International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I4P137

Volume 72 Issue 4, 378-388, April 2024
© 2024 Seventh Sense Research Group®

Original Article

Trustworthy CPS: An Enhanced Dynamic Clustered Architecture to Secure CPS with Digital Signature and Route Optimization

Sandeep Singh Bindra[1], Alankrita Aggarwal[2]

[1]*Department of Computer Science & Engineering, Chandigarh University, Punjab, India.*
[2]*Department of Computer Science & Engineering, AIT, Chandigarh University, Punjab, India.*

[1]*Corresponding Author : sandeep.bindra@gmail.com*

Received: 23 January 2024 Revised: 03 April 2024 Accepted: 11 April 2024 Published: 24 April 2024

Abstract *- Robust and adaptable security architectures are becoming essential in the face of growing cyberattacks and security breaches in Cyber-Physical Systems (CPS). To overcome these obstacles, this work has created a unique secure CPS architecture called trustworthy CPS. The method uses Fuzzy Adaptive Resonance Theory (Fuzzy ART) to dynamically cluster network nodes called security zones, enabling flexible adaptability to changing situations. A trust and energy-based selection method selects a designated security chief for each security zone, which is again dynamic. Further, to ensure the integrity and validity of the nodes, each security chief in the zone uses SHA-256 to provide cryptographic signatures. To promote inter-zone security and cooperation, security chiefs participate in communication protocols, confirm nodes as they move across clusters, and protect the system from attacks. The proposed system also adds a route optimization technique during communication. Krill Herd Optimization (KHO) and Spider Monkey Optimization (SMO) are integrated to improve route selection effectiveness and provide flexibility in real-time circumstances. This optimization helps increase the CPS network's overall resilience while reducing delays. In this research, the resilience of the architecture under such adversarial situations is explored, with a particular focus on Distributed Denial of Service (DDoS) attacks. Further, the proposed architecture is evaluated using NS-2 simulators based on distinct network scenarios, where its effective performance provides a better scope for this architecture in real-time CPS systems.*

Keywords *- CPS, Security, Clustering, Signature, Optimization.*

1. Introduction

Cyber-Physical Systems (CPS), owing to their integration with the computational and physical realms, Cyber-Physical Systems (CPS) gain popularity in this rapid technological development [1]. CPS are networked systems where physical processes, communication networks, and computer algorithms combine to create a synergy that offers previously unheard-of capabilities in various fields, from smart cities and autonomous cars to industrial automation and healthcare [2]. The need to protect CPS from potential threats and maintain security is becoming increasingly crucial as they spread [3].

The fundamental frameworks that coordinate the complex waltz between digital and physical components are known as CPS architectures [4]. To ensure effective and dependable operation, these designs must seamlessly integrate control systems, communication networks, and real-time data processing [5]. Typical architectural models are hierarchical, which arranges components into levels according to functionality and control.

Decentralized, which distributes control across several components, and centralized, which places all of the system's management under the control of a single controller [6]. In this ever-changing environment, efficient coordination of device interactions is just as necessary as device connection. CPS designs' security, flexibility, and efficiency are essential for maximizing these systems' potential and minimizing associated risks.

The resilience, robustness, and dependability of these interconnected networks can be guaranteed by strictly meeting the security requirements in CPS. The increasing integration of physical processes and computational intelligence in several areas necessitates protecting CPS against various risks [7]. Confidentiality is an essential security criterion that protects sensitive information from unwanted access. Securing confidential data or personal records in industries including healthcare, vital infrastructure, and industrial automation is essential. Another critical factor is integrity, which guarantees that data and system components do not change. Data integrity breaches may result in poor decisions, putting lives in danger or interfering with essential operations. Equally important is availability, or the constant and dependable operation of CPS. Because cyberattacks can cause downtime or disruption in services, the constant availability of CPS is a fundamental security need. To confirm the legitimacy of entities operating inside the CPS network and to guarantee that only authorized entities can access certain resources or carry out specific operations, authentication and authorization techniques are essential [8]. These security specifications provide the framework for constructing reliable and robust CPS ecosystems.

Furthermore, with the threat landscape constantly changing, it is imperative to be resilient to assaults. CPS must demonstrate that it can endure different cyber threats, such as malware, DDoS assaults, and sophisticated persistent threats [9]. Applications using sensitive or personal data in CPS are critical regarding privacy. In applications like smart cities or healthcare systems, trust must be built and maintained with strong privacy safeguards [10].

One essential component of efficient security in CPS is adaptability. Due to its dynamic nature, security measures must be flexible enough to react to new threats and shifting operating circumstances. Long-term CPS security survival depends on a proactive and flexible approach [11]. To maintain these linked systems' overall integrity and performance, security requirements for CPS must be broad, dynamic, and smoothly incorporated into the system's architecture as it expands into new areas.

1.1. Motivation

The essential need to protect CPS from growing cyber threats spurs this research. The interconnectedness of CPS makes them vulnerable, especially as it becomes increasingly integrated into other industries. Critical infrastructure has recently been the target of cyberattacks, highlighting how essential it is to provide adaptable security solutions suited to the changing needs of CPS situations.

The goal is to close the gap between security methodologies and provide a complete solution considering CPS's particular difficulties. Adaptive route optimization, secure communication, and dynamic clustering are the principal foci of the study, which attempts to proactively defend CPS against new threats, including Distributed Denial of Service (DDoS) assaults. The objective is to provide communities and companies that depend on CPS with a robust security architecture, guaranteeing the safe assimilation of these technologies into our globalized society.

1.2. Problem Statement

Security is the preeminent requirement of CPS, like other network systems. The commonly used security approaches such as cryptography secure the information by encrypting data, machine learning to detect malicious nodes, trust computation, thresholding, etc. [12] enhances security in different ways but fails when multiple attacker nodes attack the network as DDoS does.

Moreover, due to the network's dynamic nature, most security approaches are unsuccessful in controlling intruders [13]. So, the main focus of this work is to design and develop a multi-level security approach that can also adapt to dynamic network changes and provide adequate security to the network, specifically focusing on DDoS attacks where multiple attacker nodes attack the node simultaneously.

1.3. Contribution of the Proposed Work

This proposed work mainly contributes to security enhancement in CPS and protects it from attacks. Moreover, the other technical aids of this work are discussed as follows:

- The first main contribution of the work is the novel trustworthy architecture for CPS, where fuzzy ART-based dynamic clustering is proposed to divide the network into different clusters/ zones called security zones. Each security zone has its chief, called security chief, which is dynamically selected based on trust and energy factors.
- The paper's second main contribution is the security chief's verification of nodes whenever a node moves from one zone to another. This SHA-256-based digital signature verification uses a highly secured hash function.
- The third main contribution is the optimization-based route selection for communication, where two different optimization algorithms, KHO and SMO, are integrated.
- The other contributions are simulation using NS-2, distinct simulation scenarios, the presence of DDoS attacker nodes, and performance evaluation.

