Electronic Research Archive

http://www.aimspress.com/journal/ERA

ERA, 31(4): 1876–1896.
DOI: 10.3934/era.2023097
Received: 19 November 2022
Revised: 24 December 2022
Accepted: 05 January 2023
Published: 09 February 2023

*Research article*

# Integrating artificial intelligence in cyber security for cyber-physical systems

**Majed Alowaidi[1], Sunil Kumar Sharma[2,*], Abdullah AlEnizi[1] and Shivam Bhardwaj[3]**

[1] Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Majmaah 11952, Saudi Arabia
[2] Department of Information System, College of Computer and Information Sciences, Majmaah University, Majmaah 11952, Saudi Arabia
[3] Department of Computer Science, Pennsylvania State University, W255 Olmstead Building, Middletown, PA 17057, USA

* **Correspondence:** Email: s.sharma@mu.edu.sa.

**Abstract:** Due to the complexities of systems thinking and the communication between independent Cyber-Physical Systems (CPSs) areas through accumulative expansion, several security threats are posed, such as deception of channels for information sharing, hardware aspects and virtual machines. CPSs have become increasingly complex, sophisticated, knowledgeable and fully independent. Because of their complex interactions between heterogeneous virtual and objective components, CPSs are subject to significant disturbances from intended and unintended events, making it extremely difficult for scientists to predict their behavior. This paper proposes a framework for Cyber-Physical Business Systems based on Artificial Intelligence (CPBS-AI). It summarizes several safety risks in distinct CPS levels, their threat modeling and the scientific challenges they face in building effective security solutions. This research provides a thorough overview of current state-of-the-art static capable of adapting detection and tracking approaches and their methodological limitations, namely, the difficulty of identifying runtime security attacks caused by hibernation or uncertainty. The way of identifying the threat and the security attacks in networks reduce the complexities in the communication in CPS. The negligible threats exhibit an inability to be identified, avoided and blocked by Intrusion Prevention Security Systems (IPSSs), and misbehavior in the database of the safety measures is analyzed. Neural Networks (NN) and Variable Structure Control (VSC) are designed to estimate attacks and prevent the risk of threats in tracking applications using a nonlinear monitoring system based on VSC. NN and the VSC evaluate the different attacks based on the nonlinear monitoring system. The evaluation of the proposed CPBS-AI is based on the request time analysis, accuracy, loss and reliability analysis. The overall effectiveness of the system is about 96.01%.

**Keywords:** integrating; artificial intelligence; cyber security; cyber-physical systems; neural network; intrusion prevention

## 1. Introduction

Modern technology, such as Cloud Computing (CC), Cyber-Physical Systems (CPSs) and automation devices, is critical in small and Medium-Scale Enterprises (SME) and manufacturing firms [1]. Integrating data processing, connectivity and physical methods is the goal of Cyber-Physical Systems. Combined with the universe and its processes, a CPS comprises interconnected computational objects that work together [2]. Although Cyber-Physical Systems are closely related to the Internet of Things (IoT), they maintain a distinct distance because of their unique association with material objects [3]. Examples of CPS include self-driving cars, robotic technology, smart buildings, smart power grids, intelligent manufacturing and transplanted medical devices [4]. Even in CPSs, however, cyber-attacks can lead to physical system failure or damage [5]. The automatic compensation of fault consequences and the maintenance of the system's performance at some appropriate standard are two research challenges in such techniques [6]. SMEs' infrastructures have been transformed due to these breakthroughs, which have seen substantial commercial success worldwide [7]. CPSs offer sensor-based connections to industrial technologies and intelligence, new business models, opportunities for developing cutting-edge IT solutions and resources for improving current industrial computer systems [8]. Intelligent systems and IoT (IoT) environments are a few examples of these systems [9], which have emerged as exciting new areas of application for artificial intelligence. Adapting AI methods and instruments to the new CPS requirements will be difficult [10]. The acronym NN is given in the abstract as Neural Network. Neural networks are sets of algorithms designed to learn from data in a manner that is analogous to how the human mind does this. The NN in AI is defined in Figure 4 clearly: "Neural networks" can refer to biological or synthetic systems comprised of neurotransmitters. Using neural networks allows devices to make smart judgments with minimal human input. This is due to their ability to learn and predict complex and complicated correlations between input and output information.

CPSs offer comprehensive computer and networking capabilities. Computer and storage solutions provided by computer technology (CT) can be tailored to meet the needs of a wide range of businesses and organizations using IPSSs [11]. Reduced IT costs give small and medium-sized enterprises a high-performance computer advantage by their purchasing precisely the amount of software or hardware needed [12]. Cloud systems or ubiquitous production can describe Service-Oriented Architectures (SOA) and intelligent systems in manufacturing based on CPSs [13]. As a result, the idea of providing computing capabilities for manufacturing and services is accepted in NN [14]. This way, resources are available for current output, and target consumers or internet providers can access them via CPSs and other ubiquitous networks on the systems [15]. There is exponential growth for machine intelligence that can interact with the surroundings [16], such as driverless cars that supervise and connect with their surroundings and home automation that optimizes power consumption due to advances in analytics, AI and communications [17]. Ever-increasing knowledge and information are embedded in these intelligent machines, allowing them to make better and faster decisions in massively complicated data environments [18]. The information security shields of CPSs can be supplemented by control systems [19]. These systems can withstand attacks; additionally, they can be part of more extensive intrusion detection and macroeconomic variables [20]. Even in CPSs, however, cyber-attacks can lead to physical system breakdowns [21]. Artificial intelligence techniques and the means by which they are placed form the foundation of the device upon which the virtual producer operates, whether that factory is based on the edge, fog or cloud computing resources and whether its tools and structures for regulating technical mechanisms are unified or dispersed. Aspects that make up manufacturing (technological resources, organization, etc.), combined into the overall architecture, form the basis of an industrialized item in a cyber-physical system.

System performance must be maintained at some acceptable level even when faults are automatically rewarded deliberately [22]. Sensors and system processes frequently target attacks or defects [23]. Thus, these concepts have been consolidated into a single system of thought. SMEs are initially linked by various vendors using a variety of standards and interaction systems [24]. The overall system performance is used to detect the faults and the attacks in CPSs. The different types of attacks are concentrated in CPSs other than the existing methods. CPSs suggest that the environment is diverse, and advancements are structured consistently. System of thought will be even when defects are automatically rewarded deliberately, and system capacity must be maintained satisfactorily. Threats and flaws in the system are often the focus of sensors and associated procedures. As a result, these ideas have been unified into a coherent framework.

Third-party providers and trust in third parties are barriers to businesses adopting these models, which rely on concentrated communication structures.

The primary aim of this paper involves the following.

a) An intelligent classic control approach for compensating the scalar attacks on nonlinear CPSs is presented in this paper.

b) The research outlines the steps needed to implement adequate security controls at various levels of the CPS through IPSSs and NN.

c) A description of the project and in-depth research into the most recent CPS security measures are analyzed using CPBS-AI.

The following is the rest of this article: Section 2 describes the context of the cyber-physical system models. Section 3 designs the suggested cyber-physical business systems based on artificial intelligence (CPBS-AI) framework. Section 4 depicts software analysis and assessment. Lastly, Section 5 provides the conclusion and the new technological revolution's problems, which include linking numerous CPSs to conduct autonomous activities in a small environment as a future scope.

## 2. Materials and methods

More research related to CPSs is well described based on the ideas and the applications. The background section concentrates on the significant CPS research efforts from various perspectives, including application domains, confidentiality and vulnerability, among other conventional approaches below.

Cyber-Physical Systems (CPS) and Blockchain technology are becoming increasingly popular. However, developing robust and correct Smart Contracts (SCs) for these cutting-edge applications is an ongoing struggle [25]. As evidenced by the existing proposals, complex SCs cannot be designed to mitigate security and privacy challenges. As a result, various Artificial Intelligence (AI) Techniques For Safeguarding SC Privacy (AIT-SSCP) are examined in this paper.

