International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 12 | Dec - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Integrating Machine and Deep Learning for Enhanced Security in Cyber-Physical Systems: Challenges and Future Research Agenda

Simranjit Kaur *

Assistant Professor in Computer Science,
Khalsa College (ASR) Of Technology & Business Studies,
Mohali –Punjab.
Email:-simrankaurgill26@gmail.com.

Abstract: Cyber-physical systems are an essential and frequently used infrastructure for resolving today's most challenging problems. As we all know, making rapid and accurate decisions in a big data setting (also called a critical/significant environment) is a tough challenge. This chapter's potential investigates the specifics of one of the most significant technological revolutions developing "Cyber-Physical Systems" and the increasing role of artificial intelligence techniques in these systems. Artificial intelligence techniques are essential in information security because they can rapidly evaluate millions of incidents and recognize various threats – from malware leveraging zero-day vulnerabilities to risky actions that might result in a phishing attack or download of malicious code. We conducted an efficient search in Web of Science, PubMed, Scopus, and EBSCO for articles published up to April 2021 that addressed federated learning, deep learning, machine learning, graph-based approaches, intrusion detection tree approaches, and Signature Based Malicious Behavior Detection in cyber-security. Additionally, the work compared various attack detection techniques in cyber-physical systems against associated challenges and quality metrics such as accuracy, bandwidth, Variance of Noise, Sparsity rate, Pushing recall, F1-score, precision, and recall. It extensively discusses the context for artificial intelligence in cyber-security, including the different cyber-physical security attacks. The unique aspect of this work is that the survey summarizes current concepts and their limitations, focusing on future research potential in artificial intelligence techniques for Cyber-Physical Systems. This research work would facilitate multiple researchers and scholars investigating cyber-physical domains and serve as a basis for further studies.

Keywords: Artificial Intelligence; Machine Learning; Deep Learning; Cyber-Physical Systems; Cyber Security; Attacks; Malware

1. Introduction

A Cyber-physical system (CPSs) means incorporating physical techniques into the real world and control software into the cyber-physical world. These two words are interchangeably used to share information [1]. The paths through which an attacker can invade the CPS increase as the CPS's connectivity grows and becomes more complex [2]. External attackers are particularly vulnerable to the networks that connect the physical systems and the control software that aims to penetrate the CPS and cause physical system malfunctions [3]. When an attacker gains access to a network, control-critical software can be disrupted. Artificial intelligence (AI) is increasingly being used in computer security. Maintaining physical security in the cyber-physical system is one of the most common issues in cyber-physical space [4]. Cyber-physical security refers to protecting devices, software, and networks from cyber-physical attacks [5-7]. The adversaries who carry out these attacks are primarily interested in modifying/accessing

confidential information, laundering money from users, and disrupting normal business operations [8-10]. Various AI technologies detect network interference in vulnerability management analysis [11]. Deep learning is a well-known technique for detecting network intrusions. To detect network anomalies, several researchers have used machine learning methods such as convolutional neural networks [12] and help vector machines [13]. Hence, to ensure sensor security, some physical authentication methodologies are needed. The authors in [5] analyzed the side effects of threats on the actuators. The primary two attacks are a) Finite Energy Attack, which is related to the loss and alteration of packets b) Finite-Time Attack, also known as Bounded-Attack, which causes the suppression of control signals. The actuator's security control is related to the passive or active mode of operation where no action is taken without proper procedures. Authors in [14] have discussed distributed attacks on various computing resources, including Trojans, Viruses, Worms, and DoS atacks. The latest security advancement is essential to study the in-depth protection of CPS.

In contrast to traditional cyber-physical security, Cyber-physical security is an extension that considers the physical components [15]. In a conventional security system, Leakage of private information is one of the burning issues in CPS systems. Password guessing and the process of recovering passwords. In contrast to others, security tasks enable attackers to try to prevent confidential models [16]. It is vital to understand how opponents react to them for designers of security classification. This is vital to the testing community in determining better ways to predict deployment effectiveness [17].

Working with the physical components leads to security issues that contribute to the study of the CPS system [18-21].

- The widespread cyber-attacks and vulnerabilities to IoT devices.
- Modeling the security threats
- Designing the fault-tolerant system for the prevention of cyber and physical attacks.

However, prior research on AI-based cyber-security systems methods has made limited attempts to encapsulate actual knowledge by utilizing literature reviews holistically [22-23]. For example, the authors in the study [24] have discussed the approach based on machine learning to detect the application-layer CPS attack. The authors have also disclosed the pattern-based model of graph-based segmentation and dynamic programming [25]. Research done by authors in [26] has also explored the machine learning approach for CPS attack surface. That analysis also provides a natural way for reasoning attack & threat models. Another research done by authors in [27-29] has discussed machine learning methods for biological data that are further integrated for detecting Cyber-Physical attacks in cyber manufacturing systems (CMS). The experts in the study [6] have analyzed strategies for three significant cyber-physical security issues: interruption detection, malware investigation, and spam detection. The authors have investigated a few issues that impact the application of ML to cybersecurity. We relate to this need by conducting a detailed survey on implementing AI methods in a cyber-physical system [30]. This conceptual study may help summarise existing information in a field of research and enable the detection of emerging information gaps and, as a result, future research directions [19].

Therefore, new technological development must be initiated to achieve security, privacy, integrity, and confidentiality in the CPS [31-34]. The aim of this chapter is an existing review of artificial intelligence-based cyber-security systems and solutions, which have been proposed by various authors in the different types of cyber-attacks. This research covers security-related matters as a result of the cyber-physical system and discusses inherent security challenges in cyber-physical systems that can be potentially exploited by attackers [35-39]. In this chapter, we shortlisted documents that have been published by Springer, IEEE Access, Elsevier, and ACM between 2009 and 2021 to classify the detection and prevention of cyber-physical attacks.

The rest of this chapter is organized into different sections. Section 2 describes the methodologies, highlighting the selection criteria for choosing the chapters to conduct the extensive survey. In section 3, the framework of AI in CPS

security, along with the network and threat model. Moreover, section 4 is devoted to the methodologies of AI in the CPS system. Section 5 presents the comparative analysis from different research chapters on Cyber-Physical systems. In section 6, a future perspective is mentioned, and finally, the conclusion of the CPS security is given in section 7.

2. METHODOLOGIES

This section presents the methodology considered to conduct the literature survey. In this study, we have applied various methods of a systematic literature review followed by existing research studies on AI-based processes for the CPS systems. In Figure2, we describe our survey procedure in the following three steps: preparation, execution, and reporting. The research database sources are used to address questions RQ1, RQ2, RQ3, and RQ4. Some of the RQs and their objectives for the literature review are listed in Table 1. These are EBSCO, PubMed, Scopus, and other publications that draw on all four databases.

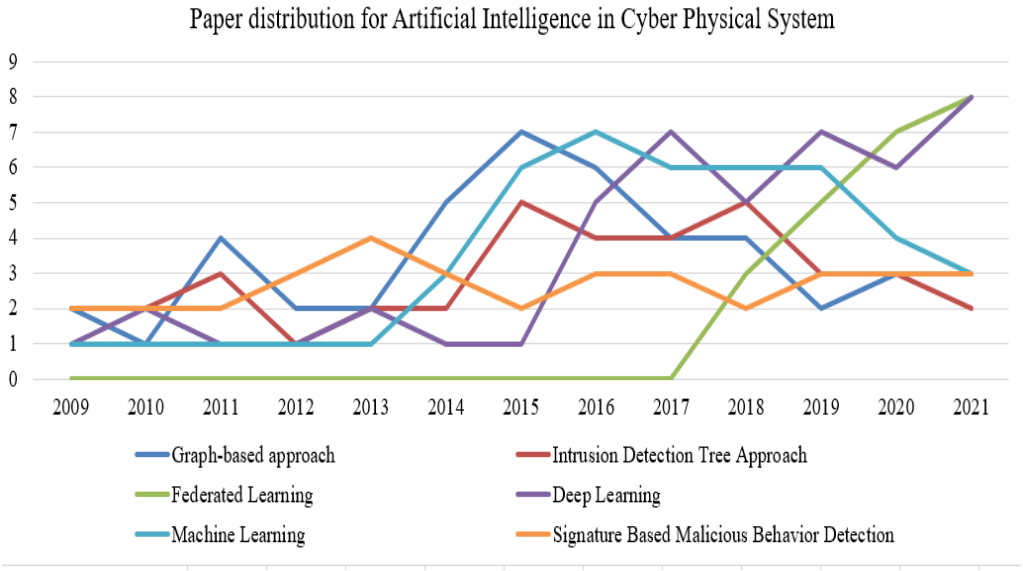

Figure 1: Distribution of papers reviewed for AI in the Cyber-Physical system

In this chapter, we used Web of Science to develop this survey for a broad spectrum of articles. This article was based on previous research using specific inclusion and exclusion criteria [40]. We have emphasized to make this review paper attractive and meaningful, the research papers of 2009 to 2021 are included. In this paper, we have downloaded two hundred eighty-nine research chapters from different databases like Scopus, web of science, EBSCO, and PubMed. This paper describes the research on Artificial Intelligence (AI) based methodologies with cyber-physical techniques.

The database search keywords with their finding are presented in Fig 2. Whereas, table 1 shows that four suitable keyword options are available — "Artificial Intelligence Technique in Cyber-Physical System ","Machine Learning in Cyber-Physical System ","Deep Learning in Cyber-Physical System ","Federated Learning in Cyber-Physical System ", (see Table 2). The steps involved in the survey are shown in the diagram in Fig 3.

Table1: Research questions and their objectives

Q.No Identified research questions	Objective
RQ.1 Which AI based approaches have been used extensively in cyber-physical systems?	It aims to design the security framework of AI for the identification of vulnerabilities.
RQ.2 What are the different types of cyber security attacks and what are the existing dataset is used to mitigate from attack?	It targets to explore the security attacks and identify the existing datasets.
RQ.3 What are the different methods that are used to measure the performance of cyber-physical system?	It targets to provide information on AI methods for cyber security systems.
RQ.4 Discuss the comparative analysis of various AI based Models and future prospective?	It aims to provide the comparison for federated, deep, and machine learning models in the secure Cyber-Physical system.