The next section of the paper stated the recent related literature in Section 2, proposed trustworthy architecture and hybrid route optimization in the proposed architecture in Section 3. Further, simulation and experimentation are discussed in Section 4, and finally, section 5 concludes the work and provides the future scope.

2. Related Work

This section of the paper discusses the recent security architecture and approaches developed for CPS security based on different parameters and factors, such as routing, communication, encryption, authorization, etc., to recognize the current security approaches in CPS and the necessities of this proposed system.

A minimally presumptive approach for security vulnerability analysis in CPS was provided by Chandratre et al. [14] to accommodate a variety of CPS architectures. Their methodology does not require a specialized understanding of system dynamics or algorithms because it includes state observers, feedback control loops, and anomaly detection methods. With the help of security criteria stated in Signal Temporal Logic (STL), the authors formulate a search-based test generation problem in the CPS security challenge. The framework's practical application and efficacy in real-world CPS components are demonstrated by simulation experiments, which confirm the presented security criteria, which are categorized into detectability and effectiveness.

Ju et al. [15] integrated millimeter-wave and physical layer security methods to address information security issues in ad hoc-based CPS. Considering the decentralized and resilient character of ad hoc CPS systems, the study presents a transmission technique that utilizes generated noise to improve confidentiality.

AN is deliberately used to produce interference, making it impossible to stop eavesdropping efforts. The study examines the trade-off between security and dependability while considering network user expectations. Theoretical analysis is used to construct analytical formulas for connection and secrecy outage probability, which show that the application of AN significantly improves its performance. The results also show a trade-off between security and dependability and that optimal outage performance is achievable for a given total transmit power.

Sheikh et al. [16] suggested an intelligent attack detection approach using machine learning (ML) algorithms to solve CPS's security flaws. The authors developed a defense method based on adversarial learning for the ToN_IoT Network dataset. This approach uses generative adversarial network models such as random forest (RF), long short-term memory (LSTM), and artificial neural network (ANN). The research sought to improve CPS security and contribute to the changing cybersecurity scene by utilizing adversarial and intelligent learning approaches. The challenging task of categorizing cybersecurity vulnerabilities in distributed CPS was tackled by Liu et al. [17]. The article addressed a multi-class classification challenge called a multi-node data-censoring situation. It was due to the inability of any data center or node to exchange its data, which left nodes with only a subset of many classes and incomplete local data. This multi-node, multi-class ensemble technique was a unique solution presented by the authors. This method entailed building a global multi-class classifier without exchanging raw data by obtaining data densities and estimated parameters from each local node. The efficacy of this strategy was confirmed by numerical studies, which showed that in scenarios with multi-node data censoring, it outperforms the full-data approach.

Ma et al. [18] concentrated on dealing with transient concealed assaults (TCAs). The primary objective of this work was to reduce this degradation without sacrificing detection rates. The authors used an event-triggered and recursive watermarking detection approach to classify trigger modes into forced, high-likelihood, and low-probability categories. The benefits of the proposed algorithms were illustrated using different tests on the dSpace platform.

To improve the identification of pertinent features from preprocessed data, Alohali et al. [19] presented an Enhanced Chicken Swarm Optimization (ECSO) with self-learning capability. Cloud-based ensemble classifiers were then trained using the chosen features. The suggested ECSO-based ensemble classifier's efficacy was experimentally evaluated against the NSL-KDD dataset, exhibiting satisfactory performance by several statistical metrics.

Sivamohan et al. [20] proposed a TEA-EKHO-IDS that combines enhanced krill herd optimization (EKHO) with trustworthy explainable artificial intelligence (XAI) to identify breaches effectively. The technique uses XAI-EKHO to choose features, improving its capacity for worldwide searching and quickening its convergence time. The integration of XAI, bi-directional LSTM, and Bayesian optimization optimizes the performance of intrusion detection. The suggested method showed a 98.96% success rate in correctly detecting and categorizing intrusions, presenting a viable option for improving cybersecurity in industrial CPS and giving insightful information about the decision-making process.

Lilhore et al. [21] developed an Effective Hybrid Machine Learning Model (EHML) in response to the growing frequency of cyberattacks. This approach uses an unsupervised learning-based data reduction method and supervised learning for crime detection. An enhanced decision tree method and the enhanced local outlier factor technique were used to pick critical features, which increased performance and accuracy. This proposed approach performed better than existing ML techniques and was validated with a Kaggle online cybercrime dataset. It achieved a 10% improvement over current ML approaches with 95.02% accuracy, 95.01% precision, 94.89% recall, and a 95.89% F1 score.

Wu et al. [22] presented a coprime factorization-based defense plan for CPSs to counter security risks, including deception and damaging cyber-physical assaults. The plan concentrated on preventing and detecting attacks, using fault diagnostic residual signals for secure transfer while keeping critical system information hidden. A filter module was included to secure reference signals and the state of the system's functioning. The objectives of this strategy were to lessen information leakage, prevent the creation of stealthy assaults that need in-depth system expertise, and make it possible to identify non-stealthy attacks. Experiments conducted on a linear system and random parameters showed that the suggested strategy works well.

Simon Thomas and Subramanian [23] discussed how several cyberattacks might compromise CPSs in smart grids. Their main objective is to identify and avert cyberattacks that occur when data is sent from the networked control center to the plant. A combination of deep feedforward neural networks and evolutionary algorithms is proposed to improve security in the CPS environment of smart grids. The methodology is assessed using the IEEE 39 bus system as a benchmark, exhibiting enhanced precision, performance indicators, and a reduced number of false positives. This study advances methods for detecting attacks in the cyberspace of smart grid systems.

To overcome the connection issues posed by Industry 4.0 for CPS, Oliveira et al. [24] used Discrete Event Systems (DES) to create a defense against actuator assaults. Controllable events were selectively encrypted before transmission using event-based symmetric cryptography, deceiving attackers about the supervisor's control operations—this preserved system integrity by averting expected effects on the plant. When the method was used in a case study in literature, it successfully detected assaults without inflicting any harm. Potential security holes exist in the studies under discussion: a lack of real-world solid validation, scalability problems that impede adaptation to more extensive systems, and doubts about adaptability to new cybersecurity threats. Resource efficiency issues arise, especially regarding computational load and the viability of real-world applications.

Furthermore, the suggested solutions' overall security efficacy may be jeopardized by a lack of multidisciplinary cooperation, well-defined and consistent security metrics, and an inadequate consideration of human aspects. These gaps must be filled to guarantee thorough and durable security measures in CPS.

3. Materials & Methods

This work proposes a secure architecture for CPS and attains successful data transmission without interference from attacker nodes. So, in this, the network is divided into clusters first. Then, each cluster, called a security zone, is responsible for evaluating the genuineness of nodes present in the zone and new nodes entering into the zones. Furthermore, route optimization is also included to improve the effectiveness of the CPS system. The detailed process and methods used are discussed as follows:

3.1. Security Zone Formation

The first stage of the research is initializing nodes that represent prospective clusters with corresponding weight vectors, as shown in Figure 1. The network is then given input patterns of sensor data or control signals from the CPS.