Medical Cyber-Physical Systems (MCPSs) prescribe a platform for the acquisition, pre-processing and cloud-based processing of healthcare information by evolving Internet of Things (IoT) sensors [26]. MCPSs include how essential signals are transformed into functionalities or used by machine-learning algorithms.

There are new possibilities in Industry 4.0 environments thanks to Artificial Intelligence (AI). Despite this, AI systems in industrial settings face significant challenges due to the lack of pertinent information and the need for truthfulness [27]. As an alternative, the advent of cyber-physical systems in Industry 4.0 opens up new possibilities for human-AI interaction. The paper proposes and describes how to build an operator 4.0-Machine Intelligence Symbiotically Human Cyber-Physical System (MIS-HCPS) framework. It has been introduced for AI systems in the workplace, which are still confronted with significant challenges due to a lack of appropriate data and a requirement for honesty.

In addition to creating a suitable extensive data analysis, significant data architecture had to be integrated with data modeling, infrastructures and a technology catalog [28]. The available information was used at the time of the decision, and methods were devised to assess a large-scale data architecture [OLSDA]. The role of cloud computing, its behaviors and its functional components can now be defined with greater clarity and neutrality thanks to a case modeling technique applied to an abstract large data structure.

Combining IoT and Big Data resulted in the Cognitive-Based IoT Big-Data (COIBD) Model creating an industrial IoT device; as a result, the COIBD System could not extract the data it needed from sampling and integration to improve management [29]. Experts proposed five-layered data architecture for Industry 4.0, including sensors, power actuators, networking, clouds and IoT technology. In addition, information management helped to ensure the long-term viability of data reactions.

Despite introduction of a Framework for a Mutually Intelligent and Symbiotic Cyber-Physical System (MIS-HCPS), artificial intelligence (AI) systems in the workplace face substantial obstacles owing to a lack of relevant data and a need for integrity.

With the proliferation of IoT devices and AI software, securing CPSs from cyberattacks is increasingly difficult. Here, we investigate how adversarial assaults affect Deep Learning-Based Anomaly Detection in CPS networks and how to defend against them by reinforcing models using antagonistic data [30]. The two CPS networks are modeled after the Bot-IoT and Modbus IoT datasets. The experimental result shows that antagonistic inputs in FGSM can affect predictive performance and that the retrained model can be used to ward off the attack.

Analytical approaches to current Cyber-Physical System (CPS) analysis are founded on principles that vary depending on whether or not safety or liveness criteria are considered. Various methods, such as stochastic modeling and contracts, are used to abstract complexity [31]. Reinforcement learning-based procedures are necessary because of the ambiguity introduced by dispersed algorithms and AI-based methods, as well as the user's perspective or unforeseen impacts like accidents or the weather. This study contrasts the viewpoint of AI researchers on researching unknown complex systems with that of experts in the field of CPS design and prediction.

As a term that encompasses both physical and electronic elements, "Cyber-Physical Systems" (CPSs) have broad use (smart grid, smart transportation, smart manufacturing, etc.). An integral part of CPSs will be the Digital Twin (DT), a cyber-clone of a tangible object or entity. With a four-layer architectural lens, this research creates a taxonomy to investigate the many attacks against DT-based

CPSs and their effects. For DT-based CPSs, we provide an attack space based on four levels (subject layer, complete line, DT layer, application server), three attack objects (confidentiality, integrity and availability), and attack kinds paired with power and expertise. Finally, we suggest using various enabling approaches (intrusion detection, blockchain, modeling, simulation and emulation) to secure DT-based CPS and propose a defensive mechanism dubbed Secured DT Development Life Cycle (SDTDLC) [32].

In [33], the authors take advantage of blockchain's prospective advantages and combines it with software-defined networking (SDN), all the time justifying the importance of addressing energy and security concerns. For the upcoming stage of industrial CPS, the proof-of-work (PoW) with private and public blockchains for the Peer-to-Peer (P2P) communication method helps solve the difficulties of energy management and security.

It is possible to use computer resources (clouds) for either centralized or decentralized cyber-physical manufacturing if artificial intelligence is treated as an individual control topic. An AI-based control system is presented, along with a description of how it may be implemented to manage the interdependencies between various cyber-physical systems and the output of factories operating under Industry 4.0 infrastructure [34].

This research introduces a high-performance real-time fine-grain object recognition framework to overcome issues with established methods for plant disease detection, such as density dispersion, irregular shape, multi-scale object classes and textural similarities. The foundation of the suggested model is the latest iteration of the You Only Look Once (YOLOv4) algorithm [35].

WilDect-YOLO [36] is introduced for an automated high-performance detection model trained using deep learning (DL) that can spot species from extinction in actual time. To facilitate robust and discriminative extraction of deep spatial objects, we include a leftover block with the CSPDarknet53's backbone and combine DenseNet blocks to enhance the preservation of vital characteristic data.

A novel design and a refined variant of Single Shot Multibox Detector (SSD), called Precise Single Stage Detector (PSSD) [37], deal with the problems of feature extraction and classification. The suggested model PSSD can produce impressive results in real time. Results from the experiments show that the suggested approach provides a better balance between speed and accuracy.

An intelligent network of methodologies and perceptions from cyber-attack scenarios was used to evaluate the danger of cyber-attack on intelligent metered systems. Analyses of the selected papers revealed a lack of progress in developing industrial analytics applications. The other conventional methods, AIT-SSCP, MCPSs, MIS-HCPS, OLSDA and COIBD, are compared with CPBS-AI.

CPBS-AI framework calculates the request time by comparing it with the existing methods. The existing method cannot detect particular attacks, and the predictive performance is not up to level. The existing methods do not ensure long-term viability. The data analytics and the data architecture with the modeling concepts have less assessment for data gathering. Safeguarding the information's confidentiality fails in many cases in the healthcare industry. The research, as mentioned earlier, the gap in the proposed CPBS-AI framework overcomes the existing method.

The suggested approach uses a conceptual framework for future research into CPBS-AI (cyber-physical business systems based on artificial intelligence) that is more effective and requires less time to request existing methods. Employing Intrusion Detection and Prevention Systems, AI-based security techniques illustrate some common CPS layer dangers and unresolved research difficulties in constructing intelligent CPS security safeguards. The methods such as AIT-SSCP, MCPSs, MIS-HCPS, OLSDA and COIBD are briefly explained in related works in Section 2.

## 3. Cyber-Physical business systems based on artificial intelligence

CPBS-AI offers a concise overview of various safety threats across varying CPS levels and the scientific obstacles that prevent us from developing security measures. CPBS-AI provides an in-depth analysis of the static capability detection and tracking systems and their methodological limitations. The ineffectiveness of IPSSs at detecting, avoiding and blocking low-level threats is examined. With a nonlinear monitoring system predicated on VSC, NN can estimate attacks and prevent the danger of threats in tracking applications.

Securing CPS networks is more complicated by these network systems' unique complexities and difficulties. The limited computational power of CPS devices is one illustration of this. Security systems must work efficiently and effectively within strict constraints without exhausting all resources available. Because of this, it is imperative to properly examine CPS design, specific applications and security challenges concerning the development of customized security solutions.

Physical domain behavior, rather than traditional technologies, is a source of CPS security risks, leading to various applications requiring physical protection and stability. Security risks must be categorized for effective preventive measures. Networked actuators, detectors, control processing elements and communications equipment are part of a more extensive distributed system called a Cyber-Physical System, represented below.