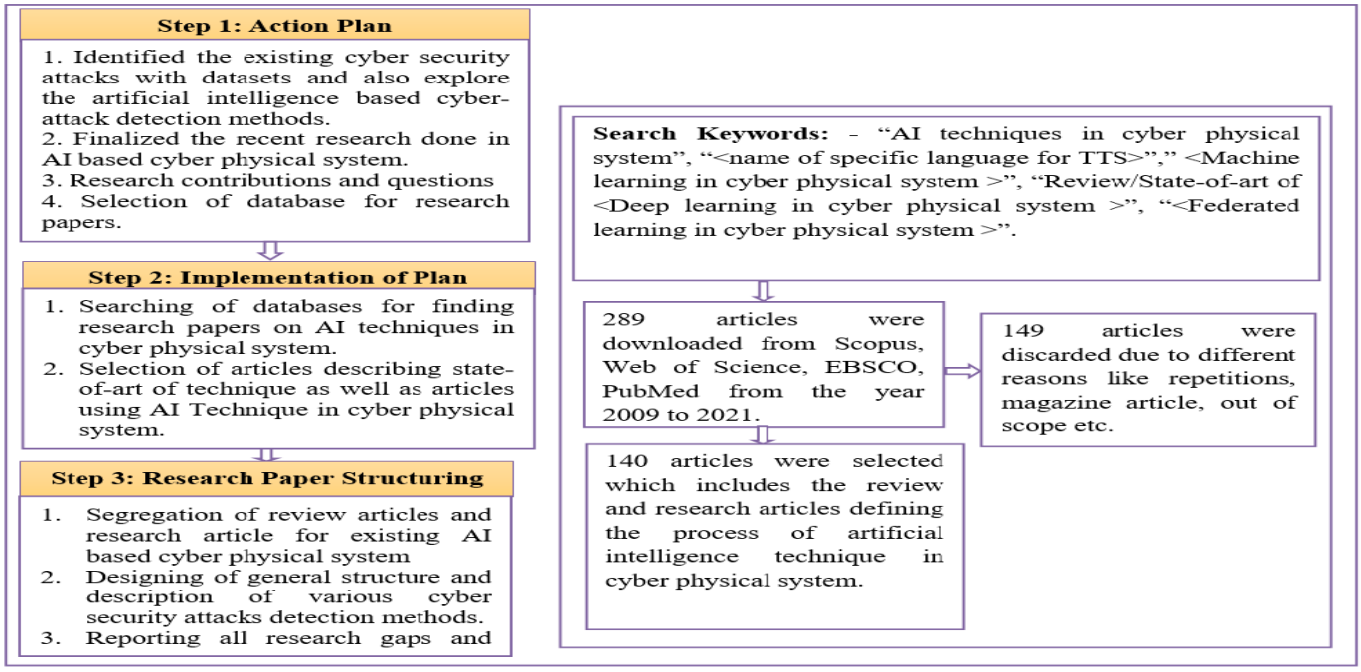

Figure 2: The mechanism for literature survey

Table 2: Database search keywords

Database	Keywords	Total hits appeared	Abstract reads	Fulltext downloaded
EBSCO	"Artificial Intelligence Technique in Cyber-Physical System" "Machine Learning in Cyber-Physical System" "Deep Learning in Cyber-Physical System" "Federated Learning in Cyber-Physical System"	41 31 41 47	41 37 41 47	27 25 19 11
PubMed	"Artificial Intelligence Technique in Cyber-Physical System" "Machine Learning in Cyber-Physical System" "Deep Learning in Cyber-Physical System" "Federated Learning in Cyber-Physical System"	51 41 46 41	51 41 46 41	24 23 21 11

Scopus	"Artificial Intelligence Technique in Cyber-Physical System" "Machine Learning in Cyber-Physical System" "Deep Learning in Cyber-Physical System" "Federated Learning in Cyber-Physical System"	73 37 51 45	73 37 51 45	22 15 18 10
Web of Science	"Artificial Intelligence Technique in Cyber-Physical System" "Machine Learning in Cyber-Physical System" "Deep Learning in Cyber-Physical System" "Federated Learning in Cyber-Physical System"	49 38 45 43	49 38 45 43	20 17 16 10

3. Background Details

This section explored different techniques and methods for modeling threats, Human-machine teaming protection, domain vulnerabilities, and security resources. We have also presented the structured framework for artificial intelligence in cybersecurity: identification, protection, detection, response, and recovery. We have also mentioned the types of attacks along with AI-based applications. We highlight types of datasets, their format and tags, and their year of origin. We will also discuss the reasons for writing this chapter and the aims and priorities.

3.1 Framework of AI in Cyber physicalSecurity

Due to increased knowledge of how susceptible AI segments are to malicious activity, worries about the CPS integrity of the entire information-handling pipeline in which AI segments are deployed have been addressed. The various application of the CPS system is described below.

- Industrial and political campaigns
- Smart Grid and its services
- Transporation system
- Healthcare and ambient assisted living

Multiple applications can be affected because of secret dependencies in the pipeline. When using AI as a part of a system, research is required to develop a strategy, engineering principles, and industry standards [44]. Threat modeling, security techniques, domain weaknesses, and acquiring human-machine learning should be included. These models must allow for iterative concepts of attacks and improvements, be built with the help of an AI professional, and take into account data availability and integrity, access controls, network orchestration and activity, conflict resolution, privacy, and a complex policy setting [45-47]. Engineering concepts should be focused on science, group experience, and AI component functionality study that involve redundancy and other mechanisms to make AI-enabled systems more trustworthy.

The primary purpose of identification in AI is to develop an organizational way to control cybersecurity risks associated with CPS systems, people, assets, data, and capabilities [51-53]. In business, various resources are used to support risk-related functions and maintain consistent operations to support multiple business needs and risk management strategies associated with cybersecurity risks management to focus and define its efforts [54-57]. As shown in Fig 4, the first stage in the AI framework is identifying vulnerabilities applied in various fields, including CBT systems [58-59], intelligent production, and grid systems [60]. The other stage, known as protection, describes the necessary vital points to ensure the mode of delivery for infrastructure-related services [61]. To support the protection function, it must retain & limit the ability for potential cybersecurity events

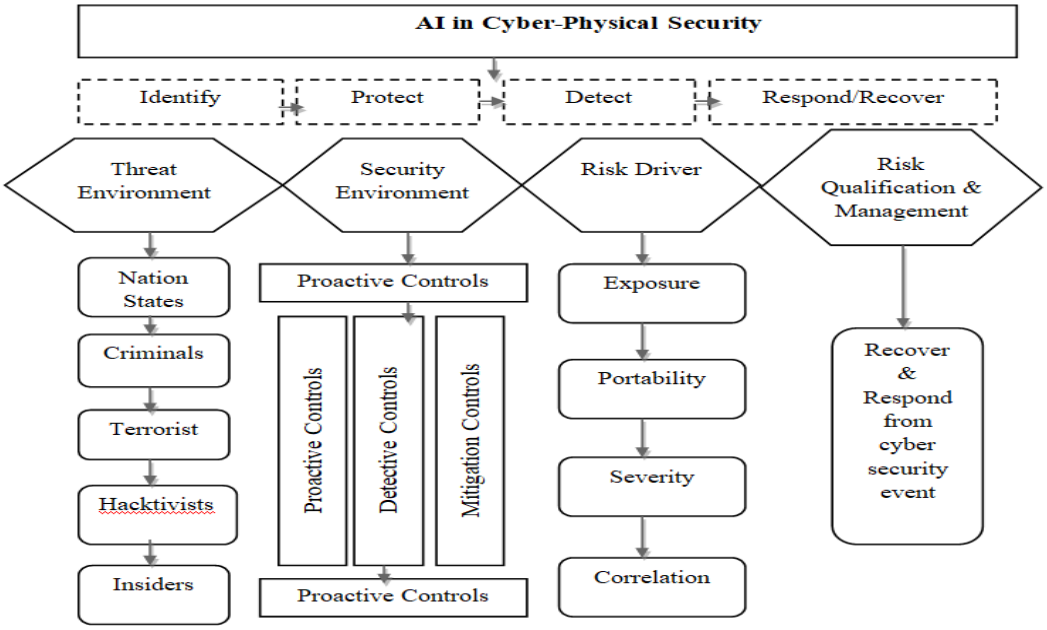

Figure3: AI Framework of Cyber Security

The primary purpose of identification in AI is to develop an organizational way to control cybersecurity risks associated with CPS systems, people, assets, data, and capabilities [51-53]. In business, various resources are used to support risk-related functions and maintain consistent operations to support multiple business needs and risk management strategies associated with cybersecurity risks management to focus and define its efforts [54-57]. As shown in Fig 4, the first stage in the AI framework is identifying vulnerabilities applied in various fields, including CBT systems [58-59], intelligent production, and grid systems [60]. The other stage, known as protection, describes the necessary vital points to ensure the mode of delivery for infrastructure-related services [61].

3.2 Network, Threat and Design Goal of CPS

A. Network Model

The vital advantage of the network model is that it provides a trusted data network for storing the information generated on the internet. This information includes the identities of CPS devices. Cyber-physical users are actors who directly interact with the devices [69-71]. These systems help retrieve the data from the trusted networks to perform the cryptographic identities connected with the trusted model. CPS devices have the capabilities of computations and cryptographic identities using blockchain so that communication becomes easy with the processes to send and receive data signals.

B. Threat Model

A cyber-physical attack is a violent and transparent attempt by an organization or entity to breach the information system of another person or organization [55]. Eavesdropping involves monitoring non-secure CPS network traffic to gain sensitive data. [75].Denial service attacks (DDOS) are distributed system attacks targeting cyber-physical resources. They are frequently carried out by Botnets, which consist of a large number of infected devices that are hijacked by DDOS attacks. Another cyber threat effect is confidentiality required for the security of private information [76-78]. The next threat model is integrity, where data can not alter without proper permission. The availability means the resource available in case of system and another hardware failure. The non-repudiation action would have to occur at the time interval [79]. Accountability is where an entity is responsible for its work [80].

C. Design Goals

One of the most prominent approaches is decentralization to achieve effectiveness and rapid decision-making in real-world applications. The decentralization of networks is necessary to maintain the security-related issues of CPS. A CPS network should no longer rely on a centralized entity anymore because it may cause performance issues [37]. In CPS distributed network environment, the entities must be unable to estimate each other's transactions. Therefore, uncertainty is highly required in distributed CPS, where privacy is a matter of concern.

The authentication process is a critical goal in real-world cyber-physical systems in which unauthorized access can quickly enter bogus data into a CPS device. For this, the blockchain-based system must assure the authenticity of the data from the trusted network

4. Reported Work

This section describes the various artificial intelligence approaches for Cyber-Physical systems. We have also represented the comparative study of different AI-based techniques such as graph-based approach, intrusion detection tree approach, other procedures and methods of deep learning, machine learning, and federated learning. Finally, the results obtained from different techniques have been demonstrated through equations and algorithms.

