I.J. Wireless and Microwave Technologies, **2022, 5, 53-73**
Published Online on October 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2022.05.06

Attacks on Cyber Physical System: Comprehensive Review and Challenges

Maloth Sagar
School of Information Technology and Engineering, Vellore Institute of Technology (VIT UNIVERSITY), Vellore, TamilNadu, India-632014
Email: maloth.sagar2019@vitstudent.ac.in

Vanmathi C.
School of Information Technology and Engineering, Vellore Institute of Technology (VIT UNIVERSITY), Vellore, TamilNadu, India-632014
Email: vanmathi.c@vit.ac.in

Received: 08 April 2022; Accepted: 25 May 2022; Published: 08 October 2022

Abstract: CPS is often comprised of several networked systems that could really observe as well as modify real-world objects and operations. They're analogous with IoT systems, and that therefore CPS concentrates mostly on interplay of mechanical, communications, as well as compute operations. As a result of their connection with IoT, a truly innovative CPS element, the "Internet of Cyber-Physical Things (IoCPT)", has been established. The speedy pace and substantial development of CPS does have a consequence upon several parts of people's lives and permits a plethora of services and applications, including such e-Health, home automation, and e-Commerce. Interlinking the physical and virtual realms, on the other hand, poses additional security risks. As a necessary consequence, CPS cyber-security increasingly piqued the interest of both academics as well as corporations. In this research work, a literature review has been undergone in terms of cyber security in cyber physical systems. All the literature papers on cyber security have been collected from standard journals like IEEE, Springer and Elsevier. The collected papers are analyzed in diverse aspects like application, dataset used, technique utilized, tool and performance recorded. Finally, the research gaps identified is manifested to guide the future researchers on intrusion detection in CPS.

Index Terms: Cyber-Physical System Security, Attack types, Performance analysis, DOS, Smart Grids, Intrusion Detection, Threats, vulnerabilities.

1. Introduction

Technology's pervasiveness has risen to unprecedented heights in recent decades, and it will soon start in a domino effect. Technology can be found in practically every sector. The innovative new Cyber-Physical Connection seems to be a combination of the related to cyberworlds joined by a core network for connectivity and feedback loops. The CPS model is shown in Fig.1 and the general architecture of CPS is manifested in Fig.2.

Nomenclature

Abbreviation	Description
FOF-PID	Fractional order fuzzy-proportional-integral-derivative
ADDS	Attack design designation system
MCPS	Medical cyber-physical systems
CPS	Cyber-physical systems
SDN	Software-defined networking
FO-PID	Fractional Order-PID
CPEMS	Cyber-physical energy management system
LDTV	Linear discontinuous time-varying
CA-PAIN	Context-aware parameter-invariant

QC	Quality control
IDS	intrusion detection system
CPPS	Cyber-Physical Production Systems
BBFO	binary bacterial foraging optimization
GRU	Gated Recurrent Unit

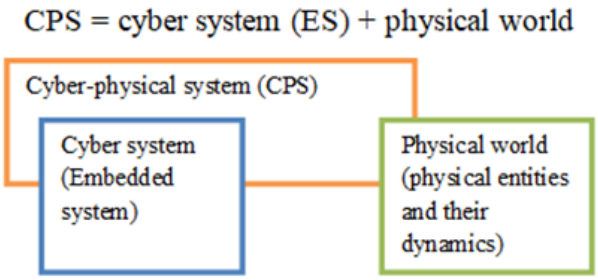

Fig.1. CPS model

With the development of supporting technologies such as sensing devices, Cloud, and IoT Technology, the Age of the internet has empowered the physical universe (such as sensing devices in diagnostic instruments, agriculture, and other fields) to link with cybersecurity [1,2,3][47-48]. The state-of-the-art IoT technology had already emerged as a consequence of a tremendous amount of time and effort injected into IoT, as well as various de facto standards exist on the bundle for implementation. Industry 4.0 integrated combined Connected devices, business networks, and industrial automation architecture inside the business with the introduction of Connected devices [3,4,5,6] [49,50,51]. Commonly used terms have become sentient and communicative due to the IoT. Any technology that involves interaction amongst network components has always had a network infrastructure as just an integrated element.

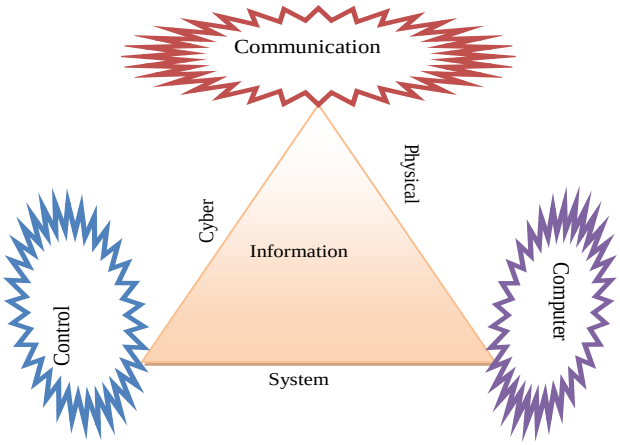

Fig.2. CPS Architecture: A general framework

Information packets within digital packets may mostly go throughout the country due to the transport and control protocols within gateways. Despite the widespread adoption of traditional embedded networking devices with closely connected control and data, conventional networking hardware is complicated, poorer persistent, and difficult to administer. By delivering cost-effective and smart infrastructure services towards the distribution network of technology [5,6], SDN [4], [52,53] has proven to be the backbone. The data and control planes are divided into two distinctly separate entities, and the control plane is moved to centralised controllers. Configuration management and performance monitoring are made easier with the new design. The SDN architecture has provided customers with the ability to programme gadgets via centralised controllers, as well as control over the underpinning network's large picture, easier deployment, and lower costs. "Cyber World" is yet another important part of the Cyber-Physical System.

Cyber Realm has been built on the foundation of cloud computing. Cloud computing, which has its origins in the 1960s whenever the notion of providing computers as a utility seems to have been created, has only recently gained traction and widespread usage. The confluence of computer capability, communication devices, and World Wide Web usage has been proven in cloud computing. Cloud computing had already come to prominence because of features including such "pay-as-you-go," flexible resources (e.g., Amazon's EC2 instances), extensive internet connectivity, and sharing resources. The whole environment recognized as CPS is indeed the result of the integration of the physical surroundings, cyberspace networks, and the current digital era [54,55],[46]. A Cyber-Physical Loop has always been

made up of processing, transmission, and control components, as well as a feedback mechanism. The merging of SDN throughout the communication layer changes a "Cyber-Physical System (CPS)" into an SD-CPS, which does have a significant impact on that information world. CPS' essential features include (a) improved networking techniques for integrating the cyber and physical worlds, (b) smart data handling, and cognitive technologies.

Cloud computing services are being swamped with huge spatial information as even more web gadgets connect to cloud-based services. Although cloud infrastructure offers a lot of computational power as well as a lot of space for information, it brings delay towards the network edge. Between the observation layer as well as the cloud layer, Fog Computing [13] establishes a layer of dispersed processing and memory assets that delivers cloud-like support or assistance end devices. Fog Computing offers network bandwidth preservation, reduction in costs, accelerated reaction speed, mobility management, and increased protection near the network edge through minimising network traffic travelling towards the cloud [14], [57,58,59]. "Everything has a price," as even the saying goes, the same would be applicable to technological modernization. On the one hand, technology has made a significant contribution to contemporary life; the rise, as well as the ubiquity of services, has increased the number of security concerns and difficulties for the innovative period. "Distributed Denial of Service (DDoS)" assaults are by far the most damaging threats to national security because they degrade availability and reliability [60,61].

The CPS is vulnerable to security breaches in diverse applications. Unfortunately, the ubiquitous utilization of CPS presents a series of potential threats that might result in significant destruction to the regulated physical items as well as damage to the people who depend on these completely. NIDS must always be installed on these kinds of systems in order to capture preventative measures before irreparable damage is caused by such assaults. Regardless of the fact that network management has long been widely utilized for cyber security, investigations, and other purposes, technological improvements have introduced a slew of new problems [2].

CPSs have a variety of major weaknesses where cyber-physical attack vulnerability penetrates, resulting in security vulnerabilities to controlling networks' dependability and robustness [4]. In today's environment, as the number of devices targeted during information flow grows, cyber-physical security system requires extra work [5]. CPS cybersecurity faces issues like trustworthiness, authenticity, validity, and confidentiality. As a result of the potential for cyber assaults, the system's ability to supply services is jeopardized, and security constraints play a significant role.

i. Confidentiality: A condition of confidentiality is obtained in CPS under various attacks by a system that is capable of detecting prevented users or intruders [26].
ii. Integrity: Information travelling from the local record system to a data center over the network may be tampered with as a result of a cyber assault. While information goes across numerous hardware devices, the integrity of CPS may be maintained by using a robust firewall mechanism to prevent unauthorized users or intruders [27].
iii. Availability: CPSs are highly structured sophisticated power systems that provide nonstop services to their clients and have mechanisms in place to prevent power outages. The Markov mechanism [28] presents a multi-cyber architecture to improve the availability of CPS.
iv. Dependability: CPS reliability is critical for the correct operation of the CPS environment. When examining the impact of unauthorized users, the reliability of such systems is critical.
v. A Stochastic Petri nets technique to monitoring services delivered by sensors and actuators during procedure execution may be used to assess the likelihood of CPS [29].
vi. Robustness: The accessibility of CPS to a particular stage allows appropriate operation of the entire system, which determines the level of robustness. Mathis proposes a rule-based resilience mechanism in terms of CPS durability for incorrectly entered parameters [30].
vii. Reliable: The reliability of such devices is determined by system tasks that correctly react to service under environmental and operational circumstances specified by the system controller or programmer, or over a certain time frame [31].

Jamming attacks, subtle deception assaults, eavesdropping attacks, and replay attacks are only some of the cyber threats that can compromise integrity and secrecy. As a result, cyber-physical attacks frequently target data confidentiality and integrity. CPSs have a variety of weak points where cyber-physical attack vulnerability compromises, resulting in security breaches to control system dependability and robustness [4]. In today's environment, the security cyber-physical systems need extra work since a growing number of devices are targeted during information transit [5]. The study of possible CPSs attacks mention here to overcome issue related to it is given [7] [9].

i. Eavesdropping: Eavesdropping comes the from gentle assault category. It means that any invader can take personal information without actively participating, but just by studying present situations, according to CPS. Such attacks are capable of obtaining data transmission over channels and producing an adversarial effect.
ii. DoS Attack: In the event of a DoS attack, the system will be pummeling with many hits, causing the system to become unstable. Attackers send fraudulent messages through flaws, disrupting the regular working of the network effect and bringing the entire network down. It also prevents forward and backward movement.

iii. Stealthy Deception Attack: This is a dynamic attack in which the intruder changes numerous control settings that can be monitored or not by the system application. Such attacks arose when the security of actuators and sensors deteriorated

Table 1. Network layers and Attack types

Network Layers	Attacks
Application Layer (Network process to Application)	Exploit user id and password
Presentation Layer (Data Presentation and Encryption)	Phishing/TLS Sniffing
Session Layer (Inter host communication)	Hijacking/FTP sniffing
Transportation Layer (End-to-End Connection)	DOS/TCP session sniffing
Network Layer (Path Determination)	Man-in-the-Middle IP/Port Sniffing
Data Link Layer (Physical Addressing)	Spoofing MAC/ARP Sniffing
Physical Layer (Binary Transmission)	Sniffing

Table1 show the number of layers present in the network and attacks that occurs in each of the layers.

iv. Jamming Attack: This type of attack occurs when an intruder jams the communication network, preventing packets from being sent and received between sensor and signal converting equipment.
v. Compromised-Key Attack (CKA): In a CKA, the attacker attempts to gain complete control of a secure channel in order to figure out and modify sensitive information by manipulating keys in order to identify other keys that will allow the attacker to create a suitable environment.
vi. Man-in-the-Middle Attack: In these attacks, corrupt packets are received by the programmer, who must determine if the packets are secure or not.

The major contribution of this literature work is:

- ✓ This study gathers various research papers on cyber-physical systems security described in depth.
- ✓ Each of the collected research works has been analyzed in different aspects like application, type of attacks, datasets collected, and techniques used for attack detection.
- ✓ The performance of the research papers is identified and it is tabulated.
- ✓ The recent research gaps identified in cyber security in cyber-physical systems are addressed, and this will be a milestone for future researchers.