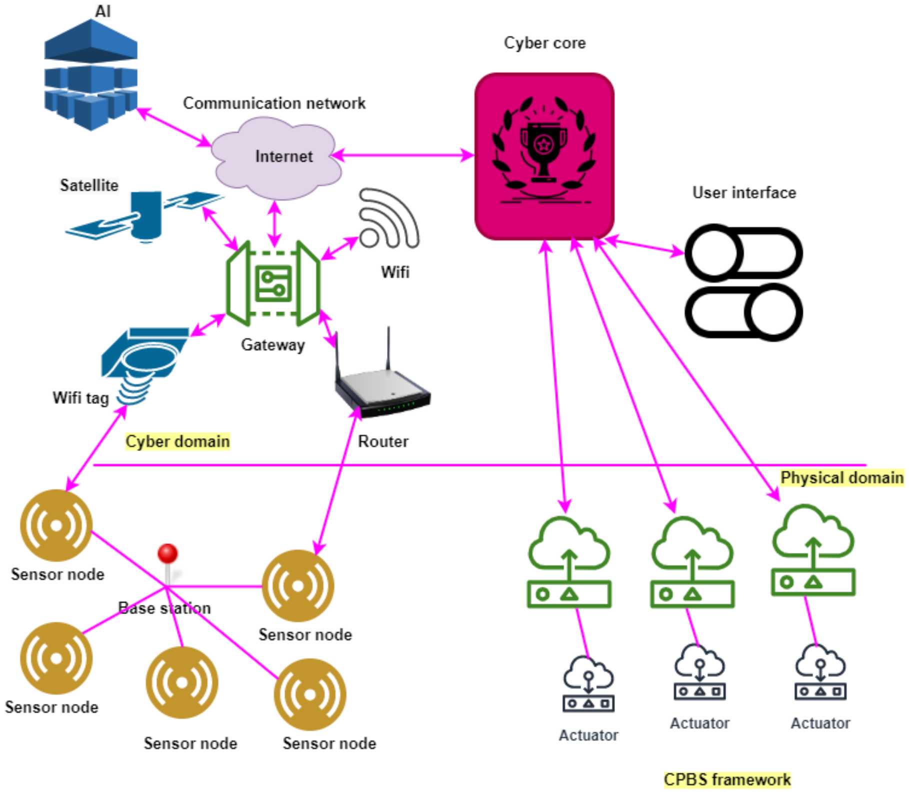

**Figure 1.** CPBS-AI framework process.

Figure 1 depicts the CPS's distinct organizational design. Components are typically linked together in a networked configuration using a Wi-Fi tag, satellite, Wi-Fi devices and router, which are interconnected with gateway and management mechanisms in CPSs. The different sensor nodes maintain the cyber domain in the communication network, the internet. The satellite data is transferred to the user interface through the gateway and Wi-Fi. The router transmits the data to each sensor node. The user interface interconnects with the physical domain. Sensor information is sent to the cyber domain via wired and wireless communication methods for simultaneous processing and actuation. System transformation and Internet backbone self-organization can be effectively facilitated by sending computing results from the cyber core into the physical domain. Because of their ability to operate in real-time, CPSs are known for their predictable behavior and ability to manage in real-time in AI systems. Increased use of CPSs in the industry can be attributed to their ability to connect systems that would otherwise be isolated from a cyber-core. CPSs are becoming more common, emphasizing how important it is to have solid security measures in place. A scalable risk assessment and a user interface require a quantification model to help quickly identify high-priority CPS security flaws in a base station, for which vulnerability scanning is required as part of recognizing the security requirements of CPSs. According to this model, privacy concerns in CPSs are represented as vulnerability dependency graphs that follow the structure of directed graphs. Graphics used to calculate system risks are used to identify which locations of the CPS are most vulnerable to attack. An acyclic graph has the problem that, as potential threats are discovered in a system, the graph size proliferates until it becomes impractical. Larger industrial designs cannot use the model because of this limitation.

There are no implementation changes to the methodology or excessive growth in the model proposed by the authors in this paper. These can be implemented in the specific sectors of CPS, such as sensors, communication networks or the CPS as a whole unit. As Eq (1) shows, most AI systems must work together to prevent minimal attacks, including learning algorithms and probabilistic reasoning.

$$sl_x = Pd^x f_{xs-1} + QS_{xs-1} = P^{xsd} st_0 + \sum_{i=0}^{j-1} \frac{Pd^{x-1-y_Q}}{S} \tag{1}$$

Attack detection is represented by $f_x$. The probability function $Pd$ is used at the given starting state $f_0$, the system reports $xs$ at any period for the input sequences $S_0, S_1, \cdots, S_{xs-1}$. Production is provided as a service by this layer, which includes services like machine tools and robotic systems for providers $xs$ by applying the summation of limits $i = 0 \; to \; j - 1$. The security aspects of detecting and overcoming the different attacks are represented as $S$. The security level is one of the major factors in overcoming all the threats and attacks in the network layers. This research work presents an operative information exchange between the customer's hardware facilities $st_0$ and the cloud-based system software $QS_{xs-1}$. As a result of human-machine communication, attack detection has improved using Eq (2).

$$f_x = Pdf_0 + \sum_{i=0}^{js-1} \frac{Pd^{xs-1-y_Q}}{S_x} \tag{2}$$

As Eq (1) shows, most AI systems must work together to prevent minimal attacks, including learning algorithms and probabilistic reasoning. Security experts should be involved. The probability function $Pd$ with the starting state $f_0$, the robotic systems for providers $xs$. $js$ represents the number of service layers. $y_Q$ represents machine communication, and $S_x$ denotes the way of attack detection.

Numerous security vulnerabilities and risks can be exploited in a cyber-physical attack due to the CPS integrating cyber and physical processes. As part of comprehensive risk management on a CPS, various system characteristics are considered when determining the overall impact of a threat vulnerability risk on the CPS. These features can be identified according to the anatomical structures of a cyber-physical network intrusion and the security concerns previously identified.

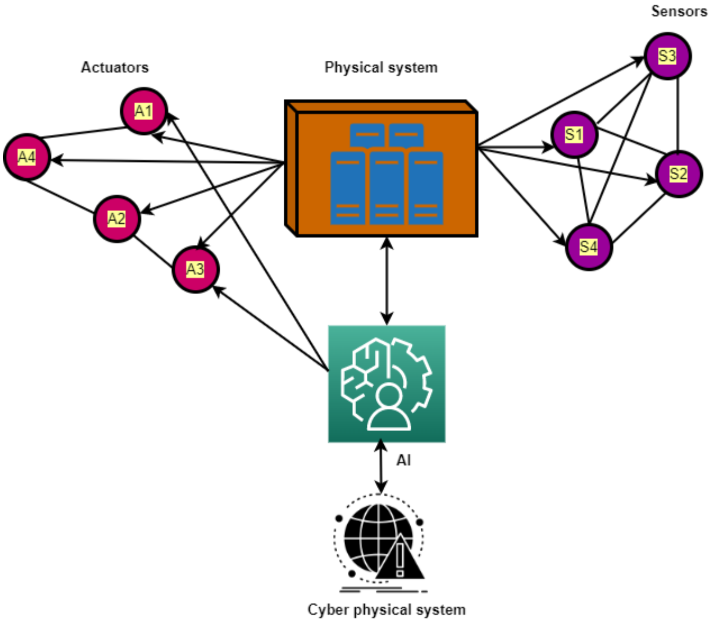

**Figure 2.** General structure of CPBS framework.

Cyber-Physical Systems consists of arithmetic, control and communication closely merged with sensory processes of different engineering domains such as physical, electronic and biological. In the proposed model, the risk means the score is primarily based on the total cost of a significant attack on a company that uses CPSs are indicated in Figure 2. It is possible to calculate the cost of operational downtime, the time spent restoring lost data and the associated financial costs. Some examples are payouts for employees, clean-up procedure expenses and the costs of abandoning facilities in cases of irreparable damage. Prices for substitutions and renovations to broken physical systems are possible. Traditional information technology (IT) structures may not have the security challenges that CPSs do. There have been several attempts at map-based solutions from other communication areas, such as sensor networks, with varying levels of success. However, as the alternatives have not been initially envisioned for CPSs, they frequently struggle to reach the system's security requirements.

Analytical approaches to current cyber-physical system (CPS) analysis are founded on principles that vary depending on whether or not safety or liveness criteria are considered. Various methods, such as stochastic modeling and contracts, are used to abstract complexity. Reinforcement learning-based procedures are necessary because of the ambiguity introduced by dispersed algorithms and AI-based methods, as well as the user's perspective or unforeseen impacts like accidents or the weather. The study contrasts the viewpoint of AI researchers on researching unknown complex systems with that of experts in the field of CPS design and prediction.