4.1 Graph-based approach

The graph-based approach may be a multi-graph representation of the information with middles compared to CPS objects or concepts and edges interfacing concepts that share similitude [81-83]. The chart regularly contains both named information and unlabelled information. HTTP requests are sent to a web server by a client. Choras et al. [24] presented a graph-based system that uses a set of standard expressions that represent typical web requests sent by clients to a web application. In this case, the map G= (V,E) is an undirected chart with vertices vi V and edges(vi,vj) E connecting the adjacent vertices. The vertices in the form correspond to the HTTP message (HTTP Ask sort, URL, parameters). An example of what happens after an HTTP GET request (given by Eq. 1) is as follows:

Algorithm 1: Implementation steps for the graph based approach:

1. for each $(vi, vj)a??E$calculate edge weights w (dissimilarity between vertices vi and vj).
2. Arrange edges ascending according to their weights w values.
3. Begin with segmentation$S0$, where each vertex v is assigned to its component.
4. Iterate over the sorted set of edges for $q = 1, \ldots, m$ and perform the following steps:
   - Let $Cq - 1i$ be the component of $Sq - 1$ containing vi and $Cq - 1j$ be the component of Sq−1 containing vj .
   - Assign $Sq = Sq - 1$
   - Merge $Cq - 1i$and$Cq - 1$
   - Segments whenever dissimilarity between them falls the predefined threshold and update Sq accordingly.
5. Return Sm as a segmentation result S.

In the above algorithm presented a graph-based system that uses a set of standard expressions that represent typical internet requests sent by clients to a web application. In this case, the map G= (V,E) is an undirected chart with vertices vi V and edges (vi,vj) E connecting the adjacent vertices. The vertices in the form correspond to the HTTP message (HTTP Ask sort, URL, parameters). Paudel et al. [95] proposed a graph based method for defining a common behavior in connected CPS devies, IoT devices. The source IP and the destination IP are also called nodes. The operation stream between the source and destination IP addresses is referred to as an edge between the hubs given in Eq. 5.

$$\boldsymbol{Gs} = \{\boldsymbol{Gi}, \boldsymbol{Gi} + \mathbf{1}, \ldots, \boldsymbol{Gt}, > +\mathbf{1}, \ldots\} \quad (5)$$

Let be a chart stream where each Gi indicates a chart at each one minuscule short-term. The inventor has considered a graph as given in Eq. 6.

$$\boldsymbol{Gi} = (\boldsymbol{v}, \boldsymbol{e}, \boldsymbol{f}) \quad (6)$$

as a generic undirected heterogeneous graph is given in Eq. 7.

$$\exists \boldsymbol{v} \in \boldsymbol{A}(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{A} \wedge \boldsymbol{x} = \boldsymbol{y} \boldsymbol{and} \forall \boldsymbol{e} \in (\boldsymbol{x}, \boldsymbol{y}) \quad (7)$$

There's an edge going from vertex x to vertex y and (x, y) is an unordered match [88-90]. At whatever point a modern graph Gi arrives within the stream, a biased-random walk of a settled length l is performed from each hub in Gi extricating a walkway p is defined as Eq. 8.

$$\boldsymbol{Gi} = \{\boldsymbol{v1}, \boldsymbol{v2}, \ldots, \boldsymbol{vl}\} \quad (8)$$

Here, the n-shingles are then constructed from a walking path, Nguyen et al. [91] also have proposed a lightweight strategy for recognizing IoT botnet attacks for the cyber guards, which is based on extricating high-level highlights from function–call charts, called PSI-Graph, for each executable record. **4.2 Intrusion Detection Tree Approach**

Intrusion Detection Tree Approach is the foremost practical framework that can handle the interruptions of the computer environments by activating alarms to create the investigators take activities to close down this interruption on the CPS network. Sarker et al. [107] suggested an Intrusion Finding Tree approach for Cyber-Physical attack detection. When the security highlights are ready, the developer has created a tree-like display to enable users to develop a data-driven, intelligent decisions interruption discovery environment. Rather than using all of the security highlights available within the provided dataset, the authors consider the authors' preferred security highlights, calculated by their significance score and ranking. Experts began with a root hub to plan a tree-like demonstration. It incrementally generates a related tree department by breaking down a given preparing dataset into smaller subsets. Hao et al. [48] have also defined the "Gini Index" as used to discern the property for the root hub in each step. Quality with a lower Gini list is chosen [94-96]. Reducing the highlight measurements by deciding the include significance and positioning, reducing highlight measurements by agreeing on the importance and placement of the highlights, and building a multi-level tree with the chosen imperative highlights in mind. In a given interruption dataset, an example of an IntruDtree considering a few highlights such as f slack, gain, duration, logged in, and their test values. Calculation lays out the general procedure for constructing an anIntruDTree as defined in Eq. 9.

(9)

4.3 Federated Learning in Cyber attack

This section gives a survey of the commitments made by distinctive analysts within the field of federated learning in cyber-Physical security in conjunction with a comparative investigation based on assaults, the strategy utilized, and the related challenges in the planning secure stage. Niknam et al. [95] have discussed an open presentation to the common thought of unified learning conjointly proposed a few conceivable applications in 5G systems, and depict key specialized challenges and open issues for future inquire about on unified learning within the setting of wireless communications [108]. Afterward, Liang et al. [76] proposed to expand combined learning with nearby representation learning on each gadget to memorize valuable and compact representations from crude information.

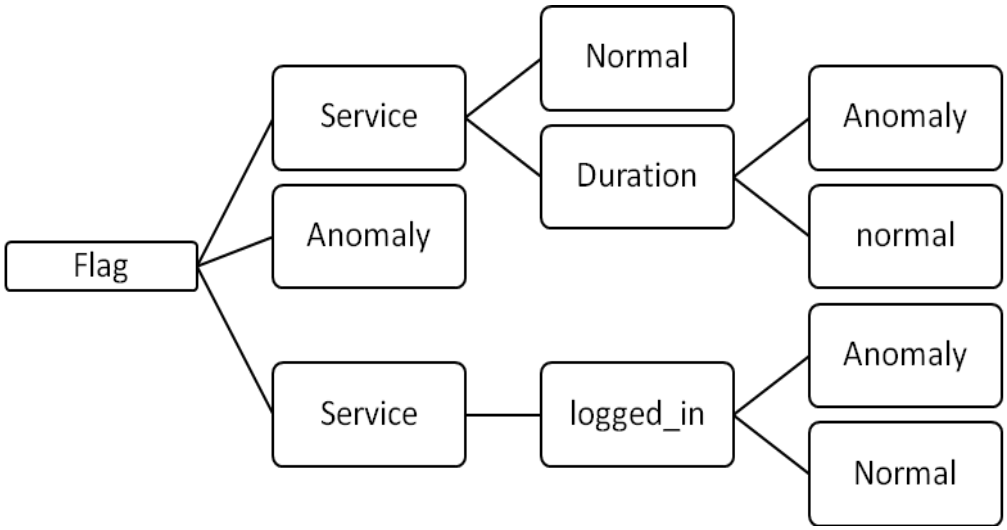

Figure 4: Intrusion Detection Tree Approach

Pang et al. [94] found it successful against nearby models which give adaptability in managing with heterogeneous information and can be adjusted to memorize reasonable representations that muddle ensured traits such as race, age, and sexual orientation. Caoet al. [21] have also explored and actualized the combined learning system as a conveyed profound learning system for privacy-preserving and parallel preparing with physical devices..

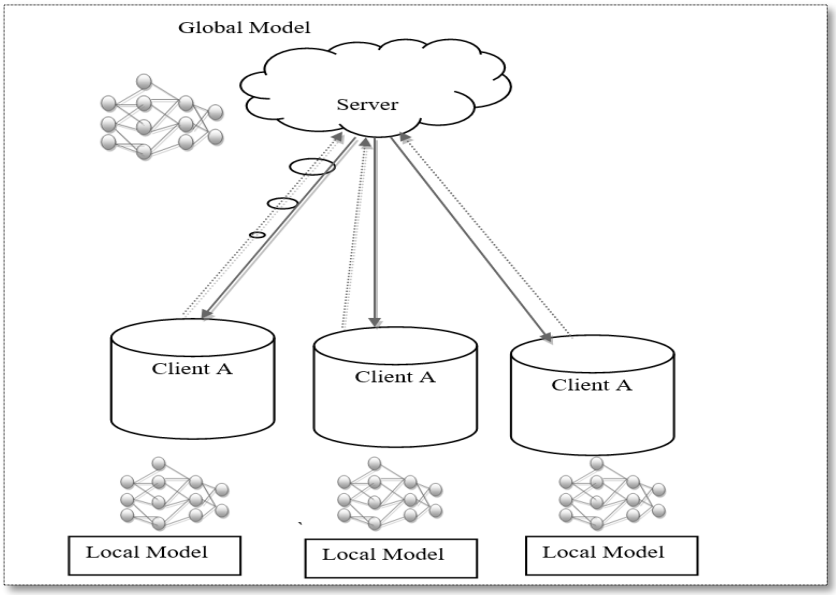

Figure 5: Federated learning model for data security

Figure5 outlines the fundamental design and relationship between the local and global model of a federated learning life cycle [75], and bolts show that, as it were, the totaled weights are sent to the worldwide information lake, as contradicted to the nearby information itself, as is the case in routine ML models [113]. As a result, FL makes it conceivable to realize superior utilization of assets, minimize information exchange and protect the security of those whose data is being exchanged [115].

4.4. Deep Learning-based Attack Detection

In this section, work done by various authors in the fields of deep learning models in cyber-Physical security. Li et al. [64] have proposed a non-specific system for veering DL cognitive computing methods into Cyber Forensics (CF) from now on alluded to as the Profound Learning Cyber Forensics (DLCF) System. DL employments a few machine

learning procedures to fathom issues through the utilization of neural systems that recreate human decision-making [7]. Based on these grounds, DL holds the potential to significantly alter the space of Cyber Forensics (CF) in an assortment of ways as well as give arrangements to measurable investigators [66]. Sebastian et al. [93] moreover proposed a strategy of mechanizing post-exploitation by combining profound support learning and the PowerShell Realm, which is popular as a post-exploitation framework. Rieke et al. [99] too displayed a novel assault strategy leveraging the assault vector, which makes profound learning expectations now not diverse from irregular speculating by debasing the precision of the forecasts. Li et al. [74] have moreover proposed a deep setting displaying engineering (DCM) for multi-turn reaction determination by utilizing BERT as the setting encoder.