The flow of the paper is structured as follows: Section 2 addresses recent work on CPS security, and Section 3 examines the study findings. In addition, in section 4, the research gaps and problems are explored. Section 5 brings the paper to a conclusion.

2. Problem Formulation and Motivation

A. Problem formulation

CPS systems, notwithstanding their obvious advantages, remain vulnerable to a variety of cyberspace and/or physical security risks, assaults, as well as obstacles. Their diverse character, dependence on sensitive and private data, and large-scale implementation all contribute to something like this. As a consequence, purposeful or unintentional breaches of the technologies might have disastrous consequences, necessitating the implementation of strong security precautions. This, nevertheless, might result in unacceptably high network overhead, significantly in relation of delay [66,67]. Continuous software, program, and operating system upgrades also should help to reduce zero-day flaws.

B. Motivation

CPS processes have indeed been assimilated into infrastructure systems (energy infrastructure, manufacturers, supply - chain management, medical services, armed services, agricultural production, and so on), attempting to make them a desirable pinpoint for network threats for just a variety of reasons, including financial, criminal, security apparatus, spying, diplomatic, and terrorist activities. As a result, any CPS flaw could be used to launch deadly attacks against such systems. Transparency, authenticity, and scalability are examples of security features that might be attacked.

3. Literature Review on Cyber Security in CPS

Technology is rapidly changing, and it is rapidly getting a footing in people's hearts. When internet-connected devices, for example, interact with other devices, they create a vast system that solves complex problems and makes people's lives easier and longer. One of the most significant and well-known technical revolutions is the "Cyber-Physical System". CPSs are systems or mechanisms that can be controlled and monitored from a distance. The CPS system uses the Internet to link other systems and people (by computer-based algorithms). In 2010, the viral assault "Stuxnet" attacked nuclear facilities in Iran. Furthermore, an attacker can remotely operate medical equipment, affecting the health of patients (as well as leaking sensitive information about patients and hospital employees). Such major problems are raised in this essay, which uses machine learning and cyber security on a regular (or alternate) basis. Maintaining such a system is a challenging effort, but if we succeed, we will save a lot of energy and avoid unwanted assaults, among other things. An illustration of the CPS- security field is manifested in Fig.3.

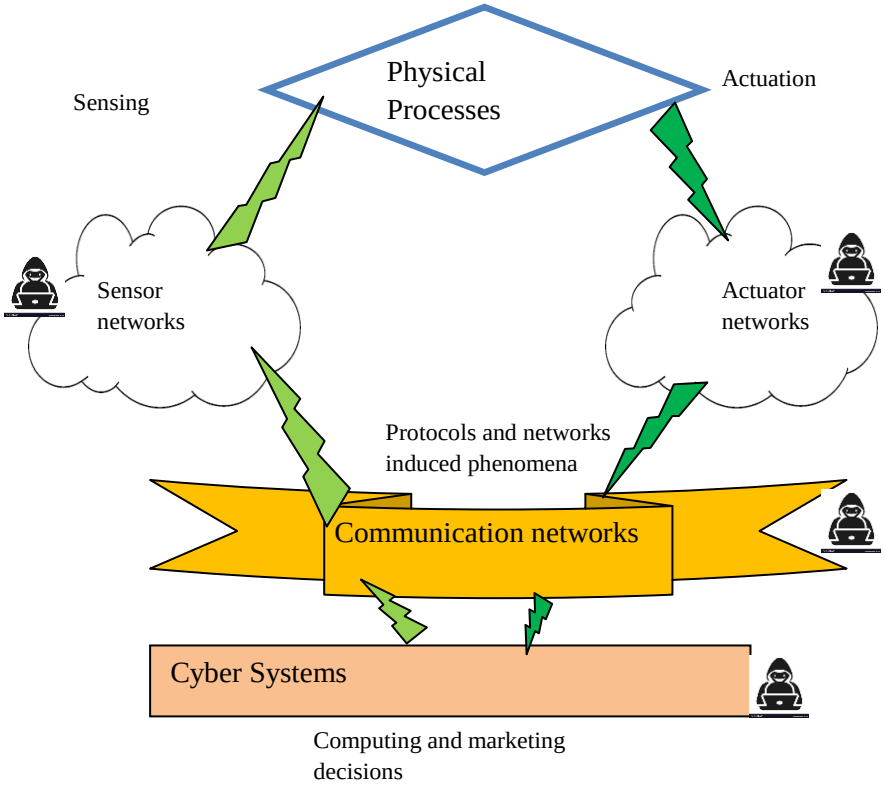

Fig. 3. CPS Security

In 2015, Vellaithurai *et al.* [1] developed a security-oriented probabilistic risk assessment approach referred to as CPINDEX for “cyber-physical security indices” towards assessing the underlying cyber-physical environment's security posture. On a particular host machine, CPINDEX deploys necessary cyber-side monitoring devices to proactively record and characterize low-level system operations including inter-process interactions across operational system assets. CPINDEX develops “stochastic Bayesian network models” integrity of the entire cyber-physical architecture using the produced records as well as geometric data about the electricity supply design, and updates them continuously depending on the latest condition of the underpinning electricity system.

In 2018, Bernieri *et al.* [2] introduced a modular approach for industrial control systems to provide cyber-physical security. The Deep Detection Architecture (DDA) was developed to bridge the barrier between computer science and control theory. Furthermore, as a baseline for validation, they provided a new cyber-physical simulation technique.

In 2017, Haller *et al.* [3] presented an approach to developing intrusion detection systems (IDS) in cyber and physical systems. The method uses a three-phase design technique that includes risk assessment, cross-association, and optimum IDS architecture to cut the volume of monitored data. Phase 1 employs sensitivity analysis in order to identify sensitive parameters to intervention programs (e.g., control signals and cyber-attacks), phase 2 employs cross-association evaluation to ideally construct the processing parameters in clusters that are the most sympathetic to organizations of initiatives, and phase 3 consists of assigning the most vulnerable processing parameters to IDS while attempting to enforce the IDS inherent limitations as well as availability prerequisites.

In 2017, Bezemskij *et al.* [4] developed a Bayesian Networks-based technique for determining how an automatic car is now under threat, and whether the assault occurred in the cyber or materialistic worldview. On such a remotely

operated vehicle developed in line with the "Generic Vehicle Architecture" standard and outfitted with such a lot of famous networking and sensor technologies, they show the practicality of the technique. Investigations with command injection, malicious nodes, and electromagnetic resonance assaults have shown that the method is effective. In 2021, Xiao *et al.* [5] have developed a "software-defined network paradigm" into CPS design to simplify CPS administration and find a resolution to networking cyber security threats. The suggested method is evaluated by employing the constructed information as well as the NSL-KDD dataset's 7 features set. It has also been proven to be successful, with accuracy rates of 99.4% and 75.44%, respectively.

In 2017, Heussen *et al.* [6] developed a novel work based on the cyber-physical intrusion detection mechanism, and it is based on field data. This demonstrates how to identify distinctive responding patterns or how to keep the characterization up-to-date. Furthermore, as a component of a cyber-physical invasion security mechanism, researchers suggest a way to use this behaviours patterns characterization to identify abnormal and possibly hazardous activity alterations. In 2019, Chavez *et al.* [7] have projected a hybrid IDS approach for distributed energy resources (DER) structures that supervise and assess both physical and cyber network information. The designers show how their approach enables the cyber-physical IDS to accomplish extra comprehensive detection and response of malicious occurrences on the DER framework through a sequence of circumstances.

In 2013, Mitchell *et al.* [8] developed a new approach for "intrusion detection and response" on CPS. based on stochastic Petri nets, they created a probabilistic model to characterize the CPS behaviour under the presence of malicious nodes. It shows a variety of attacker behaviours, as well as an "intrusion detection and response system (IDRS)" enabling responding effectively to malevolent events in real-time. These findings show that altering vulnerability management intensity in accordance with the intensity and behaviour of the intruder may greatly increase the CPS's dependability.

In 2016, Mitchell *et al.* [9] created a mathematical framework for CPS based on "stochastic Petri nets" to represent the interplay underlying adversary conduct as well as protection. They discuss numerous sorts of malfunction or failure in such a cyber-physical, notably attrition loss, pervasion inability, and information gathering breakdown. They demonstrate the conceptualization methodology using a modernized electricity infrastructure as an illustration. These findings highlight the optimized design characteristics for the modernized electricity grid's median time to failures, such as the intrusion prevention interval and redundancies level. Whenever implementing redundancies to increase overall system resilience, there is indeed an architectural tradeoff between information gathering loss, attrition inability, and posterior distribution failure. In 2019, Schnabel *et al.* [10] to investigate the "physical, communication, and computing components" of medical devices in order to improve the quality and dependability of healthcare systems, have created a novel IDS for MCPS. They looked at the issue of feature selection in MCPS. Our first findings show that Laplacian scoring algorithms are effective in optimizing feature selection while consuming less memory.

In 2018, Loukas *et al.* [11] proved the feasibility and advantages of using deep learning to outsource the concerted efforts of vulnerability scanning. This scheme yields pinpoint efficiency considerably faster reliably than conventional machine learning approaches, but it is not confined to a specific sort of threat or the in-vehicle CAN connection, as past research has been. It incorporates real-time data from both "cyber and physical processes" as information, which is what it integrates into a neural network architecture as time-series data. They employ both a "deep multi-layer perceptron" and a "recurrent neural architecture", with the latter benefiting from a hidden layer with such a long-short term memory, which would be particularly effective for understanding the information of various assaults. In 2019, Zhang *et al.* [12] presented a dynamic security control scheme centred on cryptographic algorithms based on the current security needs of the "industrial control system" and the technological factors of contemporary protective actions. The approach proposes a solution to Industrial Cyber-Physical System information security. It also provides a linkage verification mechanism between the industrial automation system's internal fire suppression fence, intruder detector, and trustworthy link site.

In 2020, Roberts *et al.* [13] through observing the physical phenomena of the grids, the technique outlined herein advances the notion of a standard intrusion detection system throughout power systems, especially power transmission systems. This is accomplished by using high-rate distribution "Phasor Measurement Units (PMUs)" in conjunction with SCADA packet analysis to analyze discrete control device behaviour. Researchers offer a collection of techniques for understanding the control algorithm of "voltage regulators and switched capacitor banks" automatically in this research. In 2020, Pinto *et al.* [14] provided an IDS solution for CPPS based on the deterministic Dendritic Cell Algorithm. To assess the efficiency of the DCA, a testing dataset was created by installing and injecting several attacks on a CPPS testbed based on OPC UA. The data demonstrate that the DCA can successfully identify such threats.

In 2016, Valdes *et al.* [15] suggested a CPS IDS in "host audit logs and network traffic (cyber plane)" for attack detection. The abnormal circumstances were identified by "explicitly coding" the physical limitations into a "hybrid CPS IDS", hence rendering the sensor CPS-specific. They describe an alternate technique, as well as early findings, for characterizing regular, defect, and assault phases inside an intelligent distribution system CPS, which can be used as part of a CPS IDS. In 2021, Maha *et al.* [16] have provided a revolutionary "cognitive computing-based IDS" for industrial CPS security. "Data gathering, preprocessing, feature selection, classification, and parameter optimization" are all part of the proposed model's processes. Preprocessing has been used in the developed framework to remove noise from the signal. The described algorithm subsequently selects an appropriate collection of features using a BBFO based feature selection approach. Apart from that, the GRU model is used to identify malicious inside the industrial CPS context. Lastly, the "Nester-accelerated Adaptive Moment Estimation (NADAM) optimizer" has been used to improve the recognition rate of the GRU model by optimizing its hyperparameters.

In 2021, Aliabad *et al.* [17] developed a Bayesian-based search and scoring approach- ARTINALI# for determining whether a CPS should be instrumented. They use ARTINALI# to build IDS for two different CPSs: "a smart meter and a smart artificial pancreas". They show that our method decreases the wide range of security monitors by 64% on average, resulting in storage and computation overhead savings of 52 and 69 per cent, respectively.