It is important to note that this guideline focuses on creating a system from the initial concept. Stepwise development and construction of new constituents is the traditional top-down approach. Therefore, it is possible to describe a system where its elements and subcomponents can be separated. Frameworks and any other existing structure that needs to be integrated are among the methods included in this scenario, referred to as a bottom-up process. Existing technologies are blended to create more complicated systems. As in Eq (3), the probability derivative processes the incoming data up to time $xs - 1$:

$$[Pd^{x-1}Q, Pd^{x-2}Q, \cdots, Pd^{0}Q]\begin{bmatrix} S_0 \\ S_1 \\ \vdots \\ S_{xs-1} \end{bmatrix}. \tag{3}$$

The physical link is established between the digital assets in the cloud, and the physical assets are $r = [Pd^{x-1}Q, Pd^{x-2}Q, \cdots, Pd^{0}Q]$, allowing data to be transferred from the cloud to both. As a result, it transfers data from the biological process to the service providers via IoT devices connected to the network. $c = \begin{bmatrix} S_0 \\ S_1 \\ \vdots \\ S_{x-1} \end{bmatrix}$.

There are several network security systems, the most common of which is the IPSS, which constantly scans a network for signs of malicious activity and records any such occurrences. For example, the IPSS may close vulnerable access points or configure firewalls to protect the network from future attacks. Employees and visitors on the network can be deterred from violating corporate security policies by using IPSS solutions to address any issues with these policies. To demonstrate that no industrial analytics applications are being developed using probability function $PdX$, a review of the papers selected for inclusion is conducted using Eq (4):

$$\begin{cases} min\, trace\ (Sn), \end{cases} \begin{cases} pdX - Pd^{T}QX & x \geq 0 \\ -Q^{T}PdX & else \end{cases} \tag{4}$$

Using a sophisticated network of methodologies and conceptions drawn from cyber-attack scenarios $(Sn)$, the researchers assessed the threat of cyber-attack on intelligent metered systems. $min\, trace\ (Sn),$ is defined as the need for data analysis in the industry grows and, with it, the realization$Pd^{T}$ that big commercial data are still in their infancy$Q^{T}$. This opened the door to a contribution that considered an architectural design that combined advanced analytics with industrial insights $x \geq 0$. Cyber-attack risk on intelligent metered systems was evaluated using a complex framework of approaches and concepts derived from cyber-attack scenarios (Sn). Mintrace (Sn) is defined as the growing need for data analysis in the growing industry. With that realization comes the realization that big commercial data are still in their infancy QT. It is allowed for a contribution considered an architectural design combining advanced analytics with industrial insights x > 0. An analysis of the included publications is performed using Eq (4) to show that no software for industrial analytics is being created that uses the probability function $P_{dX}$.

In Eq (5), the pictorial representation $g_t$ is given:

$$g_t = Pd^{T}s_0 + rc. \tag{5}$$

A row and a column of data are incoming data $r\ and\ c$. Security is referred to as initial $s_0$. The probability density function is denoted as $Pd$. Optimization software, known as CBPS-AI in Eq (5), is used to build and solve complex optimization problems that interface with numerous external corporate and non-commercial solutions. This paper's solution to semi-determined linear and nonlinear difficulties in conventional techniques uses primary-dual-path following methods. Such a method's basic premise is that iterations around a central route should be kept as short as possible to ensure that a solution is close at hand, as depicted in Figure 3.

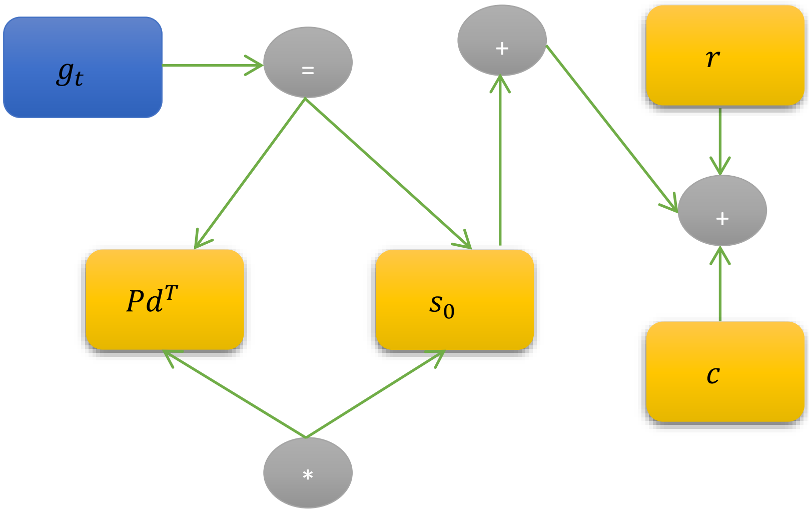

**Figure 3.** Pictorial representations of IPSS.

The network must be constantly monitored for indicators of possible infringements and threats because many access points are determined based on the Figure 3 process. Nowadays, even the most comprehensive security measures do not keep up with today's modern cyber threat. Protecting a computer network from unauthorized access is the primary goal of IPSSs to avoid an attack; these systems keep an eye on logs for any unusual activity and respond accordingly. Because they are not intended to stop seizures, intrusion detection systems keep an eye on the design and send notifications to network administrators when something suspicious is found. They terminate the connection manipulated and block the Internet protocol or user account from illegally obtaining any implementation, intended hosts or another resource provisioning.

IPSSs record data about observed events, notify security administrators of significant observed events and generate reports. Many IPSSs can react to many threats by preventing them from being accomplished. The IPSS employs various response techniques, such as halting the attack, modifying the security situation or altering the attack's substance.

Network monitoring is becoming increasingly dependent on artificial neural networks. Intrusion detection and prevention research heavily relies on artificial intelligence (AI) techniques to develop, integrate and strengthen security systems. Analyses have shown that current outlier detection systems fail to achieve satisfactory detection performance while having few false alarms. Here, the pros and cons of a neural network approach to improving false protection in intrusion detection are discussed as commercial and research tools in our proposed system CPBS-AI. By incorporating an adaptive AI system, IDS can be more adaptable to new threats. The cost of operational downtime $Odt_i$ in Eq (6) is given:

$$Odt_i(a) = ad(ms) - \sum(ms)^{1/2}.t_i(ms) \quad . \tag{6}$$

It is possible to calculate the cost in terms of operational downtime $Odt_i$, the time spent $ms$ restoring lost data $ad$ and the financial costs of the downtime $a$. $t_i$ represent the downtime rate for calculating the operational cost. A few examples include employee benefits, clean-up costs and the price of abandoning facilities due to irreparable damage $t_i$. The cost of repairing or replacing faulty physical systems is applicable in cyber threat detections and obtained using Eq (6).

The downtime's price may be estimated by adding up the time lost from regular operations (Odt i), the time spent recovering the lost data (ms) and the money lost (a). Employee benefits, clean-up expenses and the cost of abandoning facilities due to permanent damage are just a few examples. Equation 6 may be used to calculate the cost of fixing or replacing insecure physical systems.