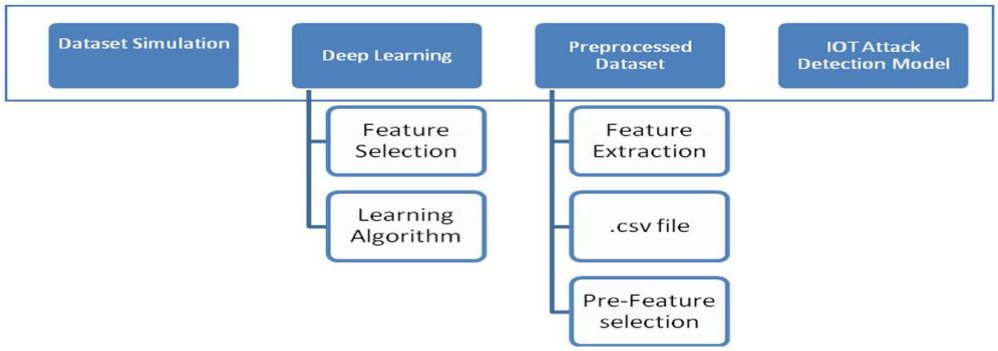

Figure 6: Deep Learning Model for the Cyber Security

As shown in Figure6, for text-based processing, critical component captures records are first translated to Semicolon Values (CSV) records. Following that, the CSV files are passed into the framework's highlight preparation module.The authors in [121] have described the features derived from the operation stream data found in the CSV files. To begin, include discussion preparation is linked to a few highlights discovered in raw datasets. Zeng et al. [4] have moreover illustrated a novel approach for organizing the Interruption Location Framework (IDS) for cybersecurity utilizing unsupervised deep Learning (DL) strategies. Exceptionally regularly, the administered learning and rules-based approach like Grunt get an issue recognizing modern attacks. Lee et al. [6] have too displayed the examination, tended to security pros, of Machine learning methods connected to the location of interruption, malware, and spam in CPS applications

Another Approach is Convolutional Neural Network (CNN) Based Methods for Attack Detection, Abnormality estimation and significance arrangement are two commonly used methods in the significant learning space, and CNN includes them both. CNN's multilayer recognition versions, in particular, are designed with limited preprograming in mind. CNN's basic model comprises contribution and abdicates layers, as well as numerous covered-up layers that link density, pooling, and full relationship layers. The CNN layer's basic model includes a variety of inputs and abdicates between layers to join with density, pooling, and maximum affiliation.

4.5 Machine learning in Cyber Security

Deng et al. [30] have proposed a method of recognizing malicious address (IP Address and port no.) has been displayed, which recognizes and squares if any suspected cases are found and passes the substance to the concerned client. Authors have utilized the SVM method for classification, location, and expectation of Boycotted IP addresses and boycotted port addresses. The proposed framework has been tried on the datasets of IPs and port addresses. The dataset has been populated with the records of unique IP Addresses and harbor addresses and with noxious IP and harbor addresses and was tried. Whose comes about are calculated by taking an average of 50 unique IP addresses, harbor addresses, and pernicious IP and Port addresses[127]. Jaiyen et al. [56] have also presented methods for a detecting the cyber-attack in the system, Progressive Choice Tree Learning (IDTL), that use the rule via Incremental Direct Discriminant Examination (ILDA) in conjunction with MahalaNobis separate for classification of the progressive tree by substantially reducing highlights that improve the classification of a variety of adverse data[128].

The outcomes of the tests uncovered that the proposed strategy could make strides in classification exactness compared with other strategies.

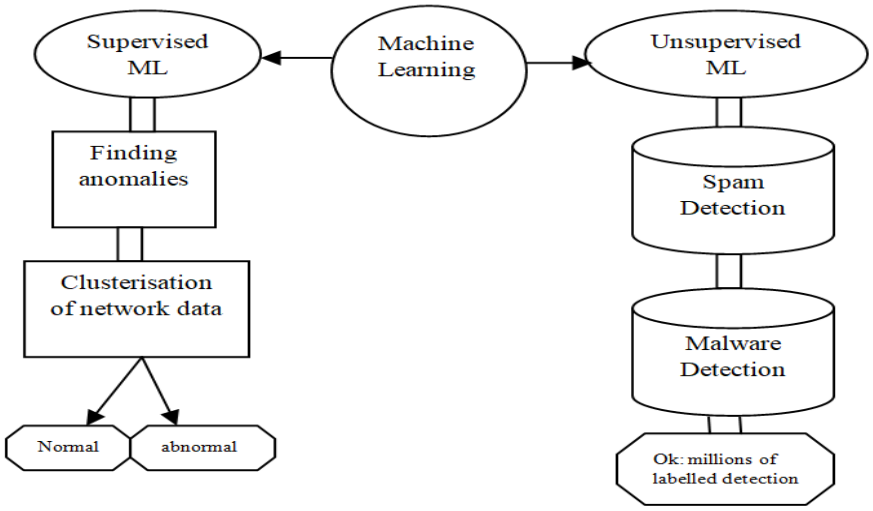

Figure 7: Machine Learning Model for Cyber Security

In Figure7, machine learning based cyber security detection engine received all relevant input [134], network, programmed binaries by matching with signature value from the extracted features includes IP addresses and network data. This static input based matching process used to identify the attacks after a long system process [135]. Chowdhury et al. [24] have also proposed a broad system to categorize and distinguish malicious programs to protect delicate information against pernicious dangers utilizing information mining and machine learning classification procedures [138].

In the set of N choice factors, m represents number for targets fi, c is the number of imperatives c(X),x(L)i is the lower bound on the ith choice variable, and x(U)i represents upper bound on the I choice variable. Moreover, Wu et al. [119] have depicted the concept as a vision of progressed fabricating framework coordinates with advances such as Web of Things, Cloud Computing, Sensors Arrange, and Machine Learning. In this investigation, physical information machine learning approaches are created and coordinate for identifying Cyber-Physical assaults in CMS. The another author have moreover depicted different sets of heuristics machine learning methods that have been illustrated to be appropriate for specific issues and indeed for distinctive stages of the same issue[140]. These heuristics are chosen to join different look characteristics and incorporate diverse look practices.

4.6 Signature Based Malicious Behavior Detection

Malware has threatened computers, systems, and foundations since the eighties. There are two significant advances to protect against this, but most organizations depend nearly only on fair one approach, the decade's ancient signature-based technique [2]. The more progressed strategy of identifying malware utilizing behavior examination picks up fast footing but is still generally new. When an anti-malware arrangement supplier distinguishes a question as pernicious, its signature is included in a database of known malware. These storehouses may contain hundreds of millions of marks that distinguish pernicious objects. This strategy of distinguishing malicious objects has been the essential method utilized by malware items and remains the base approach utilized by the most recent firewalls, mail, and organizes gateways. Sen et al. [114] have recommended an approach based on input design and coordinating relationship signatures with the sifted logs from the overstep. Signatures are carefully created for tall discovery exactness. Moreover, for identifying asked necessary consents at runtime, implied consent ask commands were recorded as marks. Feng et al. [37] have proposed signature-based behavior-based discovery methods that utilize API calls that are promising for discovering malware variations [71]. A signature-based discovery strategy matches an

already produced set of marks against the suspicious tests. A signature could be an arrangement of bytes at particular areas inside the executable, a standard expression, hash esteem of double information, or any other groups made by malware examiner which ought to recognize malware occasions precisely and their relationship [136

5. Comparative analysis

The cybersecurity framework discussed in this survey finding are the various types of attacks using deep learning, machine learning, and federated learning algorithm[138]. Cybersecurity problems can be found in various places, including mail, operating systems, cars, entertainment, banks, businesses, financial institutions, and online data storage, to name a few. For this research study, we chose a deep learning, machine learning, and federated learning-based cybersecurity attack detection concept. There are approximately 58 papers relevant to the survey subject that has been chosen [98]. Various criteria are used to estimate and relate the efficiency and performance in the reported output [140]. The comparative study for types of attack, technique, and challenges is discussed in this Table 4.

Table 4: Comparison of various Artificial Intelligence Model

Authors	Types of Attack	Techniques used	Challenges	Reported Output
Paudel et al. [95]	Model-poisoning	Poisoning Resilience Defence	Bandwidth Communication, noise interference &Robustness was not discussed in this reported study.	Error performance=0.2
Phong et al. [76]	Privacy,training issues, real-world tasks	FEDAVG, Local only, MTL, LG-FEDAVG	Methods for learning fair representations were not discussed in the reported work.	Cross-entropy loss 100-piece batch 0.01% learning rate 0.9 Momentum 0.0005 learningrate decay.The number of global epochs equals 100.
Cao et al. [21]	Model-inversion attacks, man-in-the-middle attack, Insider attacks	Deferentially private stochastic gradient descent algorithm, classification, and segmentation	Lack in speed up the process and reduced the amount of data exchanges.	Speedup=up to 9* Reduced the amount of data exchanged=up to 34%,Performance=4:5%
Zeng et al. [135]	UAV antenna angle, fading, and	Joint power allocation and scheduling design	There aredelay constraints at uplink and downlink	Bandwidth=35%

	transmission delay modifications			
Liang et al.[80]	Poisoning attacks and inference attacks	Game-theoretic research	Robustness of federarted learning system is still a major concerns	Optimal accuracy has been achieved
Gomez et al. [44]	Encryption of model submissions, secure authentication of all parties, traceability of actions, differential privacy, verification systems, model confidentiality, execution honesty as well as precautions	Medical NER Model Bi-LSTM and CRF, CNN	Formal security verification and evaluation of the proposed methods were not discussed.	Accuracy= 84%
Liang et al. [81]	Data poison attack, user Datareconstruction attack	Quantified indicator, memorization management	Eliminate unexpected memorization is still not addressed by the authors.	Accuracy=87.49 %
Enthoven et al. [36]	Active or passive attacks, Model poisoning	Gradient Subset, Robust aggregation Homomorphic Encryption, SMC, Dropout.DP	Effectiveness and Defensive methods and strategies against attack were not discussed.	Accuracy= 76.8%
Muniyandi et al. [89]	Jamming attack	Client group Prioritization	Architecture, framework, reliability, and techniquesfor decentralized the global model was not discussed.	Accuracy= 82:01% Outperforms= 49:11%
Dong et al. [35]	Privacy leakages semi-honest adversaries	TernGrad. homomorphic encryption	There is the need to focus on resisting the more powerful adversary	Better in communication and computation and more Accurate design
Haris et al. [49]	Malicious adversary, passive attack, model inversion	Generative Adversarial Network (GAN)	Lack in the evaluation of and study on the high-dimensional dataset and complex neural The network was missing.	Functionality and accuracy 90.8% ,91.5%
Kang et al. [63]	Data poisoning attack, adversarial attacks	Reputation-based scheme	More accurate and efficient validation schemes were not discussed.	Accuracy.= 76.12 percent thresholds=1.6

