_F(t)) \in [-\infty, \infty]$ and $\alpha_M \in [0, \infty]$ or $\alpha_M \notin [0, \infty]$ for a better decision. The aforementioned two factors are processed using fuzzy optimization for identifying threshold and risk occurrence between the risk and scheduled production outcome. If the accumulated data processing is analyzed in this technique, high production outcome is achieved. The successful profitable outcome is satisfied using the fuzzy harmony search, for which the proposed technique satisfies less detection time. The comparative analysis is summarized in Tables 3 and 4 for the varying schedules and Interrupts.



(**a**) (**b**)

Figure 13. Detection Time. (**a**) Detection Time. (**b**) Interupts.

Table 3. Comparative Analysis of Schedules.

Metrics	A-HIDS	SLE-AD	KD-TCNN	ERDAT
Risk Detection (%)	68.4	78.74	85.38	94.527
Outcome Interrupts	29	21	10	5
Halted Schedules	4	3	2	1
Max. Interrupt Span (min)	51.27	38.05	28.73	20.264
Detection Time (s)	20.75	16.42	12.15	8.611

Table 4. Comparative Analysis of Interrupts.

Metrics	A-HIDS	SLE-AD	KD-TCNN	ERDAT
Risk Detection (%)	71.61	78.34	85.03	91.148
Outcome Interrupts	29	20	12	5
Halted Schedules	14	3	2	1
Max. Interrupt Span (min)	50.97	40.89	32.34	20.863
Detection Time (s)	21.17	17.55	12.28	8.954

The proposed technique achieves 8.52% high-risk detection, 12.5% fewer outcome interrupts, 8.3% fewer halted schedules, 8.08% less interrupt span, and 7.94% less detection time.

The proposed technique achieves 8.55% high-risk detection, 12.59% fewer outcome interrupts, 8.3% fewer halted schedules 7.69% less interrupt span, and 7.8% less detection time.

5. Conclusions

This article introduced an explicit risk detection and assessment technique for handling adversary impacts in industrial communication networks. An Explicit Risk Detection and Assessment Method (ERDAT) reduces cyber threats in the manufacturing process, to improve communication security. The method employs a fuzzy harmony search algorithm to detect the threat and mitigate its effects. The harmony search algorithm simulates the effect of an opponent by manipulating variables related to production, such as the initiation, continuation, and termination of a process, and the results of that production. The search procedure uses an operation that is similar to the output of the approved plan to maximize the value of the objective function. The factors used in conjunction with fuzzy logic to determine a cyber risk represent a financial or non-financial hazard. An acceptable range is calculated by dividing the number of times the risk and planned production outcomes are similar from least to greatest to get the fuzzy threshold. Risks associated with the imitating crossing or falling beneath the threshold for the interruption/halting of production are therefore recognized and their source determined. For security reasons, the detecting communication source has been cut off from the manufacturing process. This helps to achieve 8.52% high-risk detection, 12.5% fewer outcome interrupts, 8.3% fewer halted schedules, 8.08% less interrupt span, and 7.94% less detection time. Future research and development have focused on side-channel research utilizing machine learning approaches to identify minimal attacks, as the attacker may have exploited a weakness unknown to security organizations. Side-channel analysis will help identify and prevent cyber–physical assaults by finding nil vulnerabilities early in the attack lifecycle.

Author Contributions: Z.D.: Conceptualization, Methodology, Software; F.S.: Data curation, Writing—Original draft preparation. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mohd, J.; Abid, H.; Ravi, P.S.; Rajiv, S. An integrated outlook of Cyber–physical systems for industry 4.0: Topical practices, architecture, and applications. *Green Technol. Sustain.* **2023**, *1*, 100001.
2. Suvarna, M.; Yap, K.S.; Yang, W.; Li, J.; Ng, Y.T.; Wang, X. Cyber–physical production systems for data-driven, decentralized, and secure manufacturing—A perspective. *Engineering* **2021**, *7*, 1212–1223. [CrossRef]
3. Wang, B.; Zheng, P.; Yin, Y.; Shih, A.; Wang, L. Toward human-centric smart manufacturing: A human-cyber-physical systems (HCPS) perspective. *J. Manuf. Syst.* **2022**, *63*, 471–490. [CrossRef]
4. Saniuk, S.; Saniuk, A.; Cagáňová, D. Cyber industry networks as an environment of the industry 4.0 implementation. *Wirel. Netw.* **2021**, *27*, 1649–1655. [CrossRef]
5. Berger, S.; Häckel, B.; Häfner, L. Organizing self-organizing systems: A terminology, taxonomy, and reference model for entities in cyber-physical production systems. *Inf. Syst. Front.* **2021**, *23*, 391–414. [CrossRef]
6. Wanasinghe, T.R.; Gosine, R.G.; James, L.A.; Mann, G.K.; De Silva, O.; Warrian, P.J. The internet of things in the oil and gas industry: A systematic review. *IEEE Internet Things J.* **2020**, *7*, 8654–8673. [CrossRef]
7. Ling, S.; Li, M.; Guo, D.; Rong, Y.; Huang, G.Q. Assembly workstation 4.0: Concept, framework and research perspectives for assembly systems implementation in the industry 4.0 era. *IFAC-Pap.* **2022**, *55*, 420–426. [CrossRef]
8. Cardin, O.; Trentesaux, D. Design and use of human operator digital twins in industrial cyber-physical systems: Ethical implications. *IFAC-Pap.* **2022**, *55*, 360–365. [CrossRef]
9. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–4.
10. Radanliev, P.; De Roure, D.; Nicolescu, R.; Huth, M.; Santos, O. Digital twins: Artificial intelligence and the IoT cyber-physical systems in Industry 4.0. *Int. J. Intell. Robot. Appl.* **2022**, *6*, 171–185. [CrossRef]
11. Rashid, S.Z.U.; Haq, A.; Hasan, S.T.; Furhad, M.H.; Ahmed, M.; Ullah, A.B. Faking smart industry: Exploring cyber-threat landscape deploying cloud-based honeypot. *Wirel. Netw.* **2022**, 1–15. [CrossRef]
12. Kaur, A.; Bhatia, M. Stochastic game network based model for disaster management in smart industry. *J. Ambient Intell. Humaniz. Comput.* **2021**, 1–19. [CrossRef]
13. Dafflon, B.; Moalla, N.; Ouzrout, Y. The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: A literature review. *Int. J. Adv. Manuf. Technol.* **2021**, *113*, 2395–2412. [CrossRef]
14. Oztemel, E.; Gursev, S. Literature review of Industry 4.0 and related technologies. *J. Intell. Manuf.* **2020**, *31*, 127–182. [CrossRef]
15. Schubert, V.; Kuehner, S.; Krauss, T.; Trat, M.; Bender, J. Towards a B2B integration framework for smart services in Industry 4.0. *Procedia Comput. Sci.* **2023**, *217*, 1649–1659. [CrossRef]
16. Pearce, H.; Pinisetty, S.; Roop, P.S.; Kuo, M.M.; Ukil, A. Smart I/O modules for mitigating cyber-physical attacks on industrial control systems. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4659–4669. [CrossRef]