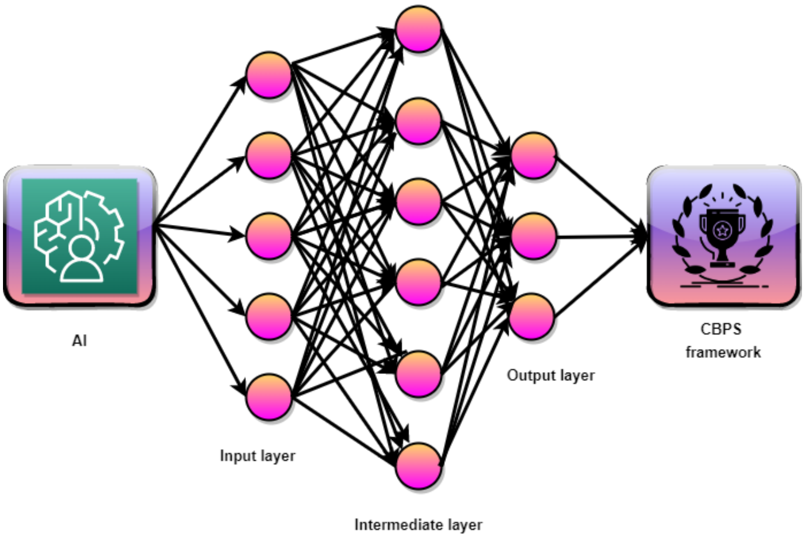

**Figure 4.** Neural network method in CBPS-AI method.

Figure 4 depicts how neural networks can be used in a cyber-physical system-based cyber security. It is an apprentice model built on the structure of a biological neural network and an algorithm based on the intrusion algorithm. The simple mental processes in this incredible image can be achieved using an AI gateway for a million light-years away. Layers "input," "intermediate" and "output" make up a neural network's overall structure. Consequently, how many neurons per layer and the total number of layers there largely depend on the system's complexity. The best network architecture must be determined. The three-layer structure of current NN architecture is the most common design choice using AI gateway.

A Neural Network (NN) models human activities in computer simulation-based cyber threats. An NN is a processing unit that has inputs and outputs. This layer's neurons receive the information from the input layer and then pass it along via weighted ties to the neurons in the topmost layer. Mathematically, the data is saved and transmitted to the next layer of neurons. The neurons in the last layer that provide the network's output are described below in Eq (7):

$$tnf_m = \sum_{n-1}^{i} icd_n \times wht_{nm} + \Delta_{wt} \;\; (m = 1,2,3 \ldots \ldots . n). \qquad (7)$$

Measurement of mass and application of equation term are used to process the incoming data $icd_n$ by hidden layer $m^{th}$ neuron from the above Eq (4). Use an accurate data transfer function $tnf_m$ and equation to communicate $wht_{nm}$ the result to the next level of neuron based weights $\Delta_{wt}$ in Eq (7) using a summation process based on certain limits $i = n - 1$. As seen in Eq (8), sigmoid functions are the most commonly used transfer function.

$$ds(x) = \frac{1}{1+e^{-sl}} + f(wht_{nm}) \tag{8}$$

As shown in Eq (8), $wt_{nm}$ the training procedure changes weights that connect each node, which iteratively alters the weight values. As a criterion for training stops, weights are changed using the steepest descent approach. The enhanced digital setting $ds(x)$ a signal $sl$ can be expressed as shown in the equation above. The parameter $f(wht_{nm})$ specifies the maximum number of times that a learning function can be transferred from $n^{th}$ output with respect to $m^{th}$ input $(wht_{nm})$. Equation (9) layer's current weight change is determined $WC$ is represented as

$$WC = \frac{1}{2}\sum_{n=1}^{i}\sum_{m=1}^{j}(wht_{nm} - wht_{nm}^{*})^{2} \, . \tag{9}$$

In Eq (9), multiple identifiers generate weight values $(wht_{nm})$ for $n = 1 \; to \; i$ and $m = 1 \; to \; j$, and the gradient descent algorithm can be implemented using summation with squared threats $(wht \; *_{nm})$ is one of the most widely used functions given in Eq (10), a layer's current weight change is determined $WC$. In Eqs (10) and (11), the parameter $d_{t-1}$ gives the data received at the $t-1$ time slot, and the variable $a_t$ denotes the current incoming data at time $t$.

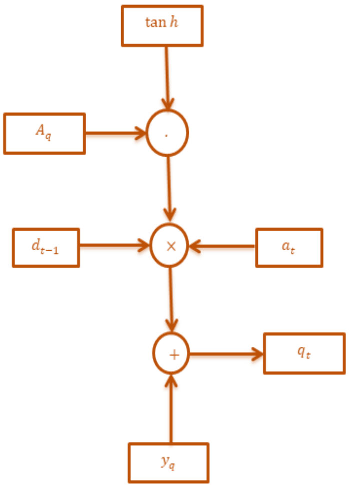

**Figure 5.** Representation of NN in CBPS-AI.

$$m_t = \rho(A_m \times (d_{t-1} \times a_t)) + y_k \tag{10}$$

$$q_t = \tan h(A_q \, . (d_{t-1} \times a_t)) + y_q \tag{11}$$

The information collected from the layer $m_t$ and the status $q_t$ are obtained from Eqs (10) and (11). $\rho$ represents the hyperbolic tangent function, and $A_m$ denotes the information generation. $a_t$ denotes the activation function. $y_k$ represents the number of service layers. $\tan h$ denotes the trigonometric function. $y_q$denotes the status of a different layer. The function $\rho(A_m \times (d_{t-1} \times a_t))$as a result, information about the layer status is generated from Eq (3). A hyperbolic tangent is then used as an activation function for the layer in Figure 5.

While simple machines can calculate much faster than neural networks, researchers are concerned that neural networks will not predict the speed at which simple machines can calculate. In the CBPS-AI system, the neural network model is nearly extinguished. Since there are many hidden layers to learning, this version focuses on a machine's output's critical significance. A wide range of information is processed by neural networks (NNs).

A variable structure control (VSC) methodology is required because of the unique characteristics of ICS. When a system changes, bias can be introduced by model-based methods, requiring the ability to respond dynamically; consequently, real-time assessment capabilities may be overlooked. Additionally, threat assessment methods must be able to quantify. CBPS-AI uses quantitative analysis to quantify risk situations into an actual specific number through contours or diagrams. Many existing ways can approximate quantitative results, such as threshold risk values. A lack of precision in risk assessment hampers a thorough defense strategy.

```
Start
Initialize network values $n, d = \{d0, d1, \ldots., dn\}, momentum\ factor\ mf, threshold\ th$;
Output parameter;
    $\boldsymbol{n} \leftarrow \boldsymbol{0}; \Delta \boldsymbol{th} \leftarrow d = \{d0, d1, \ldots., dn\}$ ;
    While $\Delta \boldsymbol{th} \leftarrow d > n$do
    $\boldsymbol{n} = \boldsymbol{n} + \boldsymbol{1}$;
        For each$d = \{d0, d1, \ldots., dn\}$;
        Re-estimate variables $mf, th$;
        End for;
    $mf \leftarrow d$;
    $n + +$;
    End;
    Return;
    Print parameter value;
Stop
```

This paper, with CBPS-AI, focuses on VCS by applying Bayesian network models with incomplete data. The above Algorithm 1 can be used to re-estimate a parameter when a new set of data d = {d0,d1,….,dn} becomes available, some of which may be partially observed. Algorithm 1 depicts a procedure that is in use while VCS is running. New security data samples are added to the parameter when they arrive with thresholds th. The current characteristics of VCS can be reflected in an improved modeling tool, which is critical for enhancing performance based on moment factor mf.

The system's industrial benchmark is introduced first. A Bayesian network value n for risk assessment is built in MATLAB to map this system. The accuracy and dynamic comparisons between the reference work and our proposed method CBPS-AI are made during our threat assessment experimentation.

Researchers conduct a risk assessment with online parameterization using the proposed method CBPS-AI based on real-time data provided by ICS in attack scenarios with missing values to evaluate the accuracy of the evaluation.

A CBPS-AI framework is been proposed in this section and tested. The simulation results for the existing and proposed CBPS-AI frameworks, such as accuracy, reliability, request time, etc., are compared with other conventional methods. According to the findings, incorporating IoT devices and an artificial intelligence model has led to better outcomes for the CBPS-AI framework.

## 4. Experimental analysis

The CICIDS2019 database has been used in the simulation to perform a suggested task. Most denial-of-service attack databases contain significant restrictions on essential data, such as erroneous duplication. In a review of more than 90 reports published between 2010 and 2020, most of them are relevant to current models, infrastructure and frameworks. Since this data is unbalanced in the first place, a duplication method is used to bring it into line to assess how well the deep learning approach is working. On the Windows 8 platform, this research is applied to the 32-bit Intel Core-i5 CPU and 16 GB of RAM using Machine Learning Packages. MATLAB 2018a is used to design machine learning algorithms.