In 2021, Thakur *et al.* [18] have projected a new approach toward extracting the valuable attributes from provided data and then classifying incursions using a deep learning approach. It's worth mentioning that perhaps the fundamental pieces of information are drawn from two separate distributions: the one which applies to all networking incursions and the other which is particular to the sector. In light of all this, they present a novel Generic-Particular autoencoder structure, in which the general autoencoder learns characteristics that are applicable to all kinds of network incursions, while the particular autoencoders acquire data points different to that sector. In 2020, Li *et al.* [19] have projected a novel multivariate ensemble classification (MEC) approach for CPES for detecting intrusions and it aids in improving the security of the system's foundation. MEC considers detecting precision, robustness, and computation effectiveness all at the same time. "Extreme gradient boosting, light gradient boosting, as well as extreme learning machines" have all been built individually as intrusion prevention detectors in MEC. The findings demonstrate that the MEC methodology has a huge amount of potential in real-world applications.

In 2020, Liu *et al.* [20] investigated the "hierarchically distributed intrusion detection scheme" that sought to prevent ICPSs from across all angles depending on the system architecture and assaulting kinds for every ICPS stratum. Possible as well as concealed assaults for the physical system-relevant perceptual executive layer are recognized based on a "process noise and measurement noise-adaptive Kalman filter (PNMN-AKF)" with the "clustered sensory system state residual anomaly monitoring". The variational Bayes approximation methodology in PNMN-AKF enables the conduct combined recursion estimate of dynamic equilibrium configurations, time-varying processes, and measurement noise covariance matrices.

In 2018, Khalili *et al.* [21] presented A "State-based IDS (SIDS)" to identify all three abnormalities. SIDS does so by first extracting relevant CPS's usual behaviour. Furthermore, by examining the data from the field layer directly, it analyzes ongoing CPS behaviours and identifies incursions. To demonstrate how SIDS functions, a small-scale nevertheless actual CPS (mixing mechanism) has been presented. Furthermore, findings from three cyber-attacks organized on a virtual dairy pasteurization process show that SIDS has been capable of detecting cyber-attacks on massive I/O CPSs. In 2018, Attia *et al.* [22] have proposed an Intrusion Detection System (IDS) bearing two smart grid security problems: First, they present a Cumulative Sum (CUSUM) algorithm that identifies predatory pricing attacks also with granularity price fluctuations; (ii) Secondly, they build an effective methodology to track and recognize any rogue node in response to the available problems with Denial of Service (DoS) attacks. When compared to other similar methods, performance studies reveal that the proposed IDS system is more resilient.

In 2020 Süzen et al. [83] how cyber-attacks on Industry 4.0 occur and the defense strategies to be prevention against attacks. The layers in Industry 4.0 and their vulnerability were fixed to determine defense strategies. Corporate and personal measures were then determined for these vulnerabilities. It was also evaluated how accurately the current assessment was applied. As a result, the study aims to provide the truest solutions to counter cyberattacks in the industry 4.0 ecosystem. Therefore, it is envisaged to minimize damage in possible attacks.

In 2021, Ma *et al.* [23] in cyber-physical networked microgrids; a programmable intrusion detection approach was developed to detect suspicious assaults on distributed energy resources (DERs). Short programmed impulses have been fed into the reactor, as well as the reaction is used to discover aberrant circumstances, according to the suggested technique. Microgrids have had very poor robustness capabilities due to the minimal or perhaps even minimal inertia caused by combinations of DER authority, making them vulnerable to assaults. Whenever numerous microgrids have been linked, a breakdown triggered by such an assault on one could indeed readily spread to surrounding systems, resulting in devastating electricity transmission outages.

In 2022, I bor *et al.* [24] have provided a unique hybrid technique for invasion detection on CPSs communications infrastructure in this research. Based on the fundamental hyperparameters of a neural network, researchers employ a bio-inspired hyperparameter searching approach for developing an enhanced deep neural network architecture. They also construct a model which is based just on enhanced neural network structure and evaluate that on two well-known datasets, the "CICIDS2017 and UNSW-NB15". Experiment shows that our approach outperformed state-of-the-art comparison approaches in predicting a variety of types of attacks exhibiting good accuracy, minimal errors, and false-positive rates.

In 2021, Jagtap *et al.* [25] have identified identify data-abnormalities within process-control network packets, this research article introduces an adaptive multi-level intrusion detection system. In terms of Accuracy, Recall, F-Score, and Classification Accuracy, the suggested technique outperforms existing approaches, and it has been proven to be resilient, scalable, and computationally appealing. In 2020, Su*et al.* [26] this study is about detecting malicious attacks and estimating secure states for linear CPSs. Characterizations for both the undetectable and indistinguishable assaults for CPSs are offered based on the examination of both attacks. Furthermore, the detectability and distinguishability of CPSs are determined using this characterization. Then the necessary circumstances for a detectable and recognizable assault are met. This study uses a "Luenberger observer (detector)" in the finite frequency domain for assault detection. Secure state estimation is achieved by removing various attacks and sensors using the finite-frequency detector.

In 2020, Qin *et al.* [27] in the context of Hi/H_ index optimization for CPS, which is described as an LDTV system, a new detection approach to identify covert assault has been proposed. To make clandestine assaults less stealthy, a

randomized modulation matrix has been added to the route of the control variables that the attacker does not know about. The detection issue was therefore transformed into a "H/H_ or H /H_ index optimization problem" using a detection filter. The Riccati calculation was done to get the best answer. Finally, a decision-making program has been developed for triggering an alert and determining if the alert has been caused by a clandestine assault or a problem. In 2020, Fang *et al.* [28] for detecting discontinuous replay attacks in CPSs, researchers explore periodic watermarking scheduling. Because the attacker may be away for a very long period, conventional ways of imposing "continuous watermarks" on "nominal control inputs" may result in a waste of control cost if system detectors are not sensitive to the new watermarks. For these kinds of abrupt replay assaults, they first establish a one-time attack duration model in this study.

In 2019, Sánchez *et al.* [29] the identification of replay attacks that alter CPS are proposed in this study using a frequency-based technique. The approach, in particular, incorporates a "sinusoidal signal" with a "time-varying frequency (authentication signal)" into the "closed-loop system" and determines the time profile of the frequency components in the output signal is consistent with the authentication signal. A dynamic decoupling approach based on vector fitting is used to reduce couplings between inputs and outputs in order to achieve this goal. As a result, a signature applied to a given input channel will only influence the output associated with that input. In 2019, Ye *et al.* [30] the security issues in CPSs against replay attacks are discussed in this study. The attacker captures and covers the sent data between the sensors' senders and receivers in replay assaults. In 2018, Nam *et al.* [31] in this study, researchers concentrate on the challenge of determining the "moment of attack," or the point whereby an invasion of a cyber-physical system begins. They present a batch-type detection method for the moment of attack using the back-and-forth observer strategy to fix the issue of "temporarily stealthy" sensor attacks of polynomial kinds (with which standard real-time anomaly detectors rarely estimate the moment of attack).

In 2021, Alqahtani *et al.* [32] have projected a new framework for distributed blind intrusion detection. In the projected model, the sensor measurements were modelled as a graph signal. The detection intrusion was carried out by utilizing the statistical features corresponding to the graph signals. On the random field Gaussian Markov, the collected raw data have been modelled and by means of adjusting the Laplacian matrix, the precision matrix was determined. In 2021, Alguliyev *et al.* [33] a "one-dimensional convolutional neural network", a "gated recurrent unit neural network", and a "long short-term memory neural network" have been projected The Adam optimizer was studied in order to increase classification accuracy. In 2019, Shafae1 *et al.* [34] have predicted that perhaps the QC instruments could be developed to operate as physically monitoring layers as an element of a defence-in-depth approach (common IT security strategy) that escalates the difficulty/cost of a victorious assault. As a consequence, this study presents a machining-specific attack design methodology as well as an ADDS, which sets out the framework for populating a broad range of different threats. In 2020, Xu *et al.* [35] NTRU lattice has been used to develop an attribute-based encryption signing system. The latter is considered to be quantum attack resilient and has been predicated on the challenge of tiny integer resolutions on the NTRU lattice. In contrast to 2 different existing quantum robustness techniques, their proposed methodology achieves much lower communication and compute costs while remaining quantum attack resilient, according to information security and performance evaluations.

In 2015, Xia *et al.* [36] "Ada-MAC, an adaptive MAC protocol based on the IEEE 802.15.4", has been suggested. The suggested technique incorporates a "schedule-based, time-triggered protocol" with such a CSMA/CA methodology that's also based on conflict. It could not only allocate Assured Timelines dynamically, but it could also supply personalized service across distinct networks based on specific types of data. On the OMNeT++ platform, the suggested scheme is based. The performance of Ada-MAC in comparison to the regular IEEE 802.15.4 MAC is evaluated through extensive simulations. The findings demonstrate the suggested protocol's advantage in terms of reliability and timeliness.

In 2021, AlZubi *et al.* [37] to securely communicate health information, the "cognitive machine learning aided Attack Detection Framework" has indeed been suggested. The Healthcare CPS will indeed be capable of transferring information over the internet storage. Machine learning techniques could perhaps forecast cyber-attack behaviour, and the processing of data can enable medical professionals to make more informed decisions. This suggested technique depends on a patient-centric architecture which secures knowledge on a smart source, such as the end-mobile person's device, and allows the end-user to regulate metadata authorization.

In 2021, Vangipuram *et al.* [38] in this work, researchers name it CoviChain, and they seamlessly integrate an off-chain decentralized storage service for uploading huge medical sets of data and a blockchain application for safely transporting the information from the afflicted individual towards the health service utilizing edge architecture. To retrieve the hashes of the data source, the COVID-19 information has always been downloaded onto the periphery as well as transported to IPFS memory. Smart contracts have been used to transfer the hash towards the blockchain while it's being received. Because the information has always been hashed repeatedly, CoviChain overcomes privacy and security problems and avoids revealing personally identifiable information while allowing for more storage devices on the blockchain at a cheaper price and in less timeframe.

In 2018, Sood *et al.* [39] Used an "adaptive neuro-fuzzy inference system", a "cloud-based cyber-physical localization system" that has been developed to determine the risk level of CHD at a preliminary phase. Individuals who have been in the middle or high assessment criteria will still have their ECG results progressively monitored. In the event of any discrepancies in Electrocardiogram data, an alarm has been sent to the user's phone as well as to health

providers or experts, allowing them to take quick or required initiatives to protect the patient's condition. This also continues to offer preventative actions and medicines based upon that patient's risk categorization.

In 2021, Tyagi *et al.* [40] have described a decentralized e-healthcare development platform for individual information management that preserves users' rights and accessibility to their information. This paper presents a new technique for securing MCPS, namely an intelligent access-control administrator. This research additionally implements several cyber security foundations in ultra-small devices to provide critical attributes for trustworthy integrated devices. In 2020, Khan *et al.* [41] created and analyzed a control system that uses a pacemaker to reduce variations and regulate heart rate. They employ a FOF-PID controller to create electric pulses in order to maintain the ideal heart rate while reducing unprecedented beat variations. The suggested control model is compared to pacemakers employing "Fuzzy-PID (F-PID)" and "FO-PID controllers". The FOF-PID controller outperforms all other controllers. Real-time heart-rate monitoring via an IoT network allows for seamless communication between the patient and the healthcare unit, perhaps avoiding a mishap in 2017, Grispos *et al.* [42] in the MCPS, the authors have integrated the forensics principles and concepts with the intention of boosting the posture of the organization in terms of assessments. This research work has given an apt solution for the MCPS problem.

In 2017, D'Auria *et al.* [43] investigated the application of CPS in robotic surgery. In addition, the authors have designed a collaborative robotic cyber-physical system with the intention of alleviating the attacks that take place in the robotic surgery systems by means of projecting a new collaborative robotic cyber-physical system In 2019, Ivanov *et al.* [44] the goal of this research is to boost the effectiveness of MCPS detectors by introducing context into medical cyber-physical systems (MCPS) application. In so many situations, supplementary data may well be utilized to deduce that real observations are noisy or incorrect; this is referred to as information context. Based on that description, the authors developed the "CA-PAIN detector", which improves on the traditional PAIN detector by recognizing events with noisy data and eliminating false alarms.

In 2021, Guo et al [45] Security measures can be defined in terms of dynamic performance, comfortability, and energy, which are the most important metrics to evaluate an electronic control unit's performance. In 2017, Zhang *et al.* [46] An attacker might infiltrate the wind turbine "supervisory control and data acquisition (SCADA)" network as well as EMS and intentionally trigger one or maybe more wind generators via finding loopholes in cyber security elements. The effectiveness of wind turbines may thereby have had an influence on the entire energy program's dependability. The combined wind turbine SCADA/EMS system architecture has been analyzed for cyber warfare simulations including cyber elements or networking. To describe the mechanisms of accomplished cyber security threats, two Bayesian attack graph methods have been employed, as well as an actually imply time-to-compromise modelling that takes into account various attacks intensities and vulnerability assessment. The advantages and drawbacks of the existing works are shown in Table 2.