Ashok et al. [66]	Alter global model parameters	Blockchain-based FL, game-theoretic incentive mechanisms can	Performance evaluation of memory, accurate data for the proposed algorithms were not performed	response time =optimal CPU-frequency= maximize utility function =maximize the
Zoph, et al. [10]	Adversarial attacks	Lagrange Coded Computing (LCC), secrete sharing, key agreement and public key infrastructure	A fair comparative analysis of the existing algorithm was missing	FedAvg= 93.19
Sathyanarayan et al. [108]	differential privacy	Differentiallyprivate (FNAS). private gradient sharing or Gaussian mechanism	gradient compression, periodic updates, diverse example selection methods were missing	Variance of Noise=0.5 Validation error (%)=14.0 ± 0.32
Han et al. [48]	Malicious threats and data contamination attacks	Uniform probability, Federated Averaging algorithm	The size of the model, bandwidth and the reliability of client connections were not addressed.	Weight decay = 4 × 10−4. Accuracy= 40.3%
Stankovic et al. [8]	Poisoning attacks, backdoor attacks	Fine-pruning, Byzantine-tolerant distributed learning	The design of the Robust system in federated learning was not discussed.	Accuracy=99%
Bhagoji et al. [15]	Poisoning attack	Layer wise Relevance Propagation (LRP) techniques	More sophisticated detection strategies at the server-side were not discussed	Accuracy =91.7%
Thing et al. [113]	Data leakage and misuse, end-users privacy	Communication-efficient federated learning techniques	Optimization methods for the low-frequent high-volume communication were not discussed.	Sparsity rate= 0.001 accuracy=55%
Karie et al. [61]	Cyber-based attacks	Clustering techniques, Deep learning cognitive computing techniques	Digital forensic investigating techniques were not reported by authors in detail.	Accuracy=optimum
Muniyandi et al. [89]	Vulnerabilities, patching issues	Deep reinforcement learning and the PowerShell Empire	The training environment, Frameworks, and methodology used by the authors is not appropriate	Probability=60% Efficiency=maximum
Parg et al. [97]	Mind Control attack	TensorFlow, CNTK, and Caffe running on CUDA	GPU function vulnerabilities were not reported in this study.	Accuracy= 0.496
Li et al. [74]	Abundant yet noisy contextual information, back-channeling	Retrieval-based methods, generation-based methods	Performance enhancement technique was not addressed.	Pushing recall= 86.8% E-Commerce Dialogue corpus= 68.5% MAP and MRR= 61.6% and 64.9%

Perera et al.[96]	Dispatch problem.	The model with such a white box. Value-Aware Model Learning (VAML), Policy-Aware Model is manifestations of data-driven models (PAML)	An adequate test case to validate performance was not reported by the authors.	Improvement= 10–20% considerable effort=13%
Dixit et al.[32]	Phishing, spear-phishing, a password attack, and a denial of service attack are all examples of phishing.	CNN-Convolutional Neural Network, AE-Auto Encoder, DBN-DeepBelief Network, RNN, GAN, and DIL-Deep Reinforcement Learning	An effective algorithm and robust design for cyber security were not discussed.	Accuracy= 99.85%.
Yuan et al. [122]	Adversarial attacks	Deep Reinforcement Learning (DRL)	Lack in the Dataset and defensive measures.	Qmax=80 Reward=10 Policy= Epsilon Greedy Epsilon=0.1
Zhanget al. [123]	Cyber-threats, ransomware, and other forms of cybercrime are all on the rise.	Firewalls, cryptographic encryption and decryption methods, anomaly detection of intrusion	Architectures and Algorithm for cyber security use cases was not reported	Accuracy= 0.968 Precision=0 .814 Recall= 0.984 F1-score= 0.891
Dai et al. [28]	Cyber-attack	N-fold cross-validation	Lac in the performance on different datasets.	Accuracy =99(%) DR = 99.27 (%) FAR= 0.85 (%)
Zeng et al.[4]	Cyber-attack	Unsupervised deep learning, K-means	More accurate and efficient validation schemes not discussed	Accuracy =100(%)
Lee et al. [6]	Adversarial attacks	RF (Shallow Learning) and another based on FNN (Deep Learning)	Have not provided solutions to mitigate detecting specific threats	F1-score =0.90 Precision=0.91 Recall=0.73
Chen et al. [22]	Malicious flow detection.	Tree-Shaped Deep Neural Network (TSDNN),oversampling method, and the under-sampling Method	Effectiveness and Defensive methods and strategies against attack were not discussed.	Accuracy= 99.63% Precision= 85.4%

Sánchez et al. [106]	Adversarial attacks	Complicated data processing and AI based techniques	Various use case application by involving IOT system was not reported in this study	f1-score = 99.33% FPR = 0.23%
Dangi et al. [29]	Malicious Socket address	Support Vector Machines (SVM)	The study was limited to malicious URL (IP) andport address	Accuracy = 95.6%
Jaiyen et al. [56]	Anomaly-based IDS detection	IDTL(Incremental Decision Tree Learning), Incremental Linear Discriminant Analysis (ILDA)and Mahalanobis distance	Incremental learning system methodology neither has nor included by authors.	IDTL accuracyNSL-KDD-75.71 SAME -96.04 Phishing-91.05
Lee et al. [6]	DGA Detection and Network Intrusion Detection	RF classifiers, FNN, DNN	Not considering the concepts of adversarial learning	Intrusion detection F1-score- 0.7985 DGA detection classifiers F1-score- 0.8999
Ferdowsi et al. [38]	Safety logs, alert data information, and analysis of insights to identify riskyuser	Multi-layer Neural Network (MNN),Random Forest (RF), SVM	Other learning algorithms should be considered to further improve the detection accuracy.	Average lift== 20%
Caspi et al. [41]	Phishing detection, Network intrusion detection	Hierarchical Clustering (HC), K-Medoids (KM)	Spam detection, virus detection, and surveillance camera robbery not discussed in the study	Success rate For segmentation = 66.2 %
Sen et al. [114]	Unauthorized access, destruction, theft, or damage	BPNN architecture,Neural Network	Execution time can be further minimized	Accuracy= 97%
Chowdhury et al. [24]	Data security, Cyberthreat, Malware	Binary associative memory (BAM),Multilayer perceptron (MLP)	High False Positive Rate.	Accuracy=98.6 %
Doku et al. [33]	Risk associated with storing data	Interest Groups (IGs),Proof of Common Interest (PoCI)	Faced Generative Adversarial Network problem	Optimum Accuracy Achieved
Pang et al. [94]	Cyber Attack, TCP SYN flooding	Federated Network Traffic Analysis Engine (FNTAE), K Nearest Neighbor (KNN) Classifier	Real-time intrusion detection experiments using Live net traffic monitoring and analysis Was not reported by the authors	Accuracy=98.19 8%

Sarkar et al. [107]	Network Attack	K-NN(K Nearest Neighbor)	Lack in the framework, architecture, and design used for the effectiveness of the system	Accuracy=85.69 %
Sathyanaryan et al. [108]	Unknown attack	KYOTO 2006+ data set,Machine Learning technique	Designing of a Robust system in machine learning was not discussed.	Accuracy =97.23% Instances= 97.23%. High true positive rate (99%)
Sen et al.[114]	Military and commercial sectors cyber attack	KDD data set, Chi square, Information Gain and Relief	Major attacks in the KDD dataset were not addressed by the authors	Accuracy= 95.0207
Saltzer et al.[128]	Cyber-Physical attack	k-Nearest Neighbors, Computer Numerical Control (CNC)	Various detection methods and data process used in the system was not appropriate	Accuracy=93.8 %
Sicari et al. [131]	Denial of service(DOS), User to Root(USR),Remote to Local attack(R2L)	KDD Cup 1999 Dataset, ISOT (Information Security and Object Technology)Dataset	New datasets for solving various national and international cyber-attacks were not addressed.	Command Execution=23% SQL Injection= 18% Path Traversal=18%

6. Future Prospective

Artificial intelligence is preferably required to solve complex problems, and the cyberphysical security area comes under that category. AI is best suited to solving some of the world's most challenging problems, and cyber-physical security is one of them [1]. Machine learning and artificial intelligence are becoming increasingly important with today's ever-increasing cyber-attacks and the proliferation of gadgets [12]. Artificial intelligence (AI) can keep track of digitized risk discovery and respond more quickly than conventional software-based approaches.

- **Detection and Response Time**

Identification of simple matters can quickly speed up through cross-referencing various attentions, and different ways of secure data are possible through AI today. Up to this time, Expertise assists in the betterment of CPS security by providing different mechanisms with the needs of occurrences of events. On the other hand, AI frameworks also provide the way for the enhancements in the actions based on the plans-based recommendations [42].

- **Network Security plans and recognition**

The development and methods for CPS assembly of security plans and recognition of the system's geographic link are the two significant aspects of system security. These practice units are pretty tedious to perform, so utilizing the AI procedures would get speed up. It will be observing and learning traffic styles even as suggested security measures make preparations. That does not save time in either situation, nor does it save a significant amount of work and money that are prepared to or can relate to areas of a mechanical flip of cases and development [69].

- **Controlling Phishing Detection and Prevention**

Phishing is a commonly used computerized attack technique in which software engineers communicate their payload using a phishing trap. Phishing messages are prevalent; one out of every ninety-nine messages may be a phishing attempt. Fortunately, AI-ML can agree to persuasion work in phishing prevention and avoidance for CPS [22]. More

than 10,000 active phishing sources will be identified and followed by a computer-based insights metric capacity unit, responding and correcting loads faster than humans. To boot, AI-enabled machine learning works at sifting phishing threats from all over the planet. There is no impediment in its comprehension of phishing endeavors to a chosen soil science region [27]. Computer-based insights have made it conceivable to partition between a fake web location and a real one chop-chop.

- **Secure & Stable Authentication**

Passwords have effectively been associated with highly acute administration in terms of confidently [24]. Physical identifiable confirmation is the most common method of secure CPS confirmation, in which AI uses different components to say apart from a private [30]. To encourage search inside, a phone will use unmistakable finger impression scanners and facial affirmation. The process includes the software analyzing precious information from all over the world and using fingers to acquire it if the login is correct. Aside from that, AI will look at various factors to determine whether or not the buyer is authorized to check into some particular device [39]. The system looks at things like how fast you type and how many mistakes make when typing.

- **Behavioral Analytics**

Another critical application of AI in cyber physical security is its ability to investigate actions of CPS. This implies that cubic centimeter calculations will figure out how to make a case by breaking down how to use gismo and online phases [69]. The particulars would incorporate everything from regular login times, and data preparation conveys to writing and reviewing examples of the AI calculations pick up on unusual exercises or other behavior that is not typical cases [74]. It would be flagged as having been bundled up by a suspicious buyer or probably sq. the buyer. It works out that stamp of the AI calculations is frequently anything from large online transactions sent to addresses other than relate a sudden spike in report exchange from archived envelopes or relate a sudden change in composing pace [101].

- **AI in preventing Online Frauds**

Companies should be able to detect a computerized attack sooner rather than later. This would be having the option to obstruct whatever the adversaries are attempting to accomplish [99]. AI is a branch of computer science that has proven to be a game-changer in detecting advanced threats for CPS [117]. It all depends on how to look at data and then get a chance to do so. It has recently taken advantage of data system flaws. AI empowers PCs to use and change equations based on the data they have gathered, learning from it, and determining the following steps to take. In a cyber-physical security context, this may imply that AI allows the machine to predict threats and detect inconsistencies with far greater precision than any human.

7. Conclusion

As CPSs are likely to play a main role in the plan and development of forthcoming engineering system. The main inkling of CPS is on the design assurance and cyber-physical security for the complex CPS system. This paper provides a definition and background of CPS. The fast and significant development of CPS system affects the people way of life and enables a broader range of facilities. The security framework and network threat model were also discussed in detail. The technical in this paper, we presented our research outcome in AI based methodologies in cyber-physical systems. We have started with recognition of that can address the security, integrity and privacy of the network. However, using AI methodologies in CPS has own challenges. Here, Controllers also direct the received quantities to the core control servers and perform the selected commands. In CPS, system operatives should be alert of the current position of the controlled objects. Thus, we have started with the framework of AI based methods In CPS. As AI is the latest technologies which have potential to improve the security if CPS.