17. Ahmadi-Assalemi, G.; Al-Khateeb, H.; Epiphaniou, G.; Aggoun, A. Super learner ensemble for anomaly detection and cyber-risk quantification in industrial control systems. *IEEE Internet Things J.* **2022**, *9*, 13279–13297. [CrossRef]
18. Wang, Z.; Li, Z.; He, D.; Chan, S. A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning. *Expert Syst. Appl.* **2022**, *206*, 117671. [CrossRef]
19. Rosado, D.G.; Santos-Olmo, A.; Sánchez, L.E.; Serrano, M.A.; Blanco, C.; Mouratidis, H.; Fernández-Medina, E. Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Comput. Ind.* **2022**, *142*, 103715. [CrossRef]
20. Traganos, K.; Grefen, P.; Vanderfeesten, I.; Erasmus, J.; Boultadakis, G.; Bouklis, P. The HORSE framework: A reference architecture for cyber-physical systems in hybrid smart manufacturing. *J. Manuf. Syst.* **2021**, *61*, 461–494. [CrossRef]
21. Farrugia, D.; Zerafa, C.; Cini, T.; Kuasney, B.; Livori, K. A real-time prescriptive solution for explainable cyber-fraud detection within the iGaming industry. *SN Comput. Sci.* **2021**, *2*, 215. [CrossRef]
22. Leong, Y.Y.; Chen, Y.C. Cyber risk cost and management in IoT devices-linked health insurance. *Geneva Pap. Risk Insur.-Issues Pract.* **2020**, *45*, 737–759. [CrossRef]
23. Pinto, R.; Gonçalves, G.; Delsing, J.; Tovar, E. Enabling data-driven anomaly detection by design in cyber-physical production systems. *Cybersecurity* **2022**, *5*, 9. [CrossRef]
24. Zängerle, D.; Schiereck, D. Modelling and predicting enterprise-level cyber risks in the context of sparse data availability. *Geneva Pap. Risk Insur.-Issues Pract.* **2022**, 1–29. [CrossRef]
25. Pantano, M.; Regulin, D.; Lutz, B.; Lee, D. A human-cyber-physical system approach to lean automation using an industrie 4.0 reference architecture. *Procedia Manuf.* **2020**, *51*, 1082–1090. [CrossRef]
26. Latino, M.E.; Menegoli, M. Cybersecurity in the food and beverage industry: A reference framework. *Comput. Ind.* **2022**, *141*, 103702. [CrossRef]
27. Miehle, D.; Häckel, B.; Pfosser, S.; Übelhör, J. Modeling IT availability risks in smart factories: A stochastic Petri nets approach. *Bus. Inf. Syst. Eng.* **2020**, *62*, 323–345. [CrossRef]
28. Shahin, M.; Chen, F.F.; Bouzary, H.; Hosseinzadeh, A.; Rashidifar, R. A novel fully convolutional neural network approach for detection and classification of attacks on industrial IoT devices in smart manufacturing systems. *Int. J. Adv. Manuf. Technol.* **2022**, 1–13. [CrossRef]
29. Jbair, M.; Ahmad, B.; Maple, C.; Harrison, R. Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Comput. Ind.* **2022**, *137*, 103611. [CrossRef]
30. Available online: https://www.kaggle.com/datasets/icsdataset/hai-security-dataset (accessed on 8 December 2022).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.