Table 2. Advantages and Drawbacks of the existing research works

Author[citation]	**Advantages**	**Drawbacks**
Xiao et *al* [5]/2021	stable for higher amplitudes	Manual response classification should be replaced by attack aims-based metrics.
		Future research will need to assess the statistical models' validity and accuracy.
Aliabadi et al. [17]/2021	Cover all attacks with low overheads (memory and time).	higher time overheads and lower detection speeds
	removes 64% of security monitors and 23% of invariants while maintaining 98% detection accuracy	
Thakur et al. [18]/2021	classify the attacks	Lower overall classification performance, Lower accuracy and F1 score and suffers from class imbalance
Jagtap et al. [25]/2021	FDetection efficiency=98%; AUC=92%; precision=0.98	This is applicable to various data analytic problems.
	lower computational cost	
Alqahtani *et al.* [32]/2021	improve the classification accuracy	Highly time-consuming. Single dataset used
Alguliyev *et al.* [33]/2021	it can be used in a variety of CPS security applications	higher Computational complexity
AlZubi *et al.* [37]/2021	When compared to other current approaches, it improves "detection accuracy, attack prediction, efficiency, minor latency, and communication cost".	higher communication costs; lower flexibility and scalability
Guo et al [45]/2021	improved dynamic performance, comfortability, and energy	higher velocity tracking error and torque ripples
Roberts *et al.* [13]/2020	lower errors	There are huge discontinuous jumps in a portion of the voltage profiles before execution. detection of abnormal activity in limited datasets
Pinto et al. [14]/2020	Lower Pearson correlation coefficient (PCC) The capacity to discern between the normal and anomalous classes is the same.	Have reached a level of complexity and Data pre-processing and selection have a high degree of reliance.
Li et al. [19]/2020	It shows the considerable potential for detection and can help avoid the problem of overfitting	lower detection accuracy
Liu et al. [20]/2020	Very low false-positive rates are possible.	The erroneous assessment may result in ineffective therapy.

Su*et al.* [26]/2020	The acquired characterization provides sufficient and necessary conditions for detestability and distinguishability.	The overdesign may increase conservativeness.
Qin*et al.* [27]/2020	lower cost and time	lower detection capability
Khan *et al.* [41]/2020	lower RMSE	sensitive data need to be secured
Zhang *et al.* [46]/2020	improved effectiveness and scalability	Detecting, mitigating, and recovering from malicious attacks takes time.
Chavez *et al.* [7]/2019	Assess a cyber-physical system's robustness in the face of malicious nodes and attacker behaviour.	Needs to achieve optimum dynamic response
Schneble et al. [10]/2019	Designed the offloading process to be lightweight and secure, ensuring data confidentiality, integrity, and authenticity.	relatively lower accuracy rates
Sánchez *et al.* [29]/19	Leads to improved detector performance.	needs to compensate the negative effects of replay attacks,
Ye *et al.* [30]/19	produce substantial changes in correlation among healthy as well as damaged networks	need to increase the data synchronization capability
Shafae1 *et al.* [34]/2019	the development of process monitoring tools that can detect both traditional process anomalies and Product-Oriented C2P attack-driven anomalies (essential for real-world deployment).	absence of trade-offs between false alarms and true positives.
	identifying characteristics that are vulnerable to a variety of assaults;	
	Determining which characteristics are the most vulnerable to certain assaults.	
Ivanov *et al.* [44]/2019	Achieves a 20% decrease in the number of false alarms	Do not have significant overlap. For effective estimation performance, appropriate numerical estimations are required.
Bernieri et al. [2]/2018	It's worth mentioning that perhaps the proposed framework is scalable to various industrial network deployments thanks to its high flexibility.	Increased redundancy is not a replacement for current IDS design techniques
Loukas et al. [11]/2018	enable dynamic coverage, configuration, and deployment	lower security
Khalili *et al.* [21]/2018	higher detection accuracy	higher computational complexity in terms of time and cost
Attia *et al.* [22]/2018	Higher detection rate=95%	Higher False Positive rate and lower detection accuracy
Nam *et al.* [31]/2018	Achieve a higher intrusion detection rate	lower accuracy of classification; higher Bayes error
Haller et al. [3]/2017	It can reduce the number of process variables used by a detection system.	Higher redundancy.
Bezemskij et al. [4]/2017	Physical threat detection is promising because it can identify physical threats with less confidence than cyber properties.	AUC performance is slightly lower
Heussen et al. [6]/2017	As the penetration of DER systems on the power system grows, so does the danger of malicious control of DER devices on the power system.	Not enough data to conduct these assessments
	Suitable for DER systems that use cyber and physical elements to monitor and notify.	
Grispos *et al.* [42]/2017	The higher trade-off between medical requirements	Need to reduce this risk
D'Auria *et al.* [43]/2017	Reducing the vulnerability of robotic surgery systems	Lower security
Mitchell et al. [9]/2016	reduced memory and training time.	Need to achieve low detection latency
Valdes et al. [15]/2016	lower convergence speed	No consideration on the security and trustworthiness
Vellaithurai *et al.* [1]/2015	It takes in cyber network configurations, power system topologies, and IDS alerts.	consumes huge time
	investigates the links between cyber and power system components.	
Xia *et al.* [36]/2015	Differentiate services for distinct nodes based on the data types they include.	Need to guarantee reliability and timeliness in high priority traffic.
Mitchell et al. [8]/	For CPSs to capture the dynamics of adversary activity and defence	Less reliable.

3.1 CPS Attack Analysis

3.1.1 Applications and Attack types

The application towards which the research has been devoted is manifested in this research work. The resultant of this analysis is shown in Table 3. The [1] focused on Power-Grid Infrastructures, [2] on Industrial Control Networks, [5] on distributed energy resources (DER), [15] on Smart grid, [19] on cyber physical energy system (CPES) and [46] on consensus-based distributed ED-cybersecurity. None of the works has been focused on the cloud computing platform. The type of attacks that has been considered in the collected research papers is discussed in this section. The resultant of this analysis is shown in Table 2. Among the attacks, the DDoS attacks are considered in most of the research works, as it is the most dangerous. The DDoS attacks has been considered in [1,2], [9,10], [14], [18], [20], [22,23,24,25], [36], [39], [41,42,43,45,46], respectively. Figure 4 describes the number of papers considered in applications of cyber physical systems

Table 3. Analysis on Applications and Attack types

Author [citation]	**Application**	**Attack type**
Ibor et al. [24]/2022	industry 4.0	DDoS
Xiao et al. [5]/2021	distributed energy resources (DER)	cyber attacks
Maha et al. [16]/2021	industry 4.0	Denial of Service (DoS) attack.
Aliabadi et al. [17]/2021	Resource-Constrained Cyber-Physical Systems	known and unknown attacks
Thakur et al. [18]/2021	industry 4.0	Web attack, Dos, brute force, port scan, bot, and infiltration
Ma et al. [23]/2021	industry 4.0	DDoS
Jagtap et al. [25]/2021	industry 4.0	DDoS
Alqahtani *et al.* [32]/2021	Secure water treatment	physical attacks
Alguliyev *et al.* [33]/2021	industry 4.0	cyber-attacks.
AlZubi *et al.* [37]/2021	Healthcare cyber-physical (HCPS) systems	cyber-attack behavior
Vangipuram *et al.* [38]/2021	decision support-healthcare-patient-centric design	linking attacks
Tyagi *et al.* [40]/2021	Outbreaks	man in middle
Guo et al [45]/21	electric vehicles with energy management systems.	denial of service (DOS) attacks, replay attacks, and deception attacks
Roberts *et al.* [13]/2020	Discrete Control Devices	false data attacks
Pinto et al. [14]/2020	Cyber-Physical Production Systems	DoS, Eavesdropping (MITM), Impersonation or Spoofing
Li et al. [19]/2020	Cyber-physical energy system (CPES).	-
Liu et al. [20]/2020	Industrial Cyber-Physical systems	DoS Attack, Deceptive Attack (Replay Attack),Noise Attack;
Su*et al.* [26]/2020	Human-machine interface (HMI)	undetectable attack and indistinguishable attack
Qin *et al.* [27]/2020	industry 4.0	covert attack
Fang *et al.* [28]/2020	industry 4.0	replay attack
Xu *et al.* [35]/2020	electronic health (e-health) system- medical cyber-physical systems	Quantum attack
Khan *et al.* [41]/2020	Identifying and Preventing Coronary Heart Disease	DDoS
Zhang *et al.* [46]/2020	consensus-based distributed ED-cybersecurity	non-colluding and colluding attacks
Chavez *et al.* [7]/2019	reference CPS model	selective forwarding, packet dropping, packet spoofing, packet replaying, packet flooding, and even Sybil attacks
Schneble et al. [10]/2019	Cloud-Based Cyber-Physical Intrusion Detection for Vehicles	DoS Command injection attack Malware attack
Sánchez *et al.* [29]/2019	Industry 4.0	replay attacks
Ye *et al.* [30]/2019	industry 4.0	replay attack
Shafae1 *et al.* [34]/2019	quality control (QC)	Product-Oriented C2P attacks
Ivanov *et al.* [44]/2019	CA-PAIN detector	quantum attack
Bernieri et al. [2]/2018	Industrial Control Networks	DDoS
Loukas et al. [11]/2018	Industrial Cyber-Physical System	DoS
Khalili et al. [21]/2018	Stage-based Cyber-Physical Systems	Denial of Service (DoS) attack.
Attia et al. [22]/2018	Pasteurization	DDoS
Nam *et al.* [31]/2018	Cyber Physical Networks	Cyber-attacks.
Sood *et al.* [39]/2018	Tracing in Healthcare-Pandemic	DDoS
Haller et al. [3]/2017	Industrial Cyber-Physical Systems	cyber attacks
Bezemskij et al. [4]/2017	autonomous robotic vehicle	false data injection, Rogue Node, Magnetic disruption
Heussen et al. [6]/2017	Distributed Energy Resource Systems	False Data Injection, Insider Threat
Grispos *et al.* [42]/2017	AARIN	DDoS
D'Auria *et al.* [43]/2017	Tracking and Stabilization of Heart-rate	DDoS
Mitchell et al. [9]/2016	Medical Cyber-Physical Systems	Denial of Service (DoS) attack.
Valdes et al. [15]/2016	Smart grid	injection attack
Vellaithurai *et al.* [1]/2015	Power-Grid Infrastructures	DDoS

Xia *et al.* [36]/2015	medical health-care scenario-sense ECG, EEG, blood pressure	DDoS
Mitchell et al. [8]/2013	Industrial CPS	attrition failure, pervasion failure, and exfiltration failure

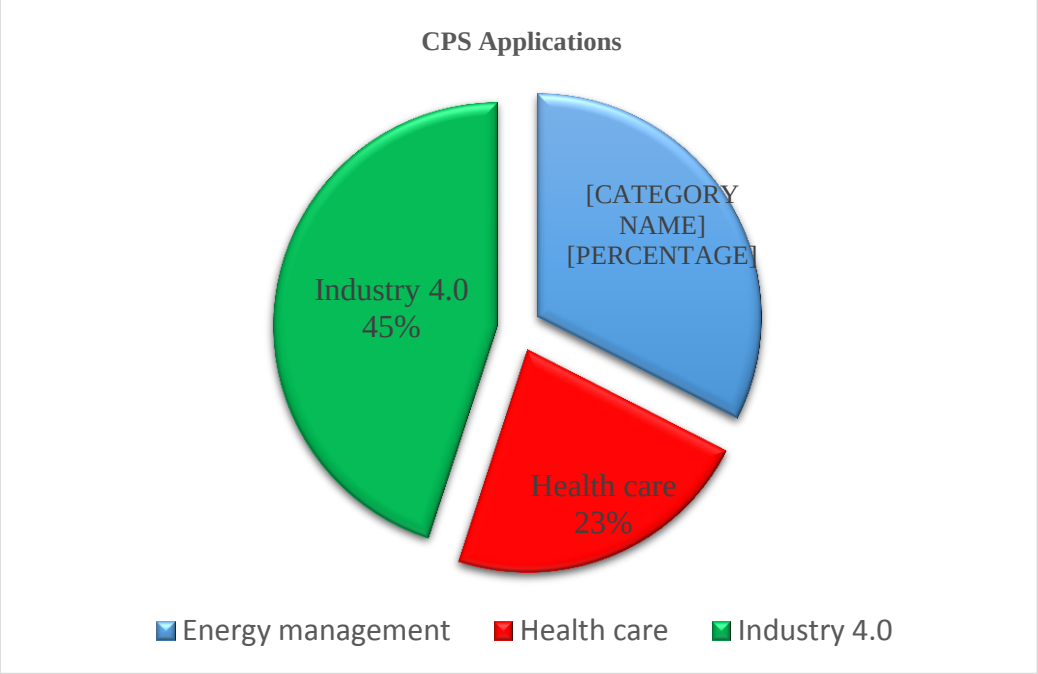

Fig. 4. Analysis of applications of CPS

3.1.2 Techniques and Tools Used

The techniques that have been used for attack detection are discussed in this section. The resultant of this analysis is shown in Table 4. In [1], the CPINDEX has been used. In addition, Bayesian Networks in [4], "linear regression, ARMAX time series modelling and two clustering methods" in [5], ARTINALI# in [17], multivariate ensemble classification-ELM, XGBoost, and LightGBM in [19] and "Fractional Order-PID (FO-PID) in [42]. The machine learning models like Bayesian Networks and Laplacian Scoring (LS); detection-g k-Nearest Neighbors (KNN) [9] and Unsupervised Machine Learning [15] has been used. But the only deep learning models Hybrid DeepGCL model [33] has been used in literature. After the utilization of the Hybrid DeepGCL model, the detection accuracy has increased above 95%. Therefore, in future, it is suggested to use the ensemble-of-deep learning classifiers model. Moreover, the attack mitigation models have not been considered in any of the literature works. The tools used for implementing the research work are manifested in this section. The MATLAB has been used for implementation in most of the research works.