Then, using metrics like cosine similarity, nodes are activated based on how close the input pattern is to their corresponding weight vectors [25]. A vigilance parameter is used as a threshold for cluster activation, and a vigilance test is used to determine if the nodes currently in place can accurately reflect the input pattern. A new node is formed to build a new cluster, representing the distinct features of the input pattern, if none of the current nodes pass the vigilance test. To enable adaptation to changing features in the CPS network, the weight vectors of nodes that pass the vigilance test are changed to better reflect the given input pattern.

Because CPS data is dynamic and multidimensional, fuzzy logic is incorporated to allow partial membership of input patterns to various clusters. The adaptive learning mechanism of fuzzy ART guarantees ongoing learning by dynamically modifying weights and parameters as the network comes across novel patterns [26]. This flexibility helps to comprehend better, monitor, and make decisions within the complex and dynamic CPS environment by supporting already existing clusters or facilitating the formation of new ones.

3.2. Security Chief Selection

After zone formation, the next essential step is to select a security chief from each zone for which two critical factors, trust and energy, are introduced. In this, trust computation focuses on the packet count, a key measure for measuring the dependability of nodes in a network.

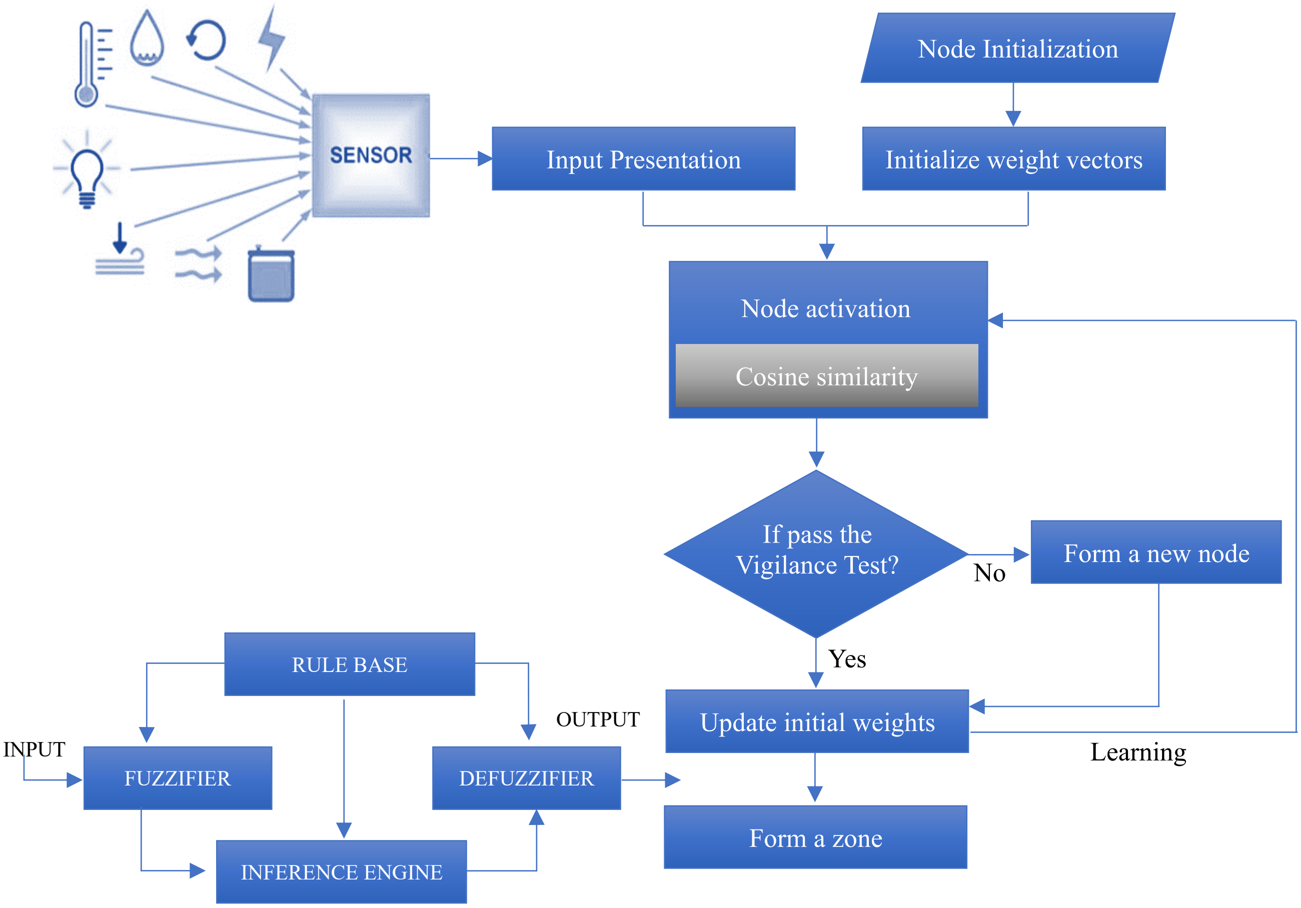

Fig. 1 Security zone formation

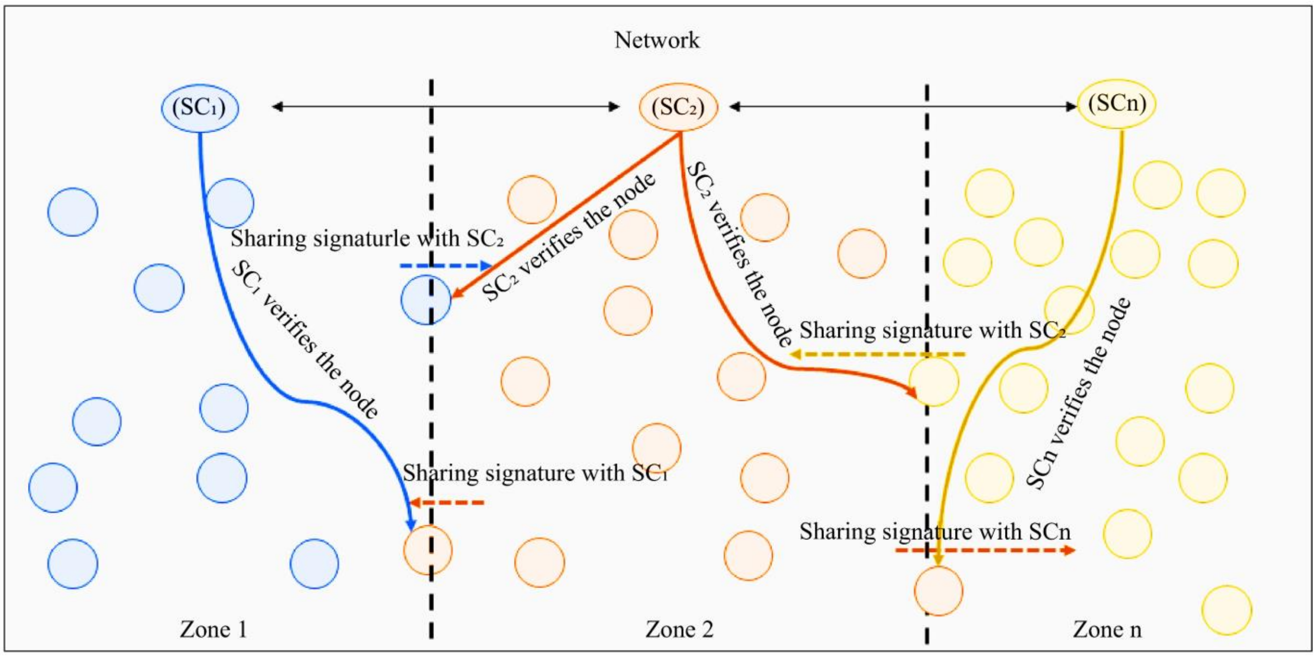

Fig. 2 Inter and Intra zone verification

The system evaluates the reliability of nodes by closely examining their transmission activities. Because they are more involved and active in the network, nodes that regularly send out more packets are considered more trustworthy. Every node in the network has its trust *(T_n)*, evaluated using the following calculations across the network, and the trust values that are obtained are kept in the node tables for each entity in the network.

$$T_n = Number\ of\ packets\ sent\ by\ nth\ node/Time \tag{1}$$

Furthermore, the energy factor is computed for each node, which utilizes the initial energy information *(E_i)* and computes the nodes' current energy level using the following:

$$E_n = E_i - (E_r + E_f + E_d) \tag{2}$$

Where E_n represents the nodes' current energy level, E_r is the energy consumed by a node when it receives a packet, E_f is the energy consumed by a node when it forwards a packet, and E_d is the ideal energy consumed by a node.

These factors are computed for each node of the zone and each zone. Then, to select a security chief (SCi) for the zone, the following computations are performed.

$$v = \frac{1}{k}\sum(T_k, E_k) \tag{3}$$

Where v is the validation value to select SC_i, so nodes having $(T_n + E_n)$ value greater than v is selected and added to the validation list, then the node having the maximum $(T_n + E_n)$ value will be selected as SC_i of a zone. The SC_i of the zone is dynamically updated over time or when nodes change their zones.

3.3. Inter and Intra Zone Verification

This step helps authorize the zone's current nodes and new nodes entering into the zone using the SHA-256 hash generation function [27]. A cryptographic hash algorithm called SHA-256 generates outputs with a fixed size of 256 bits. It is essential because it generates a unique hash value for each data set. This hash creates a safe digital signature when coupled with RSA [28]. So, here in this work, SC_i of the zone generates a unique signature for their nodes and verifies it during communication, called intra-zone verification. On the other hand, inter-zone verification is the verification of the nodes entering from one zone to another, as shown in Figure 2.

In this inter-zone verification, the SC_i of the zones plays a crucial role because they communicate with each other and share their signature so that the newly entered node will be verified. So, when the signature of the newly entered nodes is not verified from the neighbored zones, it is treated as a suspicious node.

The nodes that fall under the suspicious node category cannot participate in any network communication. Hence, the network is secured from intruders.

3.4. Route Optimization

This step is also an essential step of communication, and it utilizes an optimization algorithm to find and select an optimal path for data transmission over the network. This work proposes an integrated spider monkey [29] and krill herd optimization (SM-KHO) algorithm. Initially, the spider monkey selects the best nodes between source and destination, and further, the krill herd optimizes it to select final nodes between source and destination. The step-wise algorithm for route optimization is given as follows:

Algorithm 1: Hybrid SM-KHO for Route Optimization

Objective function: Maximize trust in the path

Input: Network nodes, Data

Output: Optimized path for data communication

```
Begin
Initialize the spider monkey population randomly within the search space and set initial parameters.
For i ← 1 to max iterations
    For each spider monkey
        Update position based on random movement
        Evaluate the fitness of the spider monkey.
        Sort the spider monkey based on fitness.
        Select top-performing monkeys and treat them as the initial population for the krill herd optimization.

        Compute the fitness of the krill based on the optimization function.
        Update the position and velocity of the krill using feeding and movement rules.
        Adjust the step size based on the fitness of the krill.
        For each krill
            Interact with neighbor Krill to exchange information.
            Update the position of krill based on social interactions.
            Avoid collision with other krill by adjusting positions.
            Implement an avoidance strategy to prevent crowding.
            Identify leaders among krill based on fitness.
            Adjust the movement of other krill to follow the leaders.
        End of for
    End of for
End of for
Select the highest fitted path as the best solution.
End
```

The above-integrated algorithm starts with the initialization of the spider monkey population, which here, in this case, is the randomly selected neighbor nodes of the source. Then, for each spider monkey, i.e., nodes, due to their movement, its positions are updated, and their fitness is evaluated. The parameter to evaluate the fitness is the trust value computed using Equation 1. Then, based on fitness and the number of nodes, top performers' mean nodes with high trust factors are further treated as the initial population of krill herd optimization. Here, the fitness of nodes is evaluated based on equation 3, and positions and node mobility information are also updated. This information is mainly required to identify the node zone and further for its verification while communicating with the security chief (SC). Based on krill optimization parameters, the path with the highest fitness values is selected as the best, and the source communicates through that path.

There can be two cases when selecting a path; in the first case, the source and destination nodes are in the same zone. In this case, when the source initiates the request for communication, it first finds the security chief of that zone. It verifies whether the destination and other path nodes are secured enough to communicate; if SC indicates that all the nodes have verified with their digital signature, then only communication starts between the source and destination. On the other hand, if the destination node is present in the other zone, then the SC of the source node zone communicates with the SC of the other zone and shares the verification details to maintain safe communication. This process is continuously updated due to the mobile nature of nodes, so the role of SC and optimization is crucial.

So, based on the above strategy, the communication of the CPS can be secured, preventing information and data theft or loss.

4. Simulation and Result Analysis

The proposed architecture of the CPS is simulated using an NS-2 simulator where two different network scenarios are simulated, including varying attacker nodes and connections. Two different attacks are implemented in these network scenarios: Distributed denial of service (DDoS) and blackhole attack. The network is simulated over the area of *100x100 m^2* with other parameters defined in the table below:

Table 1. Simulation setup

Parameter	Value
Area	100x100m^2
Number of nodes	100
Number of attacker nodes	5, 10, 15, 20 (scen-1) 5 (scen-2)
Number of connections	20 (scen-1) 20, 40, 60, 80 (scen-2)
Speed	30 m/s
Attack type	Collaborative (Blackhole and DDoS)
Simulation time	300s

The provided parameters are fundamental network settings utilized for simulating the network and evaluating the performance of the proposed architecture. Furthermore, the performance of the proposed trustworthy CPS architecture is computed using three different performance metrics: packet delivery ratio (PDR), throughput, and latency. It is also compared with approaches such as SMO [29], KHO [20], and Hybrid KH-SMO. The analysis of the network over different scenarios is discussed as follows:

4.1. Varying Attacker Nodes

In this scenario, the analysis involves varying the number of attacker nodes. The minimum configuration includes five attacker nodes, consisting of 2 blackhole nodes and 3 DDoS nodes. This ratio is maintained as the number of attacker nodes increases. The results in terms of packet delivery ratio represented the effectiveness of the proposed trustworthy CPS architecture in Figure 3.