In order to highlights the various AI based methods which are relevant to the current security of CPS systems and discussed. The comparison table provide the main contribution of authors in the areas of types of attack detection, techniques used and challenges faced for current security architecture, discussed in the study and future prospective of each chapter.

We have also considered that cyber resilience depends on the effective security controls that protect the authenticity, confidentiality, reliability, resilience, and integrity. Finally, we have emphasis on providing a future research inclination and unique features in this field. We have also identified the betterment of CPS security by providing different mechanisms, CPS assembly of security plans and recognition, for ensuring the prevention and avoidance for CPS, to determine the common method of secure CPS confirmation, the development of the security protocol. This research work would help to researcher and academicians in the field of CPS security.

References

1. Zeadally, S.; Jabeur, N. Cyber-Physical System Design with Sensor Networking Technologies; In-stitution of Engineering and Technology, **2016,** 48 (2), 78–82.
2. Abeshu, A.; Chilamkurti, N. Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing. *IEEE Commun. Mag***. 2018**, 56 (2), 169–175.
3. Sheth, A.; Anantharam, P.; Henson, C. Physical-Cyber-Social Computing: An Early 21 St Century Approach**.** *IEEE Intell. Syst* **2013**, 28 (1), 78–82.
4. Zeng, J.; Yang, L. T.; Lin, M.; Ning, H.; Ma, J. A Survey: Cyber-Physical-Social Systems and Their System-Level Design Me-Thodology. *Future Gener. Comput.Syst* **2016,** 22 (1), 78–81.
5. Liu, C. H.; Zhang, Y. Cyber Physical Systems: Architectures, Protocols and Applications; *CRC Press, Taylor & Francis Group Florida*, **2016,** 38 (1), 18–22.
6. Lee, E. A. Cyber Physical Systems: Design Challenges. In 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC); *IEEE*, **2008,** 18 (1), 28–30.
7. Johansson, K. H. Control of Cyber-Physical Systems: Fundamental Challenges and Applications to Transportation Net-Works; *Lübeck Germany*, **2014,** 48 (1), 22–25.
8. Stankovic, J. A. Research Directions for the Internet of Things. *IEEE Internet ThingsJ*. **2014**, 1 (1), 3–9.
9. Chhetri, S. R.; Lopez, A. B.; Wan, J.; Al Faruque, M. A. GAN-Sec: Generative Adversarial Network Modeling for the Security Analysis of Cyber-Physical Production Systems. In 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE*); IEEE*, **2019,** 22 (1), 38–41.
10. Zoph, B.; Le, Q. V. Neural Architecture Search with Reinforcement Learning. arXiv [cs.LG], **2016**.
11. Zoph, B.; Vasudevan, V.; Shlens, J.; Le, Q. V. Learning Transferable Architectures for Scalable Image Recognition. In 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition; IEEE, **2018,** 28 (1), 78–82.
12. Baruch, M.; Baruch, G.; Goldberg, Y. A Little Is Enough: Circumventing Defences for Distributed Learning; **2019**.
13. Beaver, J. M.; Borges-Hink, R. C.; Buckner, M. A. An Evaluation of Machine Learning Methods to Detect Malicious SCADA Communications. In 2013 12th International Conference on Machine Learning and Applications; *IEEE*, **2013**.
14. Brunton, S. L.; Kutz, J. N. Data-Driven Science and Engineering: Machine Learning, Dynamical Systems, and Control; *Cambridge University Press: Cambridge, CA*, USA, **2019**; Vol. 1.
15. Bhagoji, A. N.; Chakraborty, S.; Mittal, P.; Calo, S. Analyzing Federated Learning through an Adversarial Lens. arXiv [cs.LG], **2018**.

16. Bonawitz, K.; Eichner, H.; Grieskamp, W.; Huba, D.; Ingerman, A.; Ivanov, V.; Kiddon, C.; Konečný, J.; Mazzocchi, S.; McMahan, H. B.; Van Overveldt, T.; Petrou, D.; Ramage, D.; Roselander, J. Towards Federated Learning at Scale: *System Design*. arXiv [cs.LG], **2019**.
17. Hitaj, B.; Ateniese, G.; Perez-Cruz, F. Deep Models under the GAN: Information Leakage from Collaborative Deep Learning. arXiv [cs.CR], **2017,** 28 (1), 78–82.
18. Buczak, A. L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Commun. Surv. Tutor***. 2016**, 18 (2), 1153–1176.
19. Karimipour, H.; Dehghantanha, A.; Parizi, R. M.; Choo, K.-K. R.; Leung, H. A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids. *IEEE Access* **2019**, 7, 80778–80788.
20. Cetinkaya, A.; Ishii, H.; Hayakawa, T. A Probabilistic Characterization of Random and Malicious Communication Failures in Multi-Hop Networked Control. *SIAM j. Control Optim*. **2018,** 56 (5), 3320–3350.
21. Cao, T.-D.; Truong-Huu, T.; Tran, H.; Tran, K. A Federated Learning Framework for Privacy-Preserving and Parallel Training. arXiv [cs.DC], **2020,**18 (1), 28–32.
22. Chen, Y.-C.; Li, Y.-J.; Tseng, A.; Lin, T. Deep Learning for Malicious Flow Detection. arXiv [cs.LG], 2018.
23. Chora, M.; Kozik, R. Machine Learning Techniques Applied to Detect Cyber Attacks on Web Applications. *Log. J. IGPL* **2015**, 23 (1), 45–56.
24. Chowdhury, M.; Rahman, A.; Islam, R. Malware Analysis and Detection Using Data Mining and Machine Learning Classification. In Advances in Intelligent Systems and Computing; *Springer International Publishing: Cham*,**2018**; pp 266–274.
25. Chu, F.; Yuan, S.; Peng, Z. Machine Learning Techniques. Encyclopedia of Structural Health Monitoring; John Wiley & Sons, Ltd: Chichester, UK, **2008,** 32 (1), 22–26.
26. Applications https://www.unb.ca/cic/research/applications.html (accessed Dec 4, 2021).
27. Abebe, D. Lightweight Cybersecurity Schemes Using Elliptic Curve Cryptography in Publish-Subscribe Fog Computing,"*Mobile Net. Appl* **2017**, 22 (112), 1–11.
28. Dai, J. : : Deformable Convolutional Networks; 2017; pp 764–773.
29. Dangi, C. S. Cyber Security Approach in Web Application Using SVM. *International Journal of Computer Ap-plications* **2012**, *0975* (2,), 8887
30. Deng, L. Deep Learning: Methods and Applications. Found. Trends® Signal Process**. 2014**, 7 (3–4), 197–387.
31. Kumar, Y. Study of Machine and Deep Learning Classifications in Cyber-Physical System.
32. Dixit, P.; Silakari, S. Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review. *Comput. Sci. Rev*. **2021**, 39 (100317), 100317.
33. Doku, R.; Rawat, D. B.; Liu, C. Towards Federated Learning Approach to Determine Data Relevance in Big Data. In 2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI); *IEEE*, **2019**.
34. Computer Vision – ECCV 2014: 13Th European Conference, Zurich, Switzerland, September 6-12, 2014, Proceedings, Part IV; Fleet, D., Pajdla, T., Schiele, B., Tuytelaars, T., Eds.; *Springer International Publishing: Cham*, **2014**.
35. Dong, Y.; Chen, X.; Shen, L.; Wang, D. EaSTFLy:Efficient and Secure Ternary Federated Learning. Computers & Security **2020**, 101824, 101824.
36. Enthoven, D.; Al-Ars, Z. An Overview of Federated Deep Learning Privacy Attacks and Defensive Strategies. In Federated Learning Systems; *Springer International Publishing: Cham*, **2021**; pp 173–196.
37. Feng, C. A User-Centric Machine Learning Framework for Cyber Security Operations Cen-Ter; **2017**; pp 173–175.

38. Ferdowsi, A.; Saad, W. Generative Adversarial Networks for Distributed Intrusion Detection in the Internet of Things. arXiv [cs.CR], **2019**.
39. Ferrag, M. A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study. *J. Inf. Secur. Appl.* **2020**, 50 (102419), 102419.
40. Rao, N. T.; Dept. of Computer Science and EngineeringVignan's Institute of Information Technology (A), Visakhapatnam 530049, AP, India. Applications of Machine Learning in Cyber Security. *Int. J. Adv. Res. Comput. Inf. Secur.* **2019**, 3 (1), 1–8.
41. Caspi, G. Introducing Deep Learning: Boosting Cybersecurity with An Artificial Brain.
42. Costa, G. A Methodological Approach for Assessing Amplified Reflection Distributed Denial of Service on the Internet of Things. 2016, 4 (1), 11–18.
43. Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Baker, T. Security Threats to Critical In-Frastructure: The Human Factor. *The Journal of Supercomputing* **2018**, 1007 11227–018–2337–2.
44. Gómez, Á. L. P.; Maimó, L. F.; Celdran, A. H.; Clemente, F. J. G.; Sarmiento, C. C.; Masa, C. J. D. C.; Nistal, R. M. On the Gen-Eration of Anomaly Detection Datasets in Industrial Control Systems. *IEEE Access* **2019**, 7, 177460–177473.
45. Geetha, R.; Thilagam, T. A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security. *Arch. Comput. Methods Eng*. **2021**, 28 (4), 2861–2879.
46. Ali, S.; Al Balushi, T.; Nadir, Z.; Hussain, O. K. WSN Security Mechanisms for CPS. In Studies in Computational Intelligence; *Springer International Publishing: Cham***, 2018**; pp 65–87.
47. Hannah, J.; Mills, R.; Dill, R.; Hodson, D. Traffic Collision Avoidance System: False Injection Viability. *J. Supercomput*. **2021**, 77 (11), 12666–12689.
48. Hao, M.; Li, H.; Luo, X.; Xu, G.; Yang, H.; Liu, S. Efficient and Privacy-Enhanced Federated Learning for In-Dustrial Artificial Intelligence. *IEEE Transactions on Industrial Informatics* **2019**, 1–1, 2945367.
49. Haris, M.; Shakhnarovich, G.; Ukita, N. Recurrent Back-Projection Network for Video Super-Resolution. In 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR); *IEEE*, **2019**.
50. Hassan, M. U.; Rehmani, M. H.; Chen, J. Differential Privacy Techniques for Cyber Physical Systems: A Survey. *IEEE Commun. Surv. Tutor*. **2020**, 22 (1), 746–789.
51. Ibrahim, A.; Valli, C.; McAteer, I.; Chaudhry, J. A Security Review of Local Government Using NIST CSF: A Case Study. *The Journal of Supercomputing* **2018**, 1007 11227–018–2479–2.
52. Goodfellow, I. J.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; DavidWarde-Farley, S. Aaron Courville, and YoshuaBengio. *Generative adversarial networks* **2014**.
53. Deep Learning Method for Denial of Service Attack Detection Based on Re-Stricted Boltzmann Machine. *Big data* **2018**, 6 (2), 159–169.
54. Kang, J. : : FlowNet: Learning Optical Flow with Convolutional Networks.
55. Paridari, K.; O'Mahony, N.; Mady, A. E. D.; Chabukswar, R.; Boubekeur, M.; Sandberg, H. A Framework for At-Tack-Resilient Industrial Control Systems: *Attack Detection and Controller Reconfiguration*; Vol. 106, pp 113–128.
56. Jaiyen, S.; Sornsuwit, P. A New Incremental Decision Tree Learning for Cyber Security Based on ILDA and Mahalanobis Distance. WarasanWitsawakamsat, Chulalongkorn Univ. **2019,** 23 (5), 71–88.
57. Kumar, S.; Jha, N.; Sachdeva, N. A Deep Learning Approach for Anomaly-Based Network Intrusion Detection Systems: A Survey and an Objective Comparison. In Machine Learning and Big Data Analytics (Proceedings of International Conference on Machine Learning and Big Data Analytics (ICMLBDA) 2021); *Springer International Publishing: Cham***, 2022**; pp 227–235.
58. Jiang, F.; Fu, Y.; Gupta, B. B.; Liang, Y.; Rho, S.; Lou, F.; Meng, F.; Tian, Z. Deep Learning Based Multi-Channel Intelligent Attack Detection for Data Security. *IEEE Trans. Sustain. Comput*. **2020**, 5 (2), 204–212.