Table 4. Analysis of techniques used for attack detection

Author [citation]	**Technique**	**Tools**
Xiao et al. [5]/2021	linear regression, ARMAX time series modelling and two clustering methods.	PV simulator
Aliabadi et al. [17]/2021	ARTINALI	-
Thakur et al. [18]/2021	generic and domain-specific deep autoencoder model	-
Jagtap et al. [25]/2021	BLOSSOM	-
Alqahtani *et al.* [32]/2021	graph-based intrusion approach	-
Alguliyev *et al.* [33]/2021	Hybrid DeepGCL model	MATLAB
AlZubi *et al.* [37]/2021	CML-ADF model	MATLAB
Vangipuram *et al.* [38]/2021	Covi-Chain	MATLAB
Tyagi *et al.* [40]/2021	decentralized e-healthcare application framework	MATLAB
Guo et al [45]/2021	model predictive control (MPC)	
Roberts *et al.* [13]/2020	online algorithm	MATLAB
Pinto et al. [14]/2020	Deterministic Dendritic Cell Algorithm	Python
Li et al. [19]/2020	multivariate ensemble classification-ELM, XGBoost, and LightGBM	-
Liu *et al.* [20]/2020	process and measurement noise-adaptive Kalman filter (PNMN-AKF)	MATLAB/Simulink.
Su*et al.* [26]/2020	Luenberger observer (detector)	

Qin*et al.* [27]/2020	linear discrete time-varying (LDTV)	-
Fang *et al.* [28]/2020	one-time attack duration mode	-
Xu *et al.* [35]/2020	Certificate-less signature scheme	OMNeT++ platform
Khan *et al.* [41]/2020	Fractional Order-PID (FO-PID)	MATLAB
Zhang *et al.* [46]/2020	resilient collaborative distributed EMS (R-CoDEMS)	MATLAB
Chavez *et al.* [7]/2019	stochastic Petri net (SPN) techniques	-
Schneble et al. [10]/2019	LSTM	-
Sánchez *et al.* [29]/2019	frequency-based signature	-
Ye *et al.* [30]/2019	The stochastic coding detection scheme	-
Shafae1 *et al.* [34]/2019	attack design designation system (ADDS)	MATLAB
Ivanov *et al.* [44]/2019	Context-aware	MATLAB
Bernieri et al. [2]/2018	Deep Detection Architecture (DDA)	MATLAB/Simulink
Loukas et al. [11]/2018	Trusted network connection (TNC)	-
Khalili et al. [21]/2018	SIDS	MATLAB
Attia et al. [22]/2018	The stochastic coding detection scheme	MATLAB
Nam *et al.* [31]/2018	Back-and fourth observer approach	-
Sood *et al.* [39]/2018	ANFIS	MATLAB
Haller et al. [3]/2017	-	NS3
Bezemskij et al. [4]/2017	Bayesian Networks	PV simulator
Heussen et al. [6]/2017	hybrid IDS approach	EPRI PV Simulator
Grispos *et al.* [42]/2017	Fuzzy-PID (F-PID) controllers	MATLAB
D'Auria *et al.* [43]/2017	Forensics-Driven Approach	MATLAB
Mitchell et al. [9]/16	Feature Extraction-heartbeat, peak amplitude, wave to wave intervals, Ranking-Laplacian Scoring (LS); detection-g k-Nearest Neighbors (KNN)	-
Valdes et al. [15]/2016	Unsupervised Machine Learning	-
Vellaithurai *et al.* [1]/2015	CPINDEX	MATLAB/Simulink
Xia *et al.* [36]/2015	adaptive MAC protocol	MATLAB
Mitchell et al. [8]/2013	stochastic Petri nets	

3.2 Various CPS attack Case Studies

The case study that has been considered in each of the research works is discussed in this section. The [1] has been tested with an IEEE 30-bus test-bed; MAT-POWER framework and in [2], the "single tank with proportional water pump and a time-related water consumption law" has been used. In addition, Vinyl Monomer Acetate in [3], modular robotic vehicle in [4], load response behaviour in [5], 10 MW PV system in [6], modernized electrical grid in [8], ROBOTIC VEHICLE in [11], "On-Load Tap Changing (OLTC) transformers and capacitor banks" in [13], RTDS-electrical distribution substation circuit in [15], an "advanced metering infrastructure and a smart artificial pancreas" in [17], Milk pasteurization in [21] and HAN in [22]. In addition, frequency-based replay attack detector in [29]. "PLC I/O signals, human-machine interfaces (HMIs)" in [32] [33], and medical health-care scenario in [35]. In addition, "end-user's mobile phones and end-user control data sharing access" in [36] and integrated fusion pump in [42], surgery robotic systems in [43], four-wheel-drive CAEV in [45].

3.3 Metrics Considered and performance recorded

The diverse metric considered for analyzing the projected model is discussed in this section. The detection accuracy and ROC have been considered in most of the research works. The resultant of this analysis is shown in Table 5. The performance recorded by each of the collected research papers is discussed in this section. Figure 6 shows The attack prediction ratio of 96.5% has been recorded in [36] and Classification accuracy= 83.06% has been recorded in [19]. Moreover, in [20], the Average Detection accuracies: Jamming=93.7%; Intermediator=94.7%; DoS= 100%; Gray hole= 97.5%; Node replication=95.9%; Node hijack=96.4% and Slander=95.7% has been recorded. In addition, signal to noise ratio (SNR)=1% has been recorded in [15] and a static time delay error of ±0.5% in [13]. moreover, the performance of Training Wall Time=79.7S; Training CPU Time=74.8s; Peak Memory=55236 has been recorded in [9].