The performance of optimization algorithms—KHO, SMO, and KH-SMO—in the context of a reliable CPS is depicted in Figure 3. The evaluation considers various attacker node configurations and uses the PDR expressed as percentage values as the statistic. Whereas SMO displays PDR percentages between 91.04% and 79.46%, KHO displays PDR numbers between 93.67% and 74.58%. PDR ranging from 95.49% to 80.04% indicates a balanced performance for the hybrid technique, KH-SMO. Surprisingly, the "Trustworthy CPS" category continuously performs better than all algorithms, attaining the greatest PDR percentages (98.84% to 90.31%) for all node permutations. Furthermore, based on the acquired data, the PDR lowers as the number of attacker nodes grows. These results highlight the robustness of the Trustworthy CPS model against an increasing number of attacker nodes, guaranteeing dependable communication in various scenarios.

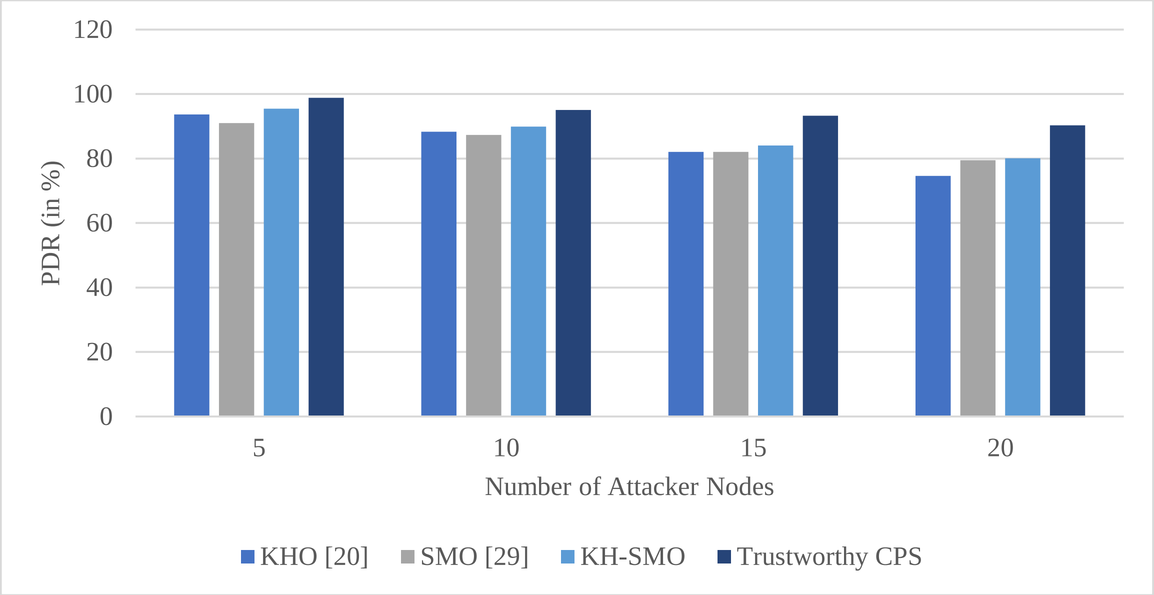

Fig. 3 Packet delivery ratio (Varying attackers)

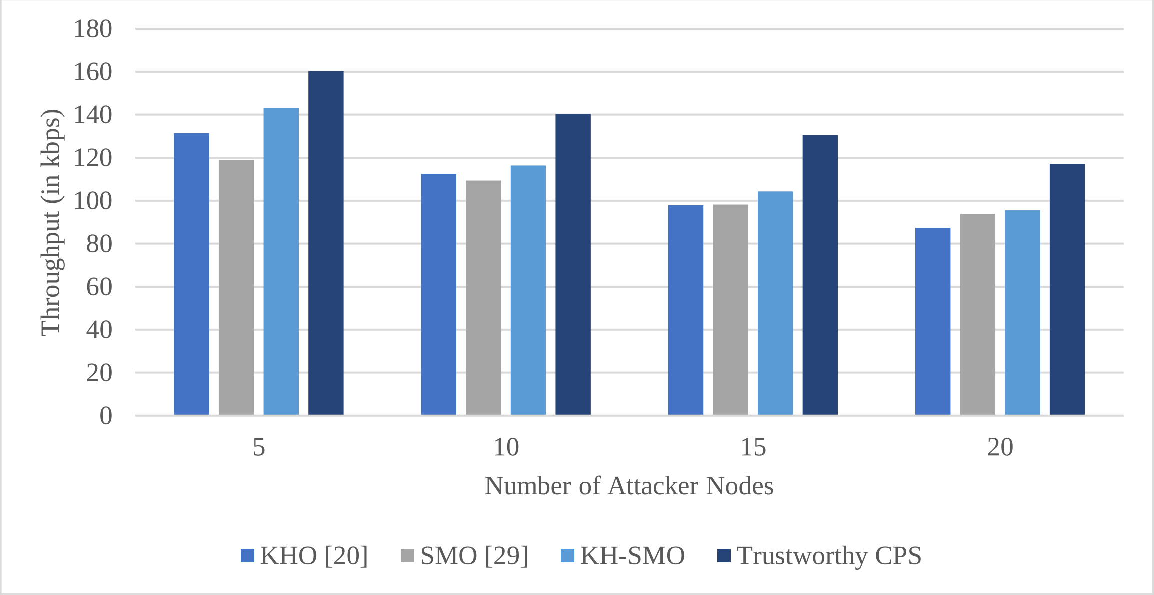

Fig. 4 Throughput (Varying attackers)

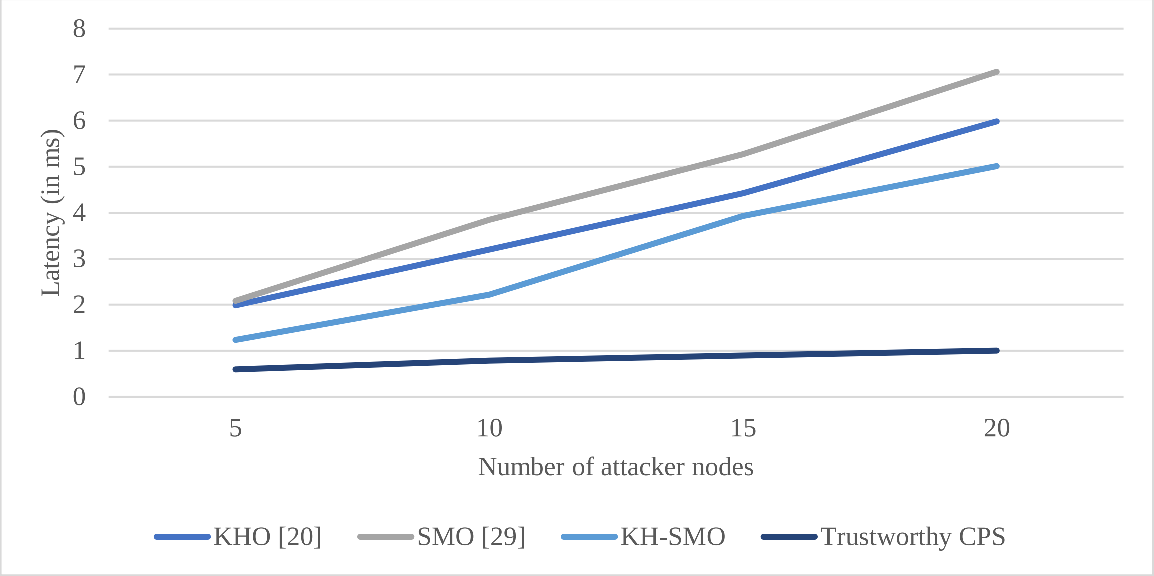

Fig. 5 Latency (Varying attackers)