59. Liu, K.; Dolan-Gavitt, B.; Garg, S. Fine-Pruning: Defending against Backdooring Attacks on Deep Neural Networks. arXiv [cs.CR], **2018**.
60. Mitchell, R.; Chen, I.-R. A Survey of Intrusion Detection Techniques for Cyber-Physical Systems. *ACM Comput. Surv*. **2014**, 46 (4), 1–29.
61. Karie, N. M.; Kebande, V. R.; Venter, H. S. Diverging Deep Learning Cognitive Computing Techniques into Cyber Forensics. *Forensic Science International: Synergy* **2019**, 1, 61–67.
62. Katzir, Z.; Elovici, Y. Quantifying the Resilience of Machine Learning Classifiers Used for Cyber Security. *Expert Syst*. Appl. **2018**, 92, 419–429.
63. Li, B.; Lu, R.; Wang, W.; Choo, K.-K. R. Distributed Host-Based Collaborative Detection for False Data Injection Attacks in Smart Grid Cyber-Physical System. *J. Parallel Distrib. Comput*. **2017**, 103, 32–41
64. Srivastava, A.; Morris, T.; Ernster, T.; Vellaithurai, C.; Pan, S.; Adhikari, U. Modeling Cyber-Physical Vulnerability of the Smart Grid with Incomplete Information. *IEEE Trans. Smart Grid* **2013**, 4 (1), 235–244.
65. Ashok, A.; Hahn, A.; Govindarasu, M. Cyber-Physical Security of Wide-Area Monitoring, Protection and Control in a Smart Grid Environment. *J. Adv. Res*. **2014**, 5 (4), 481–489.
66. Kumar, Y.; Sood, K.; Kaul, S.; Vasuja, R. Big Data Analytics and Its Benefits in Healthcare. In Studies in Big Data; *Springer International Publishing: Cham*, **2020**; pp 3–21
67. Recent Advancement of Machine Learning and Deep Learning in the Field of Healthcare System. In Computational Intelligence for Machine Learning and Healthcare Informatics; *De Gruyter*, **2020**; pp 77–98.
68. Y, K.; Kaur, K.; Singh, G.; Y, K.; Kaur, K.; Singh, G.; Y, K.; Kaur, K.; Singh, G.; Y, K.; Kaur, K.; Singh, G.; Y, K.; Kaur, K.; Singh, G. Machine Learning Aspects and Its Applications Towards Different Research Areas; **2020**; Vol. 9051502, pp 150–156
69. Phong, L. T.; Aono, Y.; Hayashi, T.; Wang, L.; Moriai, S. Privacy Preserving Deep Learning via Additively Homomorphic Encryption. *IEEE Transactions on Information Forensics and Security* **2018**, 13 (5).
70. Srivastava, A.; Morris, T.; Ernster, T.; Vellaithurai, C.; Pan, S.; Adhikari, U. Modeling Cyber-Physical Vulnerability of the Smart Grid with Incomplete Information. *IEEE Trans. Smart Grid* **2013**, 4 (1), 235–244.
71. Ashok, A.; Hahn, A.; Govindarasu, M. Cyber-Physical Security of Wide-Area Monitoring, Protection and Control in a Smart Grid Environment. *J. Adv. Res*. **2014**, 5 (4), 481–489.
72. Kumar, Y.; Sood, K.; Kaul, S.; Vasuja, R. Big Data Analytics and Its Benefits in Healthcare. In Studies in Big Data; *Springer International Publishing: Cham*, **2020**; pp 3–21.
73. Recent Advancement of Machine Learning and Deep Learning in the Field of Healthcare System. In Computational Intelligence for Machine Learning and Healthcare Informatics; *De Gruyter*, **2020**; pp 77–98
74. Kumar, Y.; Kaur, K.; Singh, G. Machine Learning Aspects and Its Applications towards Different Research Areas. In 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM); *IEEE*, 2020.
75. Phong, L. T.; Aono, Y.; Hayashi, T.; Wang, L.; Moriai, S. Privacy Preserving Deep Learning via Additively Homomorphic Encryption. *IEEETransactions on Information Forensics and Security* **2018**, 13 (5).
76. Automatic Malware Mutant Detection and Group Classification Based on the N-Gram and Clustering Coefficient. *The Journal of Supercomputing* **2015**, 74 (8), 3489–3503.
77. Li, Z.; Zhang, Q.; Du, X.; Ma, Y.; Wang, S. Social Media Rumor Refutation Effectiveness: Evaluation, Modelling and Enhancement. *Inf. Process. Manag*. **2021**, 58 (1), 102420.
78. Liang, G.; Weller, S. R.; Zhao, J.; Luo, F.; Dong, Z. Y. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Trans. Power Syst*. **2017**, 32 (4), 3317–3318.
79. Liang, G.; Zhao, J.; Luo, F.; Weller, S. R.; Dong, Z. Y. A Review of False Data Injection Attacks against Modern Power Systems. *IEEE Trans. Smart Grid* **2017**, 8 (4), 1630–1638.
80. Liang, P. P.; Liu, T.; Ziyin, L.; Allen, N. B.; Auerbach, R. P.; Brent, D.; Salakhutdinov, R.; Morency, L.-P. Think Locally, Act Globally: *Federated Learning with Local and Global Representations*. arXiv [cs.LG], **2020.**

81. Lima, A. Q.; Keegan, B. Challenges of Using Machine Learning Algorithms for Cybersecurity. In Cyber Influence and Cognitive Threats; *Elsevier*, **2020**; pp 33–52.
82. Liu, H.; Lang, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Appl. Sci. (Basel)* **2019**, 9 (20), 4396.
83. Li, L.; Li, C.; Ji, D. Deep Context Modeling for Multi-Turn Response Selection in Dialogue Systems. *Inf. Process*. Manag. **2021**, 58 (1), 102415.
84. Kim, D.; Won, Y.; Kim, S.; Eun, Y.; Park, K. J.; Johansson, K. H.; L., Y.; H.; Yang, Q. Sampling Rate Optimization for IEEE 802. 11 Wireless Control Systems; Montreal, QC, Canada, **2019**; pp 87–96 ,.
85. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A. A. A Detailed Analysis of the KDD CUP 99 Data Set. In 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications; *IEEE*, **2009**.
86. Malomo, O. O.; Rawat, D. B.; Garuba, M. Next-Generation Cybersecurity through a Blockchain-Enabled Federated Cloud Framework. *J. Supercomput*. **2018**, 74 (10), 5099–5126.
87. Moustafa, N.; Slay, J.; Creech, G. Novel Geometric Area Analysis Technique for Anomaly Detection Using Trapezoidal Area Estimation on Large-Scale Networks. *IEEE Trans. Big Data* **2019**, 5 (4), 481–494.
88. Muniyandi, A. P.; Rajeswari, R.; Rajaram, R. Network Anomaly Detection by Cascading K-Means Clustering and C4.5 Decision Tree Algorithm. *Procedia Eng*. **2012**, 30, 174–182.
89. Akhtar, N.; Mian, A. Threat of Adversarial Attacks on Deep Learning in Computer Vision: *A Survey*. arXiv [cs.CV], **2018**.
90. Nguyen, H.-T.; Ngo, Q.-D.; Le, V.-H. A Novel Graph-Based Approach for IoT Botnet Detection. Int. J. Inf. Secur. **2020**, 19 (5), 567–577.
91. NicolasPapernot, P. D. M.; Sinha, A.; Wellman, M. P. Towards the Science of Security and Privacy in Machine Learning. CoRR 03814,.
92. Sebastian, O.; Ackere Ann; R, L. E. Interdependencies in Security of Electricity Supply. *Energy* **2017**, 135 (598).
93. Pang, S.; Peng, Y.; Ban, T.; Inoue, D.; Sarrafzadeh, A. A Federated Network Online Network Traffics Analysis Engine for Cybersecurity. In 2015 International Joint Conference on Neural Networks (IJCNN); *IEEE*, **2015,** 4 (1), 1–8..
94. Paudel, R.; Muncy, T.; Eberle, W. Detecting DoS Attack in Smart Home IoT Devices Using a Graph-Based Approach. In 2019 IEEE International Conference on Big Data (Big Data); *IEEE*, **2019**.
95. Perera, A. T. D.; Kamalaruban, P. Applications of Reinforcement Learning in Energy Systems. *Renew. Sustain. Energy Rev.* **2021**, 137 (110618), 110618.
96. Rahimi, N.; Maynor, J.; Gupta, B. Adversarial Machine Learning: Difficulties in Applying Machine Learning to Existing Cybersecurity Systems; *EasyChair***, 2020**.
97. Reddy, S.; Shyam, G. K. A Machine Learning Based Attack Detection and Mitigation Using a Secure SaaS Framework. *J. King Saud Univ. - Comput. Inf. Sci*. **2020**. https://doi.org/10.1016/j.jksuci.2020.10.005.
98. Rieke, N.; Hancox, J.; Li, W.; Milletari, F.; Roth, H.; Albarqouni, S.; Bakas, S.; Galtier, M. N.; Landman, B.; Maier-Hein, K.; Ourselin, S.; Sheller, M.; Summers, R. M.; Trask, A.; Xu, D.; Baust, M.; Cardoso, M. J. *The Future of Digital Health with Federated Learning*. arXiv [cs.CY], **2020,** 3 (1), 1–8..
99. Rifkin, J. The Third Industrial Revolution: How Lateral Power Is Transforming Energy, the Economy, and the World; *St. Martin's Griffin: New York*, **2011**.
100. Riyaz, S.; Sankhe, K.; Ioannidis, S.; Chowdhury, K. Deep Learning Convolutional Neural Networks for Radio Identification. *IEEE Commun. Mag*. **201**8, 56 (9), 146–152.
101. Roopak, M.; Yun Tian, G.; Chambers, J. Deep Learning Models for Cyber Security in IoT Networks. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC); *IEEE*, **2019**.
102. Maeda, R.; Mimura, M. Automating Post-Exploitation with Deep Reinforcement Learning. *Comput. Secur*. **2021**, 100 (102108), 102108.