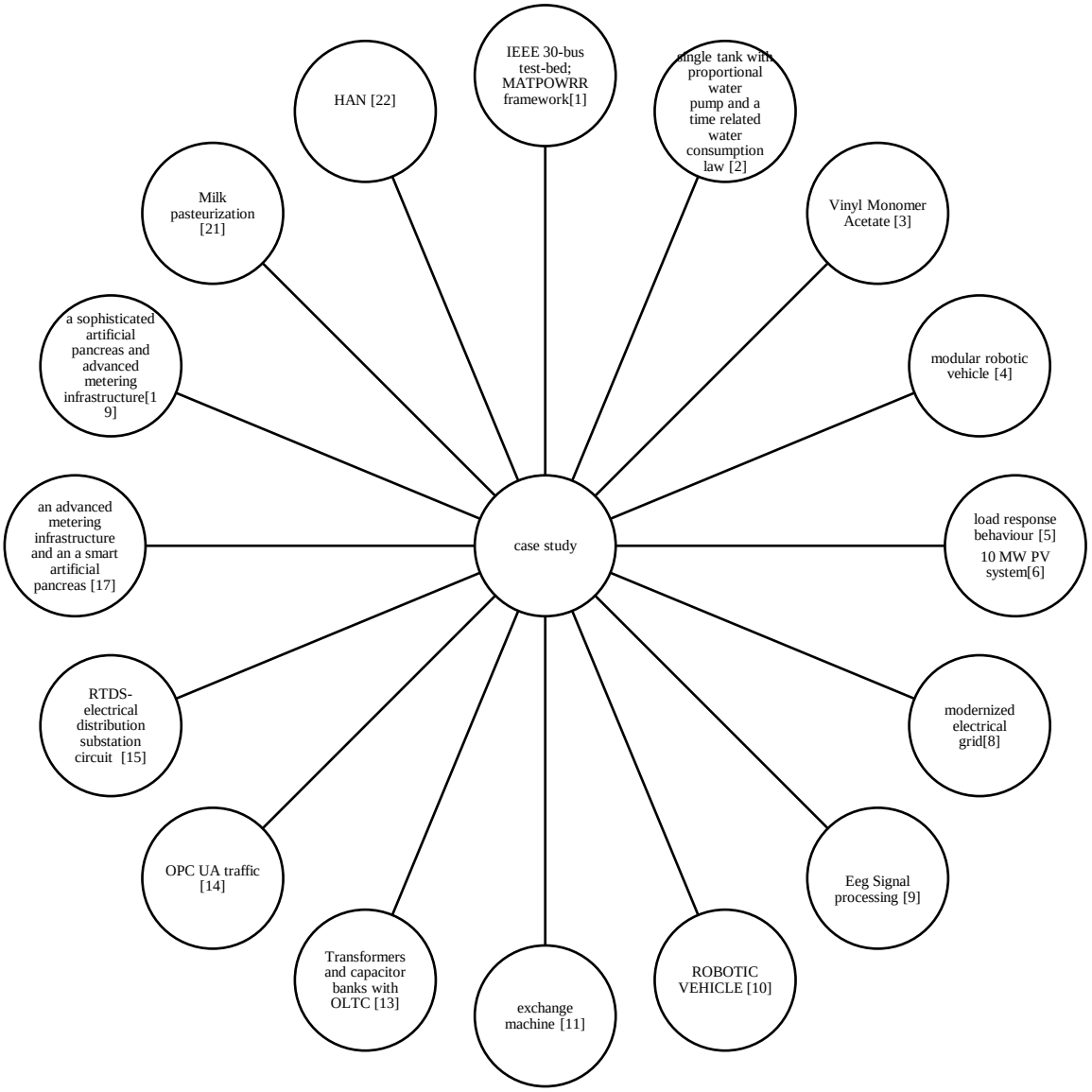

Fig. 5. Various use cases of CPS prone to attacks

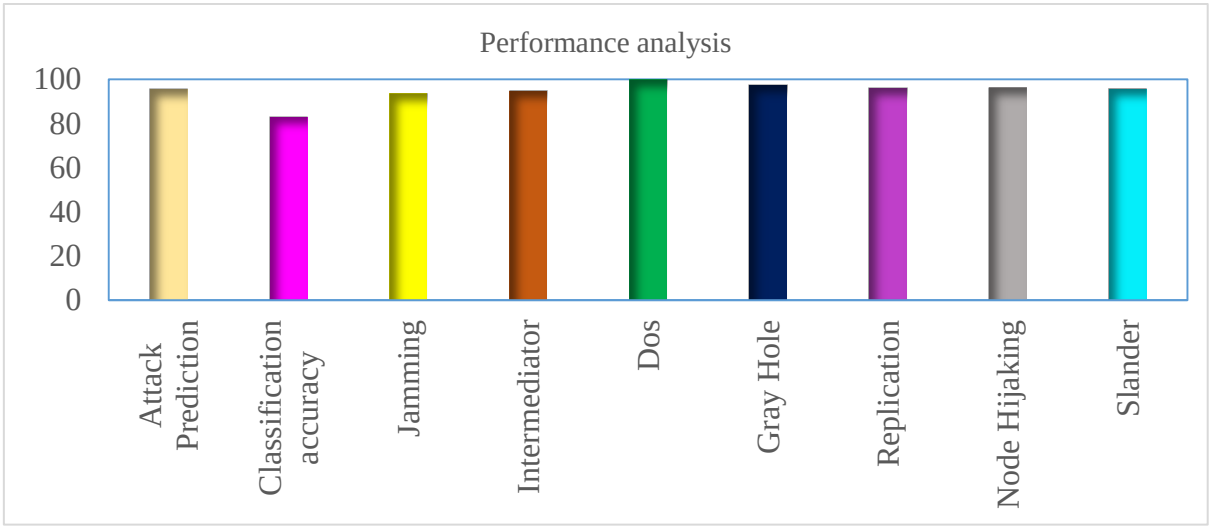

Fig. 6. Metrics and Performance

Table 5. Analysis of the Metrics Considered

Author [citation]	Metrics	Performance recorded
Ibor et al. [24]/2022	Accuracy	Accuracy=96.89(DDOS) Accuracy=98.28(DOS)
Xiao et al. [5]/2021	anomaly probability at each timestamp per house	Accuracy=99%
Maha et al. [16]/2021	Accuracy	Accuracy=98.45%
Aliabadi et al. [17]/2021	Accuracy; Attack Coverage ratio (AC); Overhead; Memory overhead; Performance overhead	Pre-Optimization=2.96 and post-Optimization=1.35; Time overhead (%): Pre-Optimization=23.3 and post-Optimization=7.3
Ma et al. [23]/2021	Accuracy, detection rate, FPR	Frequency=3000 Hz
Jagtap et al. [25]/2021	Attack detection time	Accuracy=97%(gas-pipeline dataset) Accuracy=96%(SWAT dataset)
Alqahtani *et al.* [32]/2021	Accuracy, precision, recall,	Precision (%) =99.7
Alguliyev *et al.* [33]/2021	F-measure, false alarm rate, and Log Loss, accuracy, precision.	Training loss= 0.0057; Validation loss= 0.0068; Training accuracy (%) =99.76; Validation accuracy (%) =99.75; FAR= 0.0003
AlZubi *et al.* [37]/2021	Detection Accuracy Ratio, Attack Prediction Ratio, Delay Ratio, Efficiency Ratio, Communication Cost Ratio,	Accuracy=98.2% Efficiency=97.8% Prediction=96.5%
Guo et al [45]/2021	Recovery time, Scalability analysis	In the chosen three drive cycles (NEDC, UDDS, and RDC), the MPC's energy consumptions are 1.592kWh, 1.637kWh, and 1.285kWh, respectively; the corresponding energy efficiency is enhanced by 3.2-4.5 per cent are 1.656kWh, 1.713kWh, and 1.327kWh respectively.
Roberts *et al.* [13]/2020	Utility, RMSE	static time delay error of ±0.5% and inverse time delay of ±10%.
Pinto et al. [14]/2020	Area Under the Receiver Operating Curve (AUC - ROC)	AUC is 0.99
Thakur et al. [18]/2021	Recall; precision, specificity and F1 score	DDoS (Recall)=99.939, Hulk (Recall)=99.158; XSS (Recall)=43.125, Infiltration (Recall)=50
Li et al. [19]/2020	Detection accuracy, stability and computing efficiency	Classification accuracy= 83.06% for 14-bus;79.39% for 57-bus and 74.52% for 118-bus
Liu et al. [20]/2020	AUC, ROC	Average Detection accuracies: Jamming=93.7%; Intermediator=94.7%; DoS= 100%; Gray hole= 97.5%; Node replication=95.9%; Node hijack=96.4% and Slander=95.7%
Qin *et al.* [27]/2020	ROC	detection rate of attack incidents=100%
Xu *et al.* [35]/2020	Effective utilization rate; Mean (max) end-to-end delay.	The Ada-MAC uses CFP at over 95% efficiency.
Khan *et al.* [41]/2020	FOF-PID controller maximum error is 0.72.	Simulating the controllers uses $1.56 \times 10{-}3\mu W$ of electricity.
Zhang *et al.* [46]/2020	Scalability analysis	fuel consumption=9.5%; SOC=0.6; excellent average performance of 15.9% fuel economy
Chavez *et al.* [7]/2019	Effect of Attacker Behavior, Effect of Intrusion Response, Effect of Intrusion Detection Strength	Number of intrusion detectors=7-optimal to yield the Maximum MTTF
Schneble et al. [10]/2019	Accuracy	Accuracy=86.9% detection Latency=1.163 (for 600 neuron)
S ánchez *et al.* [29]/2019	Average time	Average time of 400 s
Ye *et al.* [30]/2019	ROC curve, detection time	Detection rate=0.5s;
Shafae1 *et al.* [34]/2019	On-time delivery ratio	Precision (%) =99.7
Ivanov *et al.* [44]/2019	ROC curve	False alarm rates are around 20%
Khalili et al. [21]/2018	Accuracy	Accuracy on anomalous time-intervals
Attia et al. [22]/2018	Accuracy, detection rate, FPR	Accuracy=88%
Nam *et al.* [31]/2018	ROC,	Detection rate=0.8s;
Haller et al. [3]/2017	Changes in the sensitivity index values	Processing variable reduced by 76.8%
Bezemskij et al. [4]/2017	Area AUC&ROC	AUC=0.995;
Heussen et al. [6]/2017	Power factor values	V = 92, 99, 101, 108% of nominal voltage and Q = 25, 0, 0, -25% of reactive power capacity of the DER device
Mitchell et al. [9]/2016	Accuracy; Training Wall Time; Training CPU Time; Peak Memory	Accuracy=0.9656; Training Wall Time=79.7S; Training CPU Time=74.8s; Peak Memory=55236
Valdes et al. [15]/2016	signal to noise ratio (SNR); false alarm rate; detection rate	signal to noise ratio (SNR)=1%; false alarm rate=0.01%; detection rate =71.11%;
Vellaithurai *et al.* [1]/2015	CONTINGENCY SCORES	Contingency Scores by 11th gen. bus at 1st branch=14 and 2nd branch=15
Xia *et al.* [36]/2015	On-time delivery ratio, Attack Prediction Ratio	Attack prediction=96.5%, an accuracy ratio=98.2% an efficiency ratio=97.8%, less delay=21.3%

4. Research Gaps and Challenges

CPS does have the potential to revolutionize the way we engage with such a wide range of complicated things. CPS has indeed been used in a wide range of sectors. All CPS applications must always be created with cutting-edge technologies in consideration, as well as system-level requirements and relative impact on the actual world. This CPS application research is aimed at improving process efficiency and security, reducing consumption of resources, and improving performance. Although it is still in its infancy, CPS has been employed in a number of sectors and has achieved substantial development. Numerous current cyber-physical operations require great trustworthiness, reliability, and confidentiality, as well as assured ultra-high performance and/or ultra-low energy usage. As a consequence, CPS implementations confront significant hurdles in order to protect the data, efficiency, and compatibility. Due to its scalability, sophistication, and dynamic properties, CPS becomes subject to both virtual and real breakdowns as well as assaults. Additional characteristics that render CPS prone to security risks include the usage of a large-scale network, the deployment of unsecured communication systems, and the extensive utilization of legacy applications.

In addition, machine learning is used by the vast majority of IDSs. Useful traits for various invasions are extracted, which can then be used in supervised learning to identify attacks. A lack of relevant and enough traffic information frequently prevents feature learning from being successful. This makes training incredibly difficult because the number of incursions has been far lower than the number of non-intrusions. Unsupervised feature learning can be used to produce appropriate feature descriptions from network traffic data collected from a variety of sources to address these issues. It is possible to train a classifier using a labelled dataset that includes all traffic that is both harmless and abnormal. You can collect traffic information from the labelled dataset on an isolated and private network.

In addition, most IDS use machine learning techniques to classify assaults. In order to do research, it is necessary to extract useful features from various invasions, which may subsequently be employed in supervised learning to detect attacks. However, there is probably not enough and meaningful traffic data, making it challenging to train features. Training is made even more difficult by the fact that incursions are far less in number than non-intrusions. Unsupervised feature extraction can be utilized to build relevant feature descriptions for the data in order to address these challenges, and network traffic information from a wide range of sources can be obtained. To train the deep learning classifier, these features can be applied to a labelled (and, if necessary, smaller) dataset that includes all normal and aberrant traffic.

Despite the introduction of numerous security measures, there is a lack of appropriate solutions that can tackle all security issues inside a single framework. Although there has been a lot of study on CPS mechanisms and security strategies in previous literary studies, the deep learning techniques have not been used on large scale, and therefore the accuracy of the existing works has been lower. In addition, the pre-processing has not been considered, and so the computational complexity and processing time are found to be higher. In addition, for training the classifier that makes the decision about the presence/absence of an attack, the data features have not been taken into consideration. This process has reduced the detection accuracy of most of the models. Moreover, most of the techniques have been focused on smart grids and control systems. Since cloud computing is arising as a prime tool for data storage and transmission, the attacks on cloud devices need to be taken into consideration. Moreover, attack mitigation has not been considered in the literature.

Contrary to popular belief, challenges, threats, and vulnerabilities all refer to different aspects of CPS security. Unsolved problems are challenges, and we want to foster study on them. Our definitions of threats, vulnerabilities, attacks, and controls are based on mainstream security literature. Threats are external conditions that can harm a system, whereas vulnerabilities are internal faults that can be exploited. This section introduces CPS concerns and categorizes them as general and application-specific.

In the future, we will be able to engage with the physical environment in new ways. This revolution is not free. To fully trust the next generation's physically aware designed systems, we must restrict the use of legacy embedded systems. Be as explicit as possible to better grasp and articulate CPS system-level requirements and challenges. Fig 7 shows the main CPS concerns and their associated features. Following are concise explanations of the main challenges, with a conclusion that links them to real-world applications.

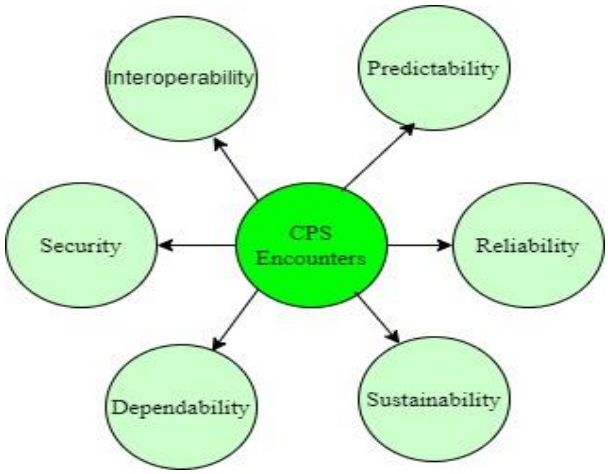

Fig. 7. Cyber-Physical System Encounters

4.1 Dependability

Dependability is a characteristic of a system in that it is able to fulfil its functionalities while maintaining or improving performance and results. When dependability is high, people will trust the system as a whole. An assured system should run as it should without being obstructed, provide services exactly as required, and never fail while it is operating. These phrases are commonly used interchangeably, especially dependability and trustworthiness. Dependability cannot be assured before the system has been put into action. In this scenario, sensor data and fast action both diminish reliability, and that means that unintended outcomes are likely. An integrated cyber and physical system makes dependability analysis all but impossible. To communicate the dependability-related information among constituent systems and underlying components, it is recommended that a common language be developed early in the design process [71,72].

4.2 Security

Security is concerned with limiting access to system resources and sensitive data to authorized users. A highly secure system should prevent data from unauthorized change and disclosure. CPSs are prone to failure due to their scalability, complexity, and dynamic nature. Manipulation of sensor measurements or command requests can be used to harm a system in order to disrupt operations or steal critical data. Employing a large-scale network (like the Internet), using unsecured communication protocols, frequently using legacy systems, or rapidly adopting commercial off-the-shelf (COTS) technologies are other security hazards [73,74].

4.3 Interoperability

Interoperability is sharing information and offering specified services. To provide or give beneficial services conducive to good communication and interoperation among system components, a highly interoperable system must supply or accept such services. To undertake long-range military operations, UAVs require seamless communication between ground and air vehicles. Interoperability standards often negatively impact complicated and vital activities, reducing their effectiveness. Assuring and certifying compatibility with a specific Smart Grid deployment under realistic operational conditions [75,76] requires standardizing devices, systems, and procedures for Smart Grid deployments.