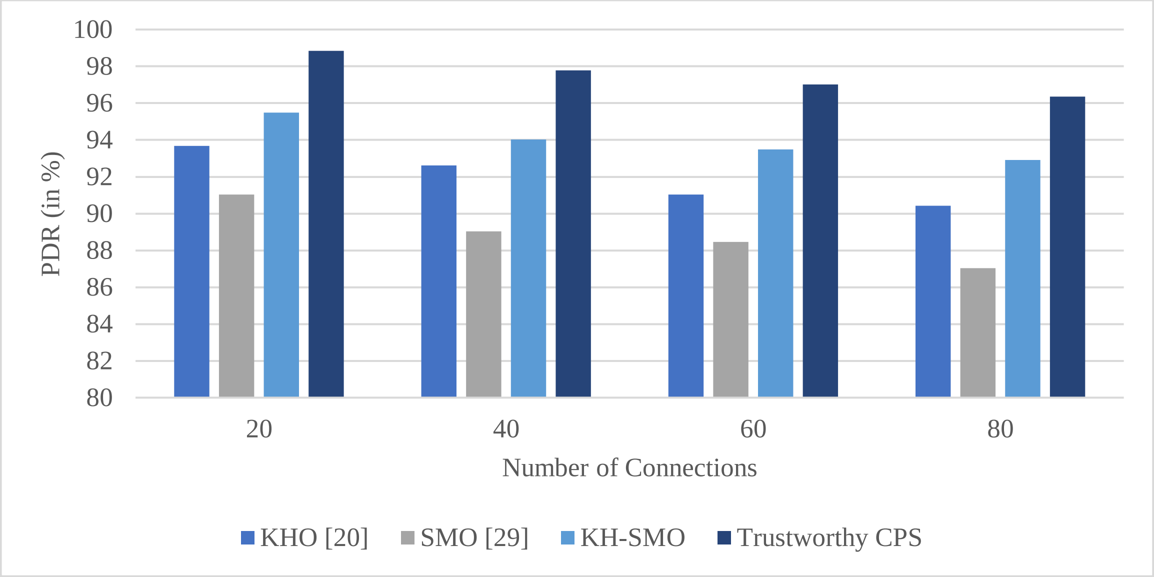

Fig. 6 Packet Delivery Ratio (Varying connections)

The throughput performance of the Trustworthy CPS, KHO, SMO, and KH-SMO is shown in Figure 4—throughput reported for various node topologies, measured in kbps. To be more precise, SMO displays percentages between 118.94 and 93.94, while KHO displays throughput figures between 131.38 and 87.27. Throughput numbers for the KH-SMO hybrid method range from 143.02 to 95.48. Among the node variants, ranging from 160.32 to 117.13, the "Trustworthy CPS" category consistently achieves the maximum throughput, outperforming all other methods. The noticeable performance trend that decreases as the number of attacker nodes rises is an exciting finding. This pattern emphasizes how more adversaries affect the system's throughput and suggests a possible link between security risks and less effective data transfer in the CPS design. The latency values for KHO, SMO, KH-SMO, and the Trustworthy CPS model are shown in Figure 5 in milliseconds. The term "latency" refers to the time lag in data transmission and is reported for various node configurations. KHO displays latency between 2.084 and 7.062 milliseconds, whereas SMO shows between 1.987 and 5.984 milliseconds. The hybrid KH-SMO method shows values between 1.235 and 5.012 milliseconds. Surprisingly, the "Trustworthy CPS" category regularly beats every algorithm and achieves the lowest latency percentage, varying from 0.594 to 1.003 milliseconds. These findings highlight the effectiveness of the Reliable CPS model in reducing latency and guaranteeing timely data transfer compared to the separate and hybrid optimization, even in the presence of variable attacker nodes.

4.2. Varying Connections

In this simulation scenario, several connections are varied to increase the traffic rate and analyze its impact on existing algorithms and proposed trustworthy CPS. Here, the minimum number of connections created was 20, increasing with step size 20 only—the simulation results of a network over this scenario are discussed in this section.

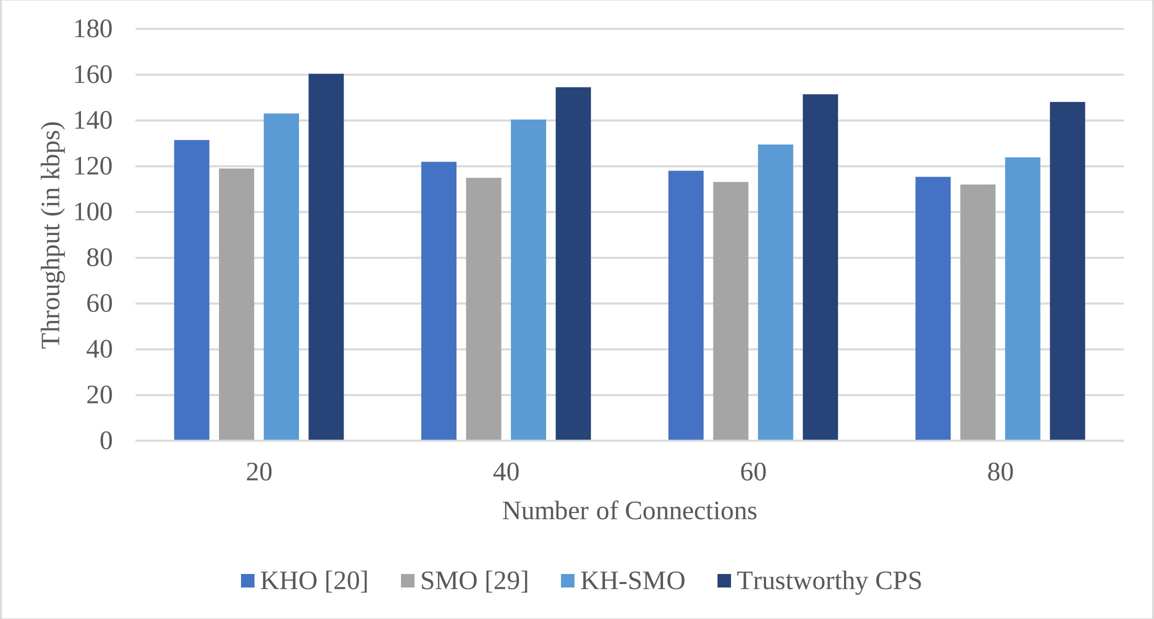

Fig. 7 Throughput (Varying connections)