Among the performance indicators is MATLAB, used for simulation purposes to conduct assessments of the CPBS-AI framework, including analyses of accuracy and loss and to compare the response times of various request types. For example, the suggested CBPS-AI framework's accuracy and dependability are evaluated and compared to industry standards. In the simulation, the section suggests and evaluates a CBPS-AI architecture. Accuracy, reliability, request time, etc. are only some of the simulated metrics evaluated with the current and planned CBPS-AI frameworks and more traditional approaches like AIT-SSCP, MCPSsMIS-HCPS, OLSDA and COIBD. Based on the results, the CBPS-AI architecture benefits more from using IoT devices and an AI model than before. History's many assaults have all been simulated beforehand. Based on the data in Table 3, it is clear that the CPS system can be subject to intermittent and continuous pulse attacks, depending on the transmission characteristics or disruption originating from outside the system. The suggested method employs nonlinear control and a neural network, with the latter being computed with Eq (8). Dynamic programming theory ensures reliability and resilience. The NN estimator's learning capabilities are used to make attack determinations. CPS is capable of significantly more than was previously believed; a new conceptual framework suggests that this is happening because of the availability of additional data from IoT devices.

### *4.1. Request time analysis comparison of the CPBS-AI system*

A comparison of the existing models and the CPBS-AI framework is shown in Figure (6). With a step size of 100, the number of transactions is increased from 100, and the simulation is analyzed using Eq (2). The proposed CPBS-AI framework results are compared to the results of the existing model in terms of the time it takes for the request message to reach the coordinator. Each transaction's request time rises as IoT devices become overwhelmed by the increasing volume of transactions.

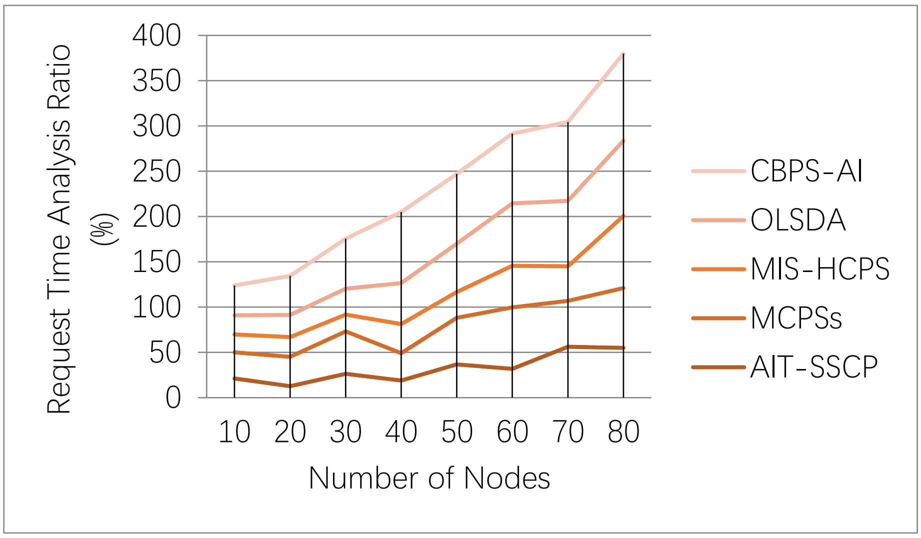

**Figure 6.** Request time analysis.

The findings of the proposed CPBS-AI framework are compared to those of the current model regarding the time it takes for the request message to reach the coordinator. As the number of requests increases, the processing time for each transaction on IoT devices increases. Since the reaction time begins to rise at a certain node, the graph is illustrated in Figure 6 with nodes numbered from 1 to 100. The reaction time of the suggested method is faster than that of the other methods.

### *4.2. Analyzing the results of a simulation*

**Table 1.** Simulation comparison.

| Method | Accuracy (%) | Loss (%) |
|---|---|---|
| AIT-SSCP | 52.3 | 64.3 |
| MCPSs | 67.1 | 57.8 |
| MIS-HCPS | 72.9 | 38.1 |
| OLSDA | 59.0 | 49.8 |
| COIBD | 64.4 | 52.7 |
| CBPS-AI | 87.8 | 24.1 |

Using the CBPS-AI framework, the simulation results are presented in Table 1. The proposed CPBS-AI framework analyses, such as accuracy and loss, are carried out using the MATLAB simulation tool. AIT-SSCP, MCPSs, MIS-HCPS, OLSDA and COIBD were used to compare the new results obtained using Eq (7). The proposed CBPS-AI framework outperforms existing models with 87.8% accuracy and 24.1% loss. The accuracy of the proposed CPBS-AI framework depends on the security aspects, reliability, vulnerability to threats and loss. The enhanced transaction level increases the transaction request time among IoT devices.

### *4.3. Assessment of the proposed CBPS-AI framework's performance*

**Table 2.** Performance assessment.

| **Method** | **Accuracy (%)** | **Reliability (%)** |
|---|---|---|
| AIT-SSCP | 52.3 | 43.2 |
| MCPSs | 67.6 | 51.6 |
| MIS-HCPS | 48.3 | 42.1 |
| OLSDA | 53.8 | 47.3 |
| COIBD | 64.0 | 38.6 |
| CBPS-AI | 92.1 | 88.1 |

Table 2 shows the performance evaluation of the proposed CBPS-AI framework. The simulation analysis of the proposed CBPS-AI framework is done with the MATLAB simulation tool. The output parameters, such as the accuracy and reliability of the proposed CBPS-AI framework, are analyzed and compared with the existing models by Eq (5). The current models fail to utilize IoT devices and machine learning procedures, resulting in abysmal performance. The proposed CBPS-AI framework with six layers with well-defined functions simplifies the operation and ensures higher performance.

The suggested CBPS-AI framework's accuracy and dependability, among other output metrics, are compared to those of existing models using analytic equation solving Eq (5). The planned output is shown in gt, a graphical representation. The results determine accuracy and dependability. The test can appropriately distinguish between sick and healthy instances, which determines accuracy. An approximate test's efficacy can be determined by counting the number of positive and negative results across all instances. Reliability in data analysis is measured total hours of operation to the total failures.

### *4.4. Reliability analysis of the CBPS-AI framework*

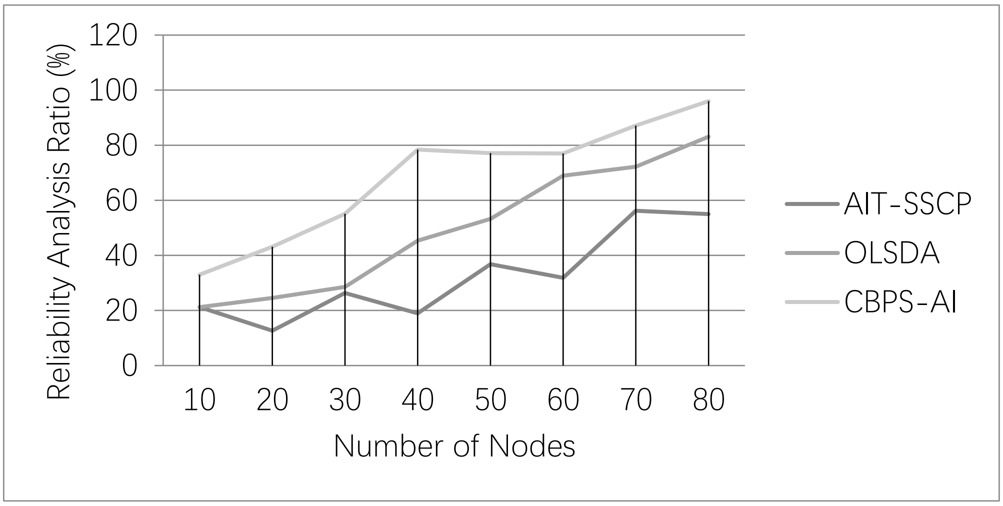

**Figure 7.** Reliability analysis.

Accuracy and reliability analyses of the CBPS-AI framework are depicted in Figure (7). This section uses the MATLAB simulation tool for existing and proposed CBPS-AI frameworks to simulate the given dataset from Eq (6). The proposed CBPS-AI framework shows more reliability than current models like AIT-SSCP, MCPSs and CBPS-AI. IoT devices and a machine learning model in the proposed CBPS-AI framework with layered architecture produce better results.