4.4 Predictability

Predicting system state, behaviour, or function requires qualitative or quantitative understanding. A highly predictable system will ensure that the system's behaviour/functionality meets all system standards. CPMS predicts patient movements and adjusts medical device parameters based on the surrounding environment. Many medical gadgets operate in real-time to meet varying timing limitations and respond to timing uncertainty (e.g., delays, jitters etc.). While certain CPMS components are predictable, others are not. To meet end-to-end time constraints, new programming and networking abstractions, as well as resource allocation and scheduling policies, must be introduced [77,78].

4.5 Sustainability

Incorporating sustainability into a firm demands enduring and maintaining system needs, as well as system resources and their optimal utilization. A highly sustainable system is long-lasting, self-healing, and dynamic. Sustainability is an important part of energy provision and management strategies. Consider the Smart Grid, which uses renewable energy sources to distribute, manage and customize energy for customers and service providers. The inability to detect power outages and the lack of defined load measures make securing the Smart Grid's long-term operation

challenging. To maintain the Smart Grid sustainability, we will need to plan and execute in the face of uncertainty, use real-time performance assessments, dynamic energy optimization approaches, and construct autonomous microgrids [79,80].

4.6 Reliability

When a system is working properly, it is reliable. We don't assume correct operation when we test a system's capabilities. This system is incredibly reliable and does everything correctly. Because CPSs are expected to perform dependably in changing, unexpected environments, CPS uncertainty must be measured throughout the design. This will allow for effective uncertainty analysis. Design/control flow flaws, ad hoc cross-domain network connections, and component defects all degrade CPS reliability [81,82].

5. Conclusion

CPS does seem to be complex control technologies that bring together computational elements in the cybersecurity industry with physical entities in the real world. Safeguarding CPS is a crucial problem that's also attracting a lot of attention these days. Considering the current security risks, incursions, and security protocols for CPS will give you a better picture of how secure it is. CPS assaults are dangerous because they cause devastating damage to system tools and infrastructure, as well as lower production, human lives, and environmental degradation.

In this research work, a literature review has been undergone in the CPS. Here, a total of 46 research papers have been collected [68,69,70]. Each of the collected paper has been analyzed in different aspects like the technology adopted application to which the research has been devoted, attack types, performance recorded as well. Finally, the research gaps identified in CPS, especially in terms of security has been presented. The weak connections, missing parts, and fresh investigations were being identified through an assessment of existing CPS privacy and security safeguards. Risk assessment and security evaluation are critical for guaranteeing CPS's stability and operational security that need to be considered in future. As a result, the purpose of this research is to investigate the difficulties in getting CPS. Despite the introduction of numerous security measures, there is a lack of appropriate solutions that can tackle all security issues inside a single framework. Although there has been a lot of study on CPS mechanisms and security strategies in previous literary studies, the deep learning techniques has not been used in large scale, and therefore the accuracy of the existing works has been lower. In addition, the pre-processing has not been considered, and so the computational complexity and processing time is found to be higher. In addition, for training the classifier that makes the decision about the presence/absence of attack, the data features have not been taken into consideration. This process has reduced the detection accuracy of the most of the models. Moreover, most of the techniques have been focused on the smart grids and control system. Since, the cloud computing is arising as a prime tool for data storage and transmission, the attacks in the cloud devices need to be taken into consideration. Moreover, the attack mitigation has not been considered in the literature.

References

[1] C. Vellaithurai, A. Srivastava, S. Zonouz and R. Berthier, "CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures," in IEEE Transactions on Smart Grid,2015vol.6,no.2,pp. 566-575,.doi: 10.1109/TSG.2014.2372315

[2] G. Bernieri, M. Conti and F. Pascucci, "A Novel Architecture for Cyber-Physical Security in Industrial Control Networks," 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), Palermo, Italy, 2018, pp. 1-6. DOI: 10.1109/RTSI.2018.8548438

[3] P. Haller and B. Genge, "Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems," in IEEE Access, vol. 5,pp.9336-9347,2017.doi: 10.1109/ACCESS.2017.2703906

[4] A. Bezemskij, G. Loukas, D. Gan and R. J. Anthony, "Detecting Cyber-Physical Threats in an Autonomous Robotic Vehicle Using Bayesian Networks," 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 2017, pp. 98-103.

[5] Y. Xiao, J. Liu and L. Zhang, "Cyber-Physical System Intrusion Detection Model Based on Software-Defined Network," 2021 IEEE 12th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2021, pp. 170-173.
doi: 10.1109/ICSESS52187.2021.9522345

[6] K. Heussen, E. Tyge and A. M. Kosek, "Residential demand response behaviour modelling applied to cyber-physical intrusion detection," 2017 IEEE Manchester PowerTech, Manchester, UK,2017, pp.1-6.doi: 10.1109/PTC.2017.7981209

[7] A. Chavez et al., "Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems," 2019 IEEE CyberPELS (CyberPELS), Knoxville, TN, USA, 2019, pp. 1-6.DOI: 10.1109/CyberPELS.2019.8925064

[8] R. Mitchell and I. -R. Chen, "Effect of Intrusion Detection and Response on Reliability of Cyber-Physical Systems," in IEEE Transactions on Reliability, vol. 62, no. 1, pp. 199-210, March,2013.doi: 10.1109/TR.2013.2240891

[9] R. Mitchell and I. Chen, "Modeling and Analysis of Attacks and Counter Defense Mechanisms for Cyber-Physical Systems," in IEEE Transactions on Reliability, vol. 65, no.1,pp.350-358,March2016,DOI: 10.1109/TR.2015.2406860

[10] W. Schneble and G. Thamilarasu, "Optimal Feature Selection for Intrusion Detection in Medical Cyber-Physical Systems," 2019 11th International Conference on Advanced Computing(ICoAC),Chennai,India,2019,pp.238243,doi:10.1109/ICoAC48765.2019.246846

[11] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon and D. Gan, "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," in IEEE Access, vol.6, pp. 3491-3508,2018, DOI: 10.1109/ACCESS.2017.2782159
[12] X. Zhang, X. Cai, C. Wang, K. Han and S. Zhang, "A Dynamic Security Control Architecture for Industrial Cyber-Physical System," 2019 IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA, 2019, pp. 148-151. DOI: 10.1109/ICII.2019.00038
[13] C. Roberts et al., "Learning Behavior of Distribution System Discrete Control Devices for Cyber-Physical Security," in IEEE Transactions on Smart Grid, vol. 11, no. 1, pp. 749-761,Jan.2020,DOI: 10.1109/TSG.2019.2936016
[14] R. Pinto, G. Gonçalves, E. Tovar and J. Delsing, "Attack Detection in Cyber-Physical Production Systems using the Deterministic Dendritic Cell Algorithm," 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria,2020, pp. 1552-1559, DOI: 10.1109/ETFA46521.2020.9212021
[15] A. Valdes, R. Macwan and M. Backes, "Anomaly Detection in Electrical Substation Circuits via Unsupervised Machine Learning," 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI), Pittsburgh, PA, USA, 2016, pp. 500-505. doi: 10.1109/IRI.2016.74
[16] Maha M. Althobaiti, K. Pradeep Mohan Kumar, Romany F. Mansour, "An intelligent cognitive computing-based intrusion detection for industrial cyber-physical systems", Measurement, 2021
[17] Maryam Raiyat Aliabadi, Margo Seltzer, Ramak Ghavamizadeh, "ARTINALI#: An Efficient Intrusion Detection Technique for Resource-Constrained Cyber-Physical Systems", International Journal of Critical Infrastructure Protection, 2021
[18] Soumyadeep Thakur, Anuran Chakraborty, Ram Sarkar, "Intrusion detection in cyber-physical systems using a generic and domain-specific deep autoencoder model", Computers & Electrical Engineering, 2021
[19] Yunfeng Li, Wenli Xue, Yang He, "Intrusion detection of a cyber-physical energy system based on multivariate ensemble classification", Energy, 2020
[20] Jinping Liu, Wuxia Zhang, Jean-Paul Niyoyita, "Toward security monitoring of industrial Cyber-Physical systems via hierarchically distributed intrusion detection", Expert Systems with Applications, 2020
[21] Abdullah Khalili, Ashkan Sami, Saber Pouresmaeeli, "SIDS: State-based intrusion detection for stage-based cyber-physical systems", International Journal of Critical Infrastructure Protection, 2018
[22] Mohamed Attia, Sidi Mohammed Senouci, Daniela Chrenko, "An efficient Intrusion Detection System against cyber-physical attacks in the smart grid", Computers & Electrical Engineering, 2018
[23] Shuyang Ma, Yan Li, Tao Xu, "Programmable intrusion detection for distributed energy resources in cyber-physical networked microgrids", Applied Energy, 2021
[24] Ayei E. Ibor, Olusoji B. Okunoye, Khadeejah A. Abdulsalam, "Novel Hybrid Model for Intrusion Prediction on Cyber-Physical Systems' Communication Networks based on Bio-inspired Deep Neural Network Structure", Journal of Information Security and Applications, 2022
[25] Sujeet S. Jagtap, Shankar Sriram V. S., Subramaniyaswamy V., "A hypergraph based Kohonen map for detecting intrusions over cyber-physical systems traffic", Future Generation Computer Systems, 2021
[26] Qingyu Su, Zhongxin Fan, Yue Long, Jian Li, "Attack detection and secure state estimation for cyber-physical systems with finite-frequency observers", Journal of the Franklin Institute, 2020
[27] Jiao Qin Maiying Zhong Yang Liu Xianghua Wang Donghua Zhou ,"Covert attack detection based on hi/ho Optimization for Cyber-Physical Systems based on Optimization for Cyber-Physical Systems ", IFAC, 2020
[28] Chongrong Fang, Yifei Qi, Peng Cheng, Wei Xing Zheng, "Optimal periodic watermarking schedule for replay attack detection in cyber-physical systems", Automatica, 2020
[29] Helem Sabina Sánchez, Damiano Rotondo, Teresa Escobet, Vicenç Puig, Jordi Saludes, Joseba Quevedo, "Detection of replay attacks in cyber-physical systems using a frequency-based signature", Journal of the Franklin Institute, 2019
[30] Dan Ye, Tian-Yu Zhang, Ge Guo, "Stochastic coding detection scheme in cyber-physical systems against replay attack", Information Sciences, 2019
[31] Jiyeon Nam, Gyunghoon Park Taekyoo Kimand Hyungbo Shim, "A Posteriori Detection of Moment of attack on Cyber-physical Systems: A Back-and-forth Observer Approach ", IFAC, 2018
[32] Abdulrahman Saad Alqahtani, Khaled Ali Abuhasel, Mohammed Alquraish, "A Novel Decentralized Analytical Methodology for Cyber-Physical Networks Attack Detection", Wireless Personal Communications, 2021
[33] Rasim Alguliyev, Yadigar Imamverdiyev, Lyudmila Sukhostat, "Hybrid DeepGCL model for cyber-attacks detection on cyber-physical systems", Neural Computing and Applications, 2021
[34] Mohammed S. Shafae1 & Lee J. Wells2 & Gregory T. Purdy3, "Defending against product-oriented cyber-physical attacks on machining systems", The International Journal of Advanced Manufacturing Technology, 2019
[35] Zhiyan Xu, Debiao He, Pandi Vijayakumar, Kim-Kwang Raymond Choo, Li Li, "Efficient NTRU Lattice-Based Certificateless Signature Scheme for Medical Cyber-Physical Systems", Journal of Medical Systems, 2020
[36] Feng Xia, Linqiang Wang, Daqiang Zhang, Daojing He, Xiangjie Kong, "An adaptive MAC protocol for real-time and reliable communications in medical cyber-physical systems", Telecommun System, 2015
[37] Ahmad Ali AlZubi, Mohammed Al-Maitah, Abdulaziz Alarifi1, "Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques", Soft Computing, 2021
[38] Sukrutha L. T. Vangipuram, Saraju P. Mohanty, Elias Kougianos, "CoviChain: A Blockchain-Based Framework for Nonrepudiable ContactTracing in Healthcare Cyber‑Physical Systems During PandemicOutbreaks", SN Computer Science, 2021
[39] Sandeep K. Sood, Isha Mahajan, "A Fog Assisted Cyber-Physical Framework for Identifying and Preventing Coronary Heart Disease", Wireless Pers Commun, 2018
[40] Amit Kumar Tyagi, S.U. Aswathy, G. Aghila, N. Sreenath, "AARIN: Affordable, accurate, reliable and innovative mechanism to protect a medical cyber-physical system using blockchain technology", International Journal of Intelligent Networks, 2021
[41] Pritam Khan, Yasin Khan, Sudhir Kumar, "Tracking and Stabilization of Heart-rate using Pacemaker with FOF-PID Controller in Secured Medical Cyber-physical System", 12th International Conference on Communication Systems & Networks (COMSNETS), 2020