103. Radanliev, P.; De Roure, D.; Van Kleek, M.; Santos, O.; Ani, U. Artificial Intelligence in Cyber Physical Systems. *AI Soc*. **2020**, 36 (3), 1–14.
104. Sahu, S.; Mehtre, B. M. Network Intrusion Detection System Using J48 Decision Tree. In 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI); *IEEE*, **2015**.
105. Sánchez, P. M. S.; Celdrán, A. H.; Maimó, L. F.; Pérez, G. M. AuthCODE: A Privacy-Preserving and Multi-Device Continuous Authentication Architecture Based on Machine and Deep Learning. arXiv [cs.CR], **2020**.
106. Sarker, I. H.; Abushark, Y. B.; Alsolami, F.; Khan, A. I. IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. Symmetry (Basel) **2020**, 12 (5), 754.
107. Sathyanarayan, V. S.; Kohli, P.; Bruhadeshwar, B. Signature Generation and Detection of Malware Families. In Information Security and Privacy; *Springer Berlin Heidelberg: Berlin, Heidelberg*, **2008**; pp 336–349.
108. Sen, R.; Chattopadhyay, M.; Sen, N. An Efficient Approach to Develop an Intrusion Detection System Based on Multi Layer Backpropagation Neural Network Algorithm: IDS Using BPNN Algorithm. In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research; *ACM: New York, NY, USA*, **2015**.
109. Mori, P.; Furnell, S.; Camp, O. Information Systems Security and Privacy : 4th International Conference, ICISSP 2018, Funchal - Madeira, Portugal, January 22-24, **2018**, Revised Selected Papers; 2019.
110. Stein, G.; Chen, B.; Wu, A. S.; Hua, K. A. Decision Tree Classifier for Network Intrusion Detection with GA-Based Feature Selection. In Proceedings of the 43rd annual southeast regional conference on - ACM-SE 43; ACM Press: New York, New York, USA, **2005**.
111. Tang, T. A.; Mhamdi, L.; McLernon, D.; Zaidi, S. A. R.; Ghogho, M. Deep Learning Approach for Network Intrusion Detection in Software Defined Networking. In 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM); *IEEE*, **2016**.
112. Thing, V. L. L. IEEE 802. 11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach; San Francisco, **2017**; pp 1–6.
113. DReLAB-Deep REinforcement Learning Adversarial Botnet: A Benchmark Dataset for Adversarial Attacks against Botnet Intrusion Detection Systems. *Data in Brief* **2021**, 34, 106631.
114. Vinayakumar, R.; Soman, K. P.; Poornachandran, P.; Akarsh, S. Application of Deep Learning Architectures for Cyber Security. In Advanced Sciences and Technologies for Security Applications; *Springer International Publishing: Cham,***2019**; pp 125–160.
115. Walker-Roberts, S.; Hammoudeh, M.; Aldabbas, O.; Aydin, M.; Dehghantanha, A. Threats on the Horizon: Understanding Security Threats in the Era of Cyber-Physical Systems. *J. Supercomput*. **2020**, 76 (4), 2643–2664.
116. https://www.blackhat.com/docs/us-15/materials/us-15-Wang-The-Applications-Of-Deep-Learning- (accessed Dec 5, **2021**).
117. Wei, J.; Mendis, G. J. A Deep Learning-Based Cyber-Physical Strategy to Mitigate False Data Injection Attack in Smart Grids. In 2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG); *IEEE*, **2016**.
118. Wu, M.; Song, Z.; Moon, Y. B. Detecting Cyber-Physical Attacks in CyberManufacturing Systems with Machine Learning Methods. *J. Intell. Manuf.* **2019**, 30 (3), 1111–1123.
119. Li, Y.; Ma, R.; Jiao, R. A Hybrid Malicious Code DetectionMethod Based on Deep Learning. *Int'l. J. Security and Its Applications* **2015**, 9, 205–16.
120. Yan, Q.; Wang, M.; Huang, W.; Luo, X.; Yu, F. R. Automatically Synthesizing DoS Attack Traces Using Generative Adversarial Networks. *Int. j. Mach. Learn. Cybern*. **2019**, 10 (12), 3387–3396.
121. Yuan, Y.; Li, Z.; Ren, K. Modeling Load Redistribution Attacks in Power Systems. *IEEE Trans. Smart Grid* **2011**, 2 (2), 382–390.
122. Zhang, X.; Chen, J.; Zhou, Y.; Han, L.; Lin, J. A Multiple-Layer Representation Learning Model for Network-Based Attack Detection. *IEEE Access* **2019**, 7, 91992–92008.

123. Zhao, J.; Mili, L.; Wang, M. A Generalized False Data Injection Attacks against Power System Nonlinear State Estimator and Countermeasures. *IEEE Trans. Power Syst*. **2018**, 33 (5), 4868–4877.
124. Wasicek, A.; Derler, P.; Lee, E. A. Aspect-Oriented Modeling of Attacks in Automotive Cy-Ber-Physical Systems; *IEEE*, **2014**; pp 1–6.
125. Koubaa, B. A. A Vision of Cyber-Physical Internet, 8th International Workshop on Real-Time Networks. Dublin, Ireland 2009.
126. Cardenas, S. A.; Sinopoli, B.; Giani, A.; Perrig, A.; Sastry, S. Challenges for Securing Cyber Physical Systems; Newark, NJ, 2009.
127. Saltzer, J. H.; Schroeder, M. D. The Protection of Information in Computer Systems, Proc. *IEEE* **2010**, 63 (9), 1278–1308.
128. Avizienis, A.; Laprie, J.-C.; Randell, B.; Landwehr, C. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Trans. Dependable Secure Comput.* **2004**, 1 (1), 11–33.
129. Wang, E. K.; Ye, Y.; Xu, X.; Yiu, S. M.; Hui, L. C. K.; Chow, K. P. Security Issues and Challenges for Cyber Physical System. In 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing; *IEEE*, **2022.**
130. Sicari, A. R.; Grieco, L. A.; Coen-Porisini, A. Security, Privacy and Trust in Internet of Things: *The Road Ahead*, *Comput. Networks* **2015**, 76, 146–164.
131. Xu, D.; Tu, M.; Sanford, M.; Thomas, L.; Woodraska, D.; Xu, W. Automated Security Test Generation with Formal Threat Models. *IEEE Trans. Dependable Secure Comput*. **2012**, 9 (4), 526–540.
132. Xinlan, Z.; Zhifang, H.; Guangfu, W.; Xin, Z. Information Security Risk Assessment Methodology Research: Group Decision Making and Analytic Hierarachy Process; Second WRI World Congress on Software Eng.
133. Neuman, C.; Tan, K. Mediating Cyber and Physical Threat Propagation in Secure Smart Grid Architectures. In 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm); *IEEE*, **2011**.
134. https://www.defcon.org/ (accessed Dec 5, 2021).
135. Krotofil, M.; Larsen, J.; Gollmann, D. The Process Matters: Ensuring Data Veracity in Cyber-Physical Systems; **2022**.
136. Djouadi, S. M.; Melin, A. M.; Ferragut, E. M.; Laska, J. A.; Dong, J.; Drira, A. Finite Energy and Bounded Actuator Attacks on Cyber-Physical Systems. In 2015 European Control Conference (ECC); *IEEE*, **2015**.
137. Singhal, A. Data Warehousing and Data Mining Techniques for Cyber Security; Springer Science + Business: Media, USA, **2007**.
138. Mitchell, R.; Chen, I.-R. Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems. *IEEE Trans. Reliab*. **2013**, 62 (1), 199–210.
139. Collins, S.; McCombie, S. Stuxnet: The Emergence of a New Cyber Weapon and Its Implications. *J. Polic. Intell. Count. Terror*. **2012**, 7 (1), 80–91.
140. Khan, A. W.; Khan, M. U.; Khan, J. A.; Ahmad, A.; Khan, K.; Zamir, M.; Kim, W.; Ijaz, M. F. Analyzing and Evaluating Critical Challenges and Practices for Software Vendor Organizations to Secure Big Data on Cloud Computing: An AHP-Based Systematic Approach. *IEEE Access* **2021**, *9*, 107309–107332.
141. Ijaz, M. F.; Attique, M.; Son, Y. Data-Driven Cervical Cancer Prediction Model with Outlier Detection and over-Sampling Methods. *Sensors (Basel)* **2022**, *20* (10), 2809.
142. Panigrahi, R.; Borah, S.; Bhoi, A. K.; Ijaz, M. F.; Pramanik, M.; Jhaveri, R. H.; Chowdhary, C. L. Performance Assessment of Supervised Classifiers for Designing Intrusion Detection Systems: A Comprehensive Review and Recommendations for Future Research. *Mathematics* **2021**, *9* (6), 690.
143. Panigrahi, R.; Borah, S.; Bhoi, A. K.; Ijaz, M. F.; Pramanik, M.; Kumar, Y.; Jhaveri, R. H. A Consolidated Decision Tree-Based Intrusion Detection System for Binary and Multiclass Imbalanced Datasets. *Mathematics* **2021**, *9* (7), 751.

144. Srinivasu, P. N.; SivaSai, J. G.; Ijaz, M. F.; Bhoi, A. K.; Kim, W.; Kang, J. J. Classification of Skin Disease Using Deep Learning Neural Networks with MobileNet V2 and LSTM. *Sensors (Basel)* **2021**, *21* (8), 2852.
145. Gupta, D.; Rani, S.; Ahmed, S. H.; Verma, S.; Ijaz, M. F.; Shafi, J. Edge Caching Based on Collaborative Filtering for Heterogeneous ICN-IoT Applications. *Sensors (Basel)* **2022**, *21* (16), 5491.
146. Rani, S.; Koundal, D.; Kavita, I.; F., M.; Elhoseny, M.; Alghamdi, M. I. An Optimized Framework for WSN Routing in the Context of Industry 4. 0. *Sensors* **2021**, *21*, 6474.
147. Dash, S.; Verma, S.; Kavita; Khan, M. S.; Wozniak, M.; Shafi, J.; Ijaz, M. F. A Hybrid Method to Enhance Thick and Thin Vessels for Blood Vessel Segmentation. *Diagnostics (Basel)* **2021**, *11* (11), 2017. https://doi.org/10.3390/diagnostics11112017.