### 4.5. *Overall performance of CBPS-AI framework compared with others*

**Table 3.** Overall comparison of CBPS-AI.

| Number of Nodes | AIT-SSCP | MCPSs | MIS-HCPS | OLSDA | CBPS-AI |
|---|---|---|---|---|---|
| 10 | 21.21 | 28.76 | 19.78 | 21.21 | 32.98 |
| 20 | 12.65 | 32.45 | 21.78 | 24.54 | 43.12 |
| 30 | 26.33 | 46.76 | 18.65 | 28.56 | 55.13 |
| 40 | 18.98 | 30.12 | 32.15 | 45.36 | 78.43 |
| 50 | 36.78 | 51.34 | 28.56 | 53.26 | 77.11 |
| 60 | 31.87 | 67.87 | 45.89 | 68.92 | 77.02 |
| 70 | 56.21 | 50.65 | 38.27 | 72.18 | 87.15 |
| 80 | 54.98 | 66.01 | 79.76 | 83.10 | 96.01 |

The proposed CBPS-AI framework achieves effectiveness of 96.01%. The number of nodes used is set as 80. The implementation is carried out only for 80 nodes. Future work can be implemented with more nodes to achieve more system effectiveness. It is shown in Table 3 that different dynamic functions and disturbances from external sources can affect the CPS system in two different ways: a continuous and a non-continuous pulse attack. Nonlinear regulation and a neural network are employed in the proposed strategy and are calculated using Eq (8). Reliability and robustness are ensured by using nonlinear control theory. Attack determination is based on the NN estimator's ability to learn. CPS is skillful at far more than previously thought; according to a new conceptual framework, CPS is becoming more computer-controlled due to the availability of new data from IoT devices.

A CBPS-AI framework has been proposed in this section and tested. The simulation results for the existing and proposed CBPS-AI frameworks, such as accuracy, reliability, request time, etc., are compared with other conventional methods, AIT-SSCP, MCPSs, MIS-HCPS, OLSDA and COIBD. According to the findings, incorporating IoT devices and an artificial intelligence model has led to better outcomes for the CBPS-AI framework. The simulation results of the proposed framework are compared with the existing methods discussed in the related work section. The comparison is made with artificial intelligence (AI) techniques for safeguarding SC privacy (AIT-SSCP) [25], Medical Cyber-Physical Systems (MCPSs) [26], Machine Intelligence Symbiotically Human Cyber-Physical System (MIS-HCPS) framework [27], On assess large-scale data architecture [OLSDA] [28], cognitive-based IoT Big-Data (COIBD) [29]. The proposed CPBS-AI framework is evaluated based on the request time analysis, loss, accuracy, effectiveness and reliability.

Manipulation of data channels, equipment details and virtualization software are just a few of the vulnerabilities that have arisen due to the increasing interconnectedness of the Internet of Things (IoT) and Cyber-Physical Systems (CPSs). The research presents an AI-driven architecture for hybrid Cyber-Physical Business Systems (CPBS-AI). Several safety threats at various CPS levels are outlined, along with their respective threat models and the scientific obstacles that must be overcome to develop appropriate security solutions. Connecting several CPSs to carry out independent duties in a confined space is a potential future scope for this new technology advancement. The proposed CPBS-AI, which has an overall effectiveness of 96.01%, implements artificial intelligence as a key tool to boost the integration of CPSs in a smart system that requires little manual effort.

## 5. Conclusions

Various CPS layers and their correlating models are briefly reviewed in this research to highlight developing secure CPS research problems. Neural networks examined here are to overcome the current limitations of the most cutting-edge static and adaptable detection and protection techniques and the technologies' current state of development. This paper proposes a conceptual framework for further research for CPBS-AI (cyber-physical business systems based on artificial intelligence). Several typical CPS layer threats and outstanding research issues in developing intelligent CPS security precautions are demonstrated by AI-based security approaches, in the end, using intrusion prevention security systems. Aside from that, the proposed work provides a glimpse into CPS safety research's future and relevance, motivating evaluations of research issues. Using intelligent nonlinear system control, here is presented a new approach to estimating and compensating attacks launched by a forward link of nonlinear CPSs. Neural networks are combined with nonlinear control in the proposed method. It is evident from this review that cyber-physical systems are on the verge of a complex program because all the necessary technology is already in place. This new technological revolution's challenges include connecting multiple CPSs to perform autonomous tasks in a compact environment, which is a future scope. Artificial intelligence is highlighted as a critical tool to increase the incorporation of CPSs in an intelligent system that requires little human effort, as implemented in our CPBS-AI with an overall performance of 96.01%. The proposed method evaluates the overall effectiveness, accuracy and loss in the form of security analysis and confidentiality. Future work can be implemented with more nodes to achieve more system effectiveness in detecting the threats and attacks related to security and confidentiality issues.

## Acknowledgments

Sunil Kumar Sharma extends their appreciation to the deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through project number (IFP-2020-130).

## Conflicts of interest

The authors declare no conflicts of interest.

## References

1. S. Walker-Roberts, M. Hammoudeh, O. Aldabbas, M. Aydin, A. Dehghantanha, Threats on the horizon: Understanding security threats in the era of cyber-physical systems, *J. Supercomput.*, **76** (2020), 2643–2664. https://doi.org/10.1007/s11227-019-03028-9
2. J. Yaacoub, O. Salman, H. Noura, N. Kaaniche, A. Chehab, M. Malli, Cyber-physical systems security: Limitations, issues and future trends, *Microprocess. Microsyst.*, **77** (2020), 103201. http://dx.doi.org/10.1016/j.micpro.2020.103201
3. M. Keshk, E. Sitnikova, N. Moustafa, J. Hu, I. Khalil, An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems, *IEEE Trans. Sustainable Comput.*, **6** (2020), 66–79. https://doi.org/10.1109/TSUSC.2019.2906657
4. N. Guzman, M. Wied, I. Kozine, M. Lundteigen, Conceptualizing the critical features of cyber-physical systems in a multi‐layered representation for safety and security analysis, *Syst. Eng.*, **23** (2020), 189–210. https://doi.org/10.1002/sys.21509
5. T. Wang, Y. Liang, Y. Yang, G. Xu, H. Peng, A. Liu, et al., An intelligent edge-computing-based method to counter coupling problems in cyber-physical systems, *IEEE Network*, **34** (2020), 16–22. https://doi.org/10.1109/MNET.011.1900251
6. A. Khalid, P. Kirisci, Z. Khan, Z. Ghrairi, K. Thoben, J. Pannek, Security framework for industrial collaborative robotic cyber-physical systems, *Comput. Ind.*, **97** (2018), 132–145. https://doi.org/10.1016/j.compind.2018.02.009
7. B. Li, Y. Wu, J. Song, R. Lu, T. Li, L. Zhao, DeepFed: Federated deep learning for intrusion detection in industrial Cyber-Physical systems, *IEEE Trans. Ind. Inf.*, **17** (2020), 5615–5624. https://doi.org/10.1109/TII.2020.3023430
8. D. Ye, T. Zhang, G. Guo, Stochastic coding detection scheme in cyber-physical systems against replay attack, *Inf. Sci.*, **481** (2019), 432–444. https://doi.org/10.1016/j.ins.2018.12.091
9. H. Kholidy, Autonomous mitigation of cyber risks in the Cyber-Physical Systems, *Future Gener. Comput. Syst.*, **115** (2021), 171–187. https://doi.org/10.1016/j.future.2020.09.002
10. P. Radanliev, D. D. Roure, M. V. Kleek, O. Santos, U. Ani, Artificial intelligence in cyber-physical systems, *AI Society*, **36** (2021), 783–796. https://doi.org/10.1007/s00146-020-01049-0
11. M. Mahmoud, M. Hamdan, U. Baroudi, Modeling and control of cyber-physical systems subject to cyberattacks: A survey of recent advances and challenges, *Neurocomputing*, **338** (2019) 101–115. https://doi.org/10.1016/j.neucom.2019.01.099
12. S. Chaudhry, T. Shon, F. Al-Turjman, M. Alsharif, Correcting design flaws: An improved and cloud-assisted key agreement scheme in cyber-physical systems, *Comput. Commun.*, **153** (2020), 527–537. https://doi.org/10.1016/j.comcom.2020.02.025
13. Z. Lv, D. Chen, R. Lou, A. Alazab, Artificial intelligence for securing industrial-based cyber-physical systems, *Future Gener. Comput. Syst.*, **117** (2021) 291–298. https://doi.org/10.1016/j.future.2020.12.001
14. C. Alippi, S. Ozawa, Computational intelligence in the time of cyber-physical systems and the internet of things, *Artif. Intell. Age Neural Networks Brain Comput.*, (2019), 245–263. https://doi.org/10.1016/B978-0-12-815480-9.00012-8
15. A. Nazerdeylami, B. Majidi, A. Movaghar, Autonomous litter surveying and human activity monitoring for governance intelligence in coastal eco-cyber-physical systems, *Ocean Coastal Manage.*, **200** (2021), 105478. https://doi.org/10.1016/j.ocecoaman.2020.105478