[42] George Grispos, William Bradley Glisson, Kim-Kwang Raymond Choo, "Medical Cyber-Physical Systems Development: A Forensics-Driven Approach", 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2017
[43] Daniela D'Auria and Fabio Persia, "A Collaborative Robotic Cyber-Physical System for Surgery Applications", 2017 IEEE International Conference on Information Reuse and Integration (IRI), 2017
[44] Radoslav Ivanov, James Weimer and Insup Lee, "Context-Aware Detection in Medical Cyber-Physical Systems", 2018 9th ACM/IEEE International Conference on Cyber-Physical Systems, 2019
[45] L. Guo et al., "Systematic Assessment of Cyber-Physical Security of Energy Management System for Connected and Automated Electric Vehicles," IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 3335-3347, May 2021. DOI: 10.1109/TII.2020.3011821
[46] Z. Cheng and M. -Y. Chow, "Resilient Collaborative Distributed Energy Management System Framework for Cyber-Physical DC Microgrids," IEEE Transactions on Smart Grid, vol. 11, no. 6, pp. 4637-4649, Nov. 2020. DOI: 10.1109/TSG.2020.3001059
[47] A. Humayed, J. Lin, F. Li and B. Luo, "Cyber-Physical Systems Security—A Survey," in IEEEInternetofThingsJournal, vol.4, no.6, pp. 1802-1831, Dec. 2017.DOI: 10.1109/JIOT.2017.2703172
[48] F. O. Olowononi, D. B. Rawat and C. Liu, "Resilient Machine Learning for Networked Cyber-Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS," in IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 524-552,Firstquarter2021,doi: 10.1109/COMST.2020.3036778
[49] L. Babun, H. Aksu and A. S. Uluagac, "CPS Device-Class Identification via Behavioral Fingerprinting: From Theory to Practice," in IEEE Transactions on Information Forensics and Security, vol. 16, pp.2413-2428,2021, DOI: 10.1109/TIFS.2021.3054968
[50] L. Zhao and W. Li, "Co-Design of Dual Security Control and Communication for Nonlinear CPS Under DoS Attack," in IEEE Access, vol. 8, pp. 19271-19285, 2020. DOI: 10.1109/ACCESS.2020.2966281
[51] R. Pal and V. Prasanna, "The STREAM Mechanism for CPS Security The Case of the Smart Grid," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol.36, no.4, pp. 537-550, April 2017, DOI: 10.1109/TCAD.2016.2565201
[52] A. Burg, A. Chattopadhyay and K. -Y. Lam, "Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-Things," in Proceedings of the IEEE, vol.106, no.1, pp.38-60, Jan. 2018,DOI: 10.1109/JPROC.2017.2780172
[53] F. Asplund, J. McDermid, R. Oates and J. Roberts, "Rapid Integration of CPS Security and Safety," in IEEE Embedded Systems Letters, vol. 11, no. 4, pp. 111-114, Dec. 2019. doi: 10.1109/LES.2018.2879631
[54] M. A. Jan et al., "Lightweight Mutual Authentication and Privacy-Preservation Scheme for Intelligent Wearable Devices in Industrial-CPS," in IEEE Transactions on Industrial Informatics,vol.17,no.8,pp.5829-5839,Aug.2021,doi: 10.1109/TII.2020.3043802
[55] A. Gu, Z. Yin, C. Cui and Y. Li, "Integrated Functional Safety and Security Diagnosis Mechanism of CPS Based on Blockchain," in IEEE Access, vol. 8, pp. 15241-15255, 2020. doi: 10.1109/ACCESS.2020.2967453
[56] I. Zografopoulos, J. Ospina, X. Liu and C. Konstantinou, "Cyber-Physical Energy SystemsSecurity:ThreatModeling,RiskAssessment,Resources,Metrics,andCaseStudies,"in IEEEAccess, vol.9, pp.29775-29818,2021,doi: 10.1109/ACCESS.2021.3058403
[57] M. Amin, F. F. M. El-Sousy, G. A. A. Aziz, K. Gaber and O. A. Mohammed, "CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review," in IEEE Access, vol. 9, pp. 38571-38601, 2021. DOI: 10.1109/ACCESS.2021.3063229
[58] A. Nourian and S. Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber-Physical Systems Applied to Stuxnet," in IEEE Transactions on Dependable and secure computing, vol. 15, no,1, pp.2-13,1Jan.-Feb.2018, DOI: 10.1109/TDSC.2015.2509994
[59] Z. Yang, W. Yan and Y. Xiang, "On the Security of Compressed Sensing-Based Signal Cryptosystem," in IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 3, pp. 363-371,Sept.2015,DOI: 10.1109/TETC.2014.2372151
[60] Q. Xu, P. Ren, H. Song and Q. Du, "Security-Aware Waveforms for Enhancing Wireless Communications Privacy in Cyber-Physical Systems via Multipath Receptions," in IEEEInternetofThingsJournal, vol.4, no.6, pp.1924-1933, Dec.2017, DOI: 10.1109/JIOT.2017.2684221
[61] X. Zhou, Z. Yang, M. Ni, H. Lin, M. Li and Y. Tang, "Analysis of the Impact of Combined Information-Physical-Failure on Distribution Network CPS," in IEEE Access, vol.8, pp.44140-44152,2020, DOI: 10.1109/ACCESS.2020.2978113
[62] C. -C. Chan, C. -Z. Yang and C. -F. Fan, "Security Verification for Cyber-Physical Systems Using Model Checking," in IEEE Access, vol. 9, pp. 75169-75186, 2021. DOI: 10.1109/ACCESS.2021.3081587
[63] S. H. Bouk, S. H. Ahmed, R. Hussain and Y. Eun, "Named Data Networking's Intrinsic Cyber-Resilience for Vehicular CPS," in IEEE Access, vol. 6, pp. 60570-60585, 2018. DOI: 10.1109/ACCESS.2018.2875890
[64] C. Hennebert and J. D. Santos, "Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis," in IEEE Internet of Things Journal, vol. 1, no. 5, pp. 384-398, Oct. 2014, DOI: 10.1109/JIOT.2014.2359538
[65] A. Alipour-Fanid, M. Dabaghchian, N. Wang, L. Jiao and K. Zeng, "Online-Learning-Based Defense Against Jamming Attacks in Multichannel Wireless CPS," in IEEE Internet of things journal, vol. 8, no.17, pp.13278-13290,1Sept.1,2021,DOI: 10.1109/JIOT.2021.3066476
[66] P. Venkitasubramaniam, J. Yao and P. Pradhan, "Information-Theoretic Security in Stochastic Control Systems," in Proceedings of the IEEE, vol. 103, no. 10, pp. 1914-1931, Oct.2015,DOI: 10.1109/JPROC.2015.2466089
[67] J. Zhang, Y. Wang, S. Li and S. Shi, "An Architecture for IoT-Enabled Smart Transportation Security System: A Geospatial Approach," in IEEE Internet of Things Journal, vol.8, no.8, pp.6205-6213,15April15,2021, DOI: 10.1109/JIOT.2020.3041386
[68] W. Yan, L. K. Mestha and M. Abbaszadeh, "Attack Detection for Securing Cyber-Physical Systems," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8471-8481, Oct. 2019, DOI: 10.1109/JIOT.2019.2919635

[69] A. J. Alam Majumder, C. B. Veilleux and J. D. Miller, "A Cyber-Physical System to Detect IoT Security Threats of a Smart Home Heterogeneous Wireless Sensor Node," in IEEEAccess, vol. 8, pp.205989-206002,2020, DOI: 10.1109/ACCESS.2020.3037032
[70] A. Chattopadhyay, K. -Y. Lam and Y. Tavva, "Autonomous Vehicle: Security by Design," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 11, pp. 7015-7029,Nov.2021,DOI: 10.1109/TITS.2020.3000797
[71] Grit Denker, Nikil Dutt, Sharad Mehrotra, Mark-Oliver Stehr, Carolyn Talcott, and Nalini Venkatasubramanian, "Resilient dependable cyber-physical systems: a middleware perspective," Journal of Internet Services and Applications, vol. 3, no. 1, pp. 41-49, 2012.
[72] Kai Höfig, "A vehicle control platform as safety element out of context," at HiPEAC Computing Systems Week, Barcelona, Spain, May 15, 2014. Retrieved on October 31, 2014from http://rts.eit.uni-kl.de/hipeac-ws-0514/Presentations/KaiHoefig.pdf
[73] "Designed-In Cyber Security for Cyber-Physical Systems," Workshop Report by the Cyber Security Research Alliance (CSRA) and Co-sponsored with NIST, 2013. Retrieved onSeptember26,2014fromhttp://www.cybersecurityresearch.org/documents/CSRA_Workshop_Report.pdf
[74] Aja Waseem Anwar and Saqib Ali, "Trust-Based Secure Cyber-Physical Systems," in Proc. of Workshop Proceedings: Trustworthy Cyber-Physical Systems, Tech Report Series, Computing science, Newcastle Uni., 2012.
[75] Jeremiah Gertler, "U.S. Unmanned Aerial Systems," CRS Report for Congress, Congressional Research Service, 2012. Retrieved on September 26, 2014, from http://fas.org/sgp/crs/natsec/R42136.pdf
[76] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, NIST Special Publication 1108R2, 2012. Retrieved on September 26, 2014, from http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf
[77] "Cyber-Physical Systems: Situation Analysis of Current Trends, Technologies, and Challenges," in Proc. of NIST CPS Workshop, 2012. Retrieved on September 26, 2014, from http://events.energetics.com/NIST-CPSWorkshop/pdfs/CPS_Situation_Analysis.pdf
[78] High Confidence Software and Systems Coordinating Group, "High-confidence medical devices: Cyber-physical systems for 21st-century health care," A Research and Development Needs Report, NCO/NITRD, 2009. Retrieved on June 25, 2014, from http://www.whitehouse.gov/files/documents/cyber/NITRD-High-ConfidenceMedical Devices.pdf
[79] Ayan Banerjee, et al., "Ensuring safety, security and sustainability of mission-critical cyber-physical systems," in Proc. of the IEEE, vol. 100, no. 1, pp.283-299, 2011.
[80] James A. Momoh, "Fundamentals of Analysis and Computation for the Smart Grid," in Proc. Of IEEEPower and Energy Society General Meeting. pp. 1–5, 2010
[81] Acatech - National Academy of Science and Engineering, "Cyber-Physical Systems Driving force for innovation in mobility, health, energy and production," Position Paper, December2011.RetrievedonJune25,2014fromhttp://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Stellungnahmen/acatech_POSITION_CPS_Englisch_WEB.pdf
[82] "Strategic R&D Opportunities for 21st Century Cyber-Physical Systems," Report of the Steering Committee for Foundations in Innovation for Cyber-Physical Systems, RetrievedonSeptember26,2014from http://www.nist.gov/el/upload/12-Cyber-Physical-Systems020113_final.pdf
[83] Sözen, A. A. (2020). A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem. International Journal of Computer Network & Information Security, 12(1).

Authors' Profiles

Maloth Sagar received the Master of Technology degree from Jawaharlal Technological University Hyderabad in 2016. He is currently working towards Ph.D Degree in Deep Learning at Vellore Institute of Technology (VIT UNIVERSITY), Vellore. His main research interest includes cyber-physical systems, Deep learning and cyber security.

Dr Vanmathi C received her Ph.D degree in Information Technology and Engineering from VIT University, M.Tech (IT) from Sathyabhama University and B.E. Computer Science from Madras University. She is working as an Associate Professor in the School of Information Technology at VIT University, Vellore Campus, India. She is having 16 years of research experience. Her area of research includes Deep Learning, Computer Vision, Soft Computing, Cyber-Physical Systems and the Internet of Things. She is a member of the Computer Society of India and Soft Computing Research Society.

How to cite this paper: Maloth Sagar, Vanmathi C., " Attacks on Cyber Physical System: Comprehensive Review and Challenges", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.12, No.5, pp. 53-73, 2022. DOI:10.5815/ijwmt.2022.05.06