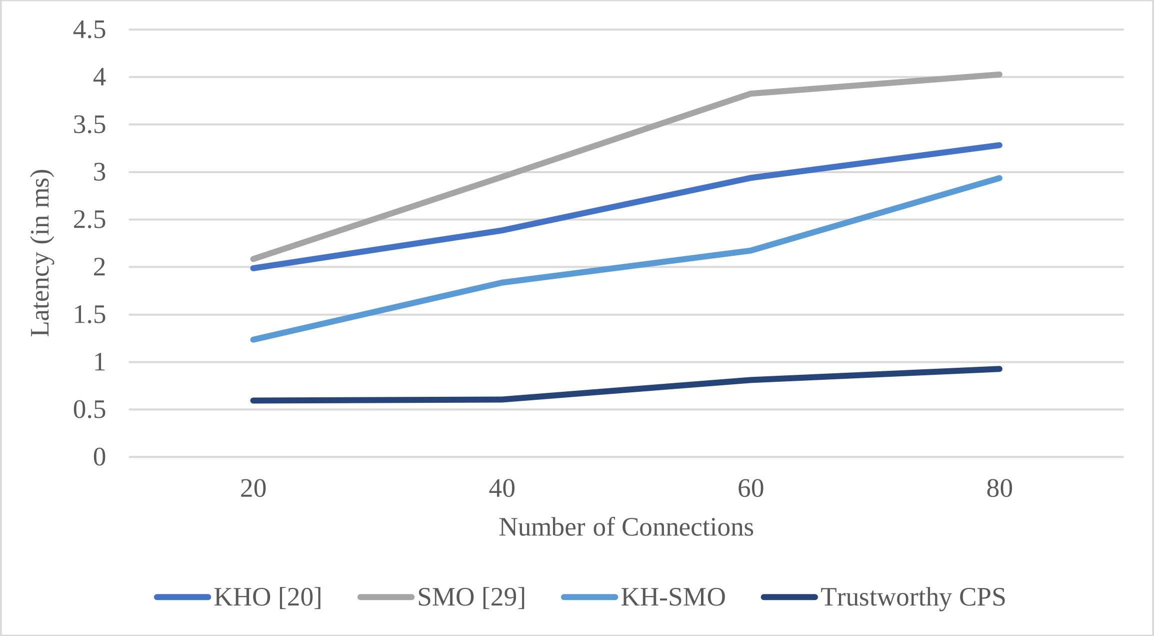

Fig. 8 Latency (Varying connections)

The graph in Figure 6 shows PDR fluctuations for the KHO, SMO, KH-SMO, and proposed Trustworthy CPS, with increasing connectivity. As connection percentages increase, KHO's PDR varies from 93.67% to 90.43%, SMO varies from 91.04% to 87.03%, and KH-SMO steadily decreases from 95.49% to 92.92%. Outperforming all other categories, the "Trustworthy CPS" achieves the greatest PDR percentages, ranging from 98.84% to 96.36%. Interestingly, PDR decreases for all algorithms as connection percentages rise, highlighting the better robustness of the Trustworthy CPS model in sustaining effective packet delivery over individual and hybrid optimization methods in various connection circumstances. Figure 7 shows the throughput numbers, expressed in kilobits per second (kbps), for various connection percentages. The performance of KHO, SMO, KH-SMO, and the Trustworthy CPS are shown in the findings. KHO's throughput varies from 131.38 kbps to 115.31 kbps on the graph, showing a decline as connection percentages rise. SMO displays throughput percentages that fluctuate over different connection levels, ranging from 118.94 kbps to 111.97 kbps. Throughput statistics for the KH-SMO hybrid technique range from 143.02 kbps to 123.81 kbps, suggesting a nuanced response in performance to varying connection percentages. The "Trustworthy CPS" method achieves the highest throughput percentages, ranging from 160.32 kbps to 148.04 kbps, continuously outperforming other algorithms. The graphical depiction provides a visual understanding of how varying connection percentages impact the throughput of each algorithm, with the Trustworthy CPS model exhibiting better performance across all circumstances.

For various optimization strategies, the latency results—which show the time interval measured in milliseconds—are recorded for different connection percentages and presented in Figure 8. As the connection % rises, KHO displays latency numbers ranging from 1.987 ms to 3.283 ms. SMO shows latency percentages for connection settings ranging from 2.084 ms to 4.027 ms. With latency values ranging from 1.235 ms to 2.936 ms, the hybrid technique KH-SMO exhibits sophisticated reactions to varying connection percentages. Surprisingly, the "Trustworthy CPS" routinely beats other algorithms and achieves the lowest latency percentages (0.594 ms to 0.927 ms) throughout network variances. These findings highlight the Trustworthy CPS model's effectiveness in reducing latency and guaranteeing timely data transmission compared to standalone and hybrid optimization methods in various connection settings.

The results obtained from the assessment of two different scenarios categorically confirm the enhanced efficacy and better performance of the suggested Trustworthy CPS compared to other approaches. After a thorough review of all these cases, it is evident that the Trustworthy CPS performs better than the other approaches, demonstrating increased efficiency and a higher degree of efficacy in achieving the intended performance metrics. These findings validate the Trustworthy CPS model's resilience and dependability, making it a more capable and practical approach to enhancing network performance and guaranteeing the safe and dependable functioning of Cyber-Physical Systems.The experimentation results present the effectiveness of the proposed approach. The reason behind this improvement is multi-level protection from the attacker nodes and the optimum path for data transmission. For instance, if an intruder tries to enter any zone, the security chief who verifies the nodes can identify it.

This centralized security hence blocks the intruders and also intimate to other zone nodes to avoid communication with the identified intruder. Moreover, the optimum path selection avoids insecure, lengthy, and interrupted paths, making the data transmission smooth and fast. In this way, the proposed approach provides a robust solution for secure and effective communication.

5. Conclusion

In conclusion, the thorough assessment of the proposed Trustworthy CPS highlights its resilience and efficiency in various situations. With its hybrid KH-SMO combination, the Trustworthy CPS is a robust solution that enhances communication and protects Cyber-Physical Systems from future threats.The suggested architecture is organized into phases that are clearly described. Fuzzy ART is first used to cluster network nodes, dynamically guaranteeing flexible and effective grouping. The system's dependability is then increased by assigning a security head based on energy and trust factors to each cluster or security zone. Then, every security head uses SHA-256 to create a signature, a robust hashing method that allows nodes in each zone to be verified securely. Additionally, the design uses the hybrid KHO and SMO algorithms to include route optimization during communication.