16. P. Radanliev, D. Roure, R. Nicolescu, M. Huth, O. Santos, Digital twins: artificial intelligence and the IoT cyber-physical systems in Industry 4.0, *Int. J. Intell. Rob. Appl.*, **6** (2022), 171–185. https://doi.org/10.1007/s41315-021-00180-5
17. S. Shaw, Z. Rowland, V. Machova, Internet of Things smart devices, sustainable industrial big data, and artificial intelligence-based decision-making algorithms in cyber-physical system-based manufacturing, *Econom., Manage. Financ. Mark.*, **16** (2021), 106–116. https://doi.org/10.22381/emfm16220217
18. S. Mihalache, E. Pricop, J. Fattahi, Resilience enhancement of cyber-physical systems: A review, *Power Syst. Resilience*, (2019), 269–287. https://doi.org/10.1007/978-3-319-94442-5_11
19. R. Verma, Smart city healthcare Cyber-Physical system: Characteristics, technologies and challenges. *Wireless Pers. Commun.*, **122** (2022), 1413–1433. https://doi.org/10.1007/s11277-021-08955-6
20. R. Davidson, Cyber-physical production networks, artificial intelligence-based decision-making algorithms, and big data-driven innovation in Industry 4.0-based manufacturing systems, *Econom., Manage., Financ. Mark.*, **15** (2020) 16–22. http://dx.doi.org/10.22381/EMFM15320202
21. M. Yildirim, Artificial intelligence-based solutions for cyber security pproblems, in *Artificial Intelligence Paradigms for Smart Cyber-Physical System*, (2021), 68–86. https://doi.org/10.4018/978-1-7998-5101-1.ch004
22. N. Naik, P. Nuzzo, Robustness contracts for scalable verification of neural network-enabled cyber-physical systems, in *2020 18th ACM-IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE)*, (2020), 1–12, http://dx.doi.org/10.1109/MEMOCODE51338.2020.9315118
23. A. Lavaei, B. Zhong, M. Caccamo, M. Zamani, Towards trustworthy AI: Safe-visor architecture for uncertified controllers in stochastic cyber-physical systems, in *Proceedings of the Workshop on Computation-Aware Algorithmic Design for Cyber-Physical Systems*, (2021), 7–8. https://doi.org/10.1145/3457335.3461705
24. S. Mazumder, J. Enslin, F. Blaabjerg, Guest Editorial: Special Issue on Sustainable Energy Through Power-Electronic Innovations in Cyber-Physical Systems, *IEEE J. Emerging Sel. Top. Power*, **9** (2021), 5142–5145. https://doi.org/10.1109/JESTPE.2021.3109578
25. J. Fitzgerald, P. Larsen, K. Pierce, Multi-modelling and co-simulation in the engineering of cyber-physical systems: towards the digital twin, *From Software Engineering to Formal Methods and Tools, and Back. Lecture Notes in Computer Science*, In: ter Beek, M., Fantechi, A., Semini, L. (eds), https://doi.org/10.1007/978-3-030-30985-5_4
26. G. Popescu, S. Petreanu, B. Alexandru, H. Corpodean, Internet of Things-based real-time production logistics, cyber-physical process monitoring systems, and industrial artificial intelligence in sustainable smart manufacturing, *J. Self-Governance Manage. Econom.*, **9** (2021), 52–62. https://doi.org/10.22381/jsme9220215
27. T. Agarwal, P. Niknejad, A. Rahimnejad, M. Barzegaran, L. Vanfretti, Cyber-physical microgrid components fault prognosis using electromagnetic sensors, *IET Cyber-Phys. Syst.: Theor. Appl.*, **4** (2019),173–178. https://doi.org/10.1049/iet-cps.2018.5043
28. A. AlZubi, M. Al-Maitah, A. Alarifi, Cyber-attack detection in healthcare using cyber-physical systems and machine learning techniques. *Soft Comput.*, **25** (2021), 12319–12332. https://doi.org/10.1007/s00500-021-05926-8

29. P. Durana, N. Perkins, K. Valaskova, Artificial intelligence data-driven internet of things systems, real-time advanced analytics, and cyber-physical production networks in sustainable smart manufacturing, *Econ. Manag. Finance. Mark.*, **16** (2021), 20–30. https://doi.org/10.22381/emfm16120212.
30. Z. Jadidi, S. Pal, N. Nayak, A. Selvakkumar, C. Chang, M. Beheshti et al., Security of machine learning-based anomaly detection in cyber physical systems, in *2022 International Conference on Computer Communications and Networks (ICCCN)*, (2022), 1–7. https://doi.org/10.1109/ICCCN54977.2022.9868845
31. E. Veith, L. Fischer, M. Tröschel, A. Niebe, Analyzing cyber-physical systems from the perspective of artificial intelligence, in *Proceedings of the 2019 International Conference on Artificial Intelligence*, (2019), 85–95. https://doi.org/10.1145/3388218.3388222
32. A. Hussaini, C. Qian, W. Liao, W. Yu, A taxonomy of security and defense mechanisms in digital twins-based cyber-physical systems, in *2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, (2022), 597–604. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics55523.2022.00112
33. S. Latif, F. Wen, C. Iwendi, F. li, S. Mohsin, Z. Han, S. Band, AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems, *Comput. Commun.*, **181** (2022), 274–283. https://doi.org/10.1016/j.comcom.2021.09.029
34. A. Gurjanov, V. Babenkov, I. Zharinov, O. Zharinov, Cyber-physical systems control principles and congregation of resources for a centralized and decentralized artificial intelligence, in *Journal of Physics: Conference Series*, **2373** (2022), 062017. https://doi.org/10.1088/1742-6596/2373/6/062017
35. A. Roy, R. Bose, J. Bhaduri, A fast accurate fine-grain object detection model based on YOLOv4 deep neural network. *Neural Comput. Appl.*, **34** (2022), 3895–3921. https://doi.org/10.1007/s00521-021-06651-x
36. A. Roy, J. Bhaduri, T. Kumar, K. Raj, WilDect-YOLO: An efficient and robust computer vision-based accurate object localization model for automated endangered wildlife detection. *Ecol. Inf.*, (2022), 101919. https://doi.org/10.1016/j.ecoinf.2022.101919
37. A. Chandio, G. Gui, T. Kumar, I. Ullah, R. Ranjbarzadeh, A. M. Roy, et al., Precise single-stage detector, preprint, arXiv:2210.04252. https://doi.org/10.48550/arXiv.2210.04252

AIMS Press

©2023 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0).