This dynamic combination minimizes exposure to possible assaults and enables the system to adapt and optimize pathways effectively, guaranteeing successful communication. The suggested design places even more emphasis on security by taking into account possible dangers like DDoS and blackholes. The design uses RSA and SHA-256 for secure authentication and intrusion prevention, and signature verification is used during route selection to improve security further. The average performance of the Trustworthy CPS is further demonstrated by combining the average results from the two implemented scenarios. These results indicate an average PDR of 95.935%, an average throughput of 134.17kbps, and a minimal latency of 0.776ms across various network situations. This performance and the proposed architecture's well-defined processes and adaptive measures establish the Trustworthy CPS as a dependable and robust solution for cyber-physical system performance optimization and communication security.

References

[1] Ayaskanta Mishra et al., “Emerging Technologies and Design Aspects of Next Generation Cyber Physical System with a Smart City Application Perspective,” *International Journal of System Assurance Engineering and Management*, vol. 14, pp. 699-721, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Maki K. Habib, and Chimsom Isidore Chukwuemeka, “CPS: Role, Characteristics, Architectures and Future Potentials,” *Procedia Computer Science*, vol. 200, pp. 1347-1358, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] David G. Rosado et al., “Managing Cybersecurity Risks of Cyber-Physical Systems: The MARISMA-CPS Pattern,” *Computers in Industry*, vol. 142, pp. 1-20, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Shaokai Lin et al., “Towards Building Verifiable CPS using Lingua Franca,” *ACM Transactions on Embedded Computing Systems*, vol. 22, no. 5s, pp. 1-24, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Jiacheng Xie, Shuguang Liu, and Xuewen Wang, “Framework for a Closed-Loop Cooperative Human Cyber-Physical System for the Mining Industry Driven by VR and AR: MHCPS,” *Computers & Industrial Engineering*, vol. 168, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Sunil Kr. Singh et al., *Evolving Requirements and Application of SDN and IoT in the Context of Industry 4.0, Blockchain and Artificial Intelligence*, Software Defined Networks, Wiley, pp. 427-496, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Zakir Ahmad Sheikh et al., “Intelligent and Secure Framework for Critical Infrastructure (CPS): Current Trends, Challenges, and Future Scope,” *Computer Communications*, vol. 193, pp. 302-331, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Neha Agrawal, and Rohit Kumar, "Security Perspective Analysis of Industrial Cyber Physical Systems (I-CPS): A Decade-Wide Survey," *ISA Transactions*, vol. 130, pp. 10-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Muhammad Fakhrul Safitra, Muharman Lubis, and Hanif Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability*, vol. 15, no. 18, pp. 1-32, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] P. Muralidhara Rao, and B.D. Deebak, "Security and Privacy Issues in Smart Cities/Industries: Technologies, Applications, and Challenges," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 10517-10553, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Valentina Casola et al., "Designing Secure and Resilient Cyber-Physical Systems: A Model-based Moving Target Defense Approach," *IEEE Transactions on Emerging Topics in Computing*, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Dipankar Dasgupta, Zahid Akhtar, and Sajib Sen, "Machine Learning in Cybersecurity: A Comprehensive Survey," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, vol. 19, no. 1, pp. 57-106, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] May Bashendy, Ashraf Tantawy, and Abdelkarim Erradi, "Intrusion Response Systems for Cyber-Physical Systems: A Comprehensive Survey," *Computers & Security*, vol. 124, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Aniruddh Chandratre et al., "Stealthy Attacks Formalized as STL Formulas for Falsification of CPS Security," *Proceedings of the 26th ACM International Conference on Hybrid Systems: Computation and Control*, New York, USA, no. 15, pp. 1-8, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ying Ju et al., "Reliability-Security Trade-off Analysis in mmWave Ad Hoc Based CPS," *ACM Transactions on Sensor Networks*, vol. 2, no. 2, pp. 1-23, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Zakir Ahmad Sheikh et al., "Defending the Defender: Adversarial Learning Based Defending Strategy for Learning Based Security Methods in Cyber-Physical Systems (CPS)," *Sensors*, vol. 23, no. 12, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Junyi Liu et al., "CPS Attack Detection under Limited Local Information in Cyber Security: An Ensemble Multi-Node Multi-Class Classification Approach," *ACM Transactions on Sensor Networks*, vol. 20, no. 2, pp. 1-27, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Lei Ma et al., "Recursive Watermarking-Based Transient Covert Attack Detection for the Industrial CPS," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1709-1719, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Manal Abdullah Alohali et al., "Swarm Intelligence for IoT Attack Detection in Fog-Enabled Cyber-Physical System," *Computers and Electrical Engineering*, vol. 108, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] S. Sivamohan, S.S. Sridhar, and S. Krishnaveni, "TEA-EKHO-IDS: An Intrusion Detection System for Industrial CPS with Trustworthy Explainable AI and Enhanced Krill Herd Optimization," *Peer-to-Peer Networking and Applications*, vol. 16, pp. 1993-2021, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Umesh Kumar Lilhore et al., "EHML: An Efficient Hybrid Machine Learning Model for Cyber Threat Forecasting in CPS," *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, Greater Noida, India, pp. 1453-1458, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Shimeng Wu et al., "Attack Prevention and Detection For Cyber-Physical Systems Based on Coprime Factorization Technique," *2023 IEEE 32nd International Symposium on Industrial Electronics (ISIE)*, Helsinki, Finland, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] S. Simonthomas, and R. Subramanian, "Detection and Prevention of Cyber-Attacks in Cyber-Physical Systems based on Nature Inspired Algorithm," *2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)*, Coimbatore, India, pp. 483-487, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] Samuel Oliveira et al., "Security of Cyber-Physical Systems Against Actuator Attacks through Cryptography*," *2023 International Conference on Information Technology (ICIT)*, Amman, Jordan, pp. 758-764, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] David G. Lowe, "Similarity Metric Learning for a Variable-Kernel Classifier," *Neural Computation*, vol. 7, no. 1, pp. 72-85, 1995. [CrossRef] [Google Scholar] [Publisher Link]

[26] Igor Škrjanc et al., "Evolving Fuzzy and Neuro-Fuzzy Approaches in Clustering, Regression, Identification, and Classification: A Survey," *Information Sciences*, vol. 490, pp. 344-368, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[27] Hassan. M. Elkamchouchi, Abdel-Aty M. Emarah, and Esam A. A. Hagras, "A New Secure Hash Dynamic Structure Algorithm (SHDSA) for Public Key Digital Signature Schemes," *Proceedings of the Twenty Third National Radio Science Conference (NRSC'2006)*, Menouf, Egypt, pp. 1-9, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[28] Yevgeniy Dodis, Iftach Haitner, and Aris Tentes, "On the Instantiability of Hash-and-Sign RSA Signatures," *Theory of Cryptography: 9th Theory of Cryptography Conference*, Taormina, Sicily, Italy, pp. 112-132, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[29] Jagdish Chand Bansal et al., "Spider Monkey Optimization Algorithm for Numerical Optimization," *Memetic Computing*, vol. 6, pp. 31-47, 2014. [CrossRef] [Google Scholar] [Publisher Link]