Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2025 SCPE. Volume 26, Issues 1, pp. 16–33, DOI 10.12694/scpe.v26i1.3438

REVIEW ON THE USE OF FEDERATED LEARNING MODELS FOR THE SECURITY OF CYBER-PHYSICAL SYSTEMS

MUHAMMED RAFEEQ WAR,[*] YASHWANT SINGH,[†] ZAKIR AHMAD SHEIKH,[‡] AND PRADEEP KUMAR SINGH[§]

Abstract. The field of critical infrastructure has undergone significant expansion over the past three decades, spurred by global economic liberalization and the pursuit of development, industrialization, and privatization by nations worldwide. This rapid growth has led to a proliferation of critical infrastructure across various sectors, necessitating decentralization efforts to manage the associated burdens effectively. With the advent of artificial intelligence and machine learning, computer scientists have sought innovative approaches to detect and respond to the evolving landscape of cyber threats. Despite efforts to subscribe to these changes, attackers continually devise new methods to evade detection, requiring constant vigilance and adaptation from cybersecurity professionals. Traditional centralized models of machine and deep learning demand substantial data and computational resources, making them susceptible to single-point failures. To address these challenges, scientists have introduced federated learning—a decentralized technique that minimizes computational costs while prioritizing data privacy and preservation. This review article delves into recent research and review papers concerning critical infrastructure security and federated learning, exploring various architectures, threats, vulnerabilities, and attack vectors. Through our analysis, we provide a comprehensive overview of federated learning, cyber-physical systems security, and the advantages of integrating federated learning into critical infrastructure environments. By synthesizing insights from diverse sources, our study contributes to a deeper understanding of federated learning's applications and implications in safeguarding critical infrastructures. We highlight the potential of federated learning to enhance cybersecurity measures while addressing the unique challenges posed by modern-day threats. As organizations and nations navigate the complexities of securing their critical assets, the adoption of federated learning emerges as a promising strategy to bolster resilience and protect against emerging cyber risks.

Key words: Constraint CPS, CPS Security, Cyber Security, Distributed Learning, Federated Learning, Intelligent Security

1. Introduction.

Our primary goal in this research is to enhance the security of Cyber-Physical Systems (CPS) by leveraging federated learning techniques. CPS are increasingly integrated into critical infrastructures, such as power grids, transportation systems, and healthcare facilities, thereby amplifying the urgency of securing these systems against cyber threats [1]. Traditional machine learning approaches encounter several challenges when applied to CPS security. One major obstacle is the need to centralize data for model training, which poses significant privacy and security risks, especially when dealing with sensitive information from distributed sources. Additionally, traditional methods often struggle with scalability and efficiency when handling large volumes of heterogeneous data distributed across diverse CPS devices and environments. Federated learning presents a promising solution to these challenges by enabling collaborative model training across decentralized edge devices while preserving data privacy. By distributing the learning process among multiple edge devices without centralizing data, FL mitigates privacy concerns and reduces the risk of data breaches. Moreover, FL leverages local model updates and aggregation techniques to accommodate the heterogeneity of data sources and optimize model performance across diverse CPS environments [2]. Through our research, we aim to demonstrate how federated learning can effectively address the security challenges inherent in CPS environments while maintaining data privacy and scalability. By leveraging FL techniques, we strive to enhance the robustness and resilience of CPS against various cyber threats, thereby contributing to the advancement of secure and trustworthy CPS deployments.

[*] Central University of Jammu, India (warrafeeq0@gmail.com)

[†] Department of Computer Science and Information Technology, Central University of Jammu, India (yashwant.csit@cujammu.ac.in)

[‡] Department of Computer Science and Information Technology, Central university of Jammu, India (zakir.csit@cujammu.ac.in)

[§] Department of Computer Science and Engineering, Central University of Jammu, India (pradeep.cse@cujammu.ac.in)

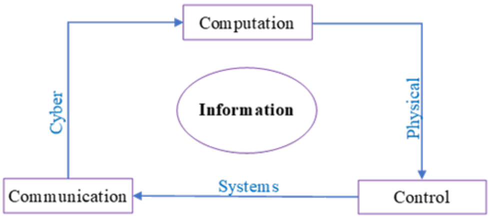

Fig. 1.1: Workflow of cyber-physical systems

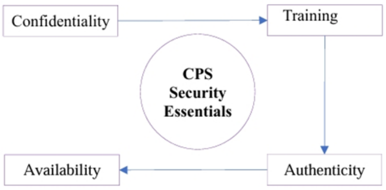

Fig. 1.2: Workflow of CPS

The term cyber-physical system (CPS) refers to a system that integrates computer and physical components to interact with the real environment [3]. Communication components allow information to be exchanged between physical and computational components, such as wireless networks, wired connections, and protocols. Control components are in charge of controlling the interactions between physical and computational components, such as feedback loops, decision-making algorithms, and control systems. Computation, exchange information communication and control components interact in the CPS environment as depicted in Figure 1.1. Due to their extensive network dependence and interconnectedness, cyber-physical systems (CPS) are more susceptible to online assaults [1]–[4],[7]. and security against the same can be ensured through the utilization of preventive strategies, detection mechanisms, and mitigation/isolation mechanisms. CPS has objects that integrate computing, storage, and communication capabilities to manage and communicate with a physical process. They are linked to the virtual world and one another via global digital networks. Any security compromise will have serious consequences [6-9]. Any unauthorised Process has the potential to severely destroy the entire system as well as private data. These are the primary prerequisites for CPS security [8].

Availability is the capacity to sustain operational goals in CPS and may be defined as the ability to prevent or survive denial-of-service (DoS) assaults on the information gathered by sensor networks, the instructions delivered by controllers, and the physical actions conducted by actuators. Similarly, CPS integrity seeks to sustain operational goals by avoiding, detecting, or surviving deception attempts in data provided and received by sensors, controllers, and actuators. The goal of confidentiality in cyber-physical systems is to prevent an adversary from inferring the state of the physical system by listening in on communication channels between sensors and controllers, and between controllers and actuators, or by using side-channel attacks on sensors, controllers, and actuators [10]. The study has discussed many aspects of CIA in the table 1.1. These aspects include the attacks, category of attacks [3], [4], [6], [11], [12], [13], [14].

Table 1.1 lists several security features, their explanations, associated security measures, and attack types and names for CPS (Cyber-Physical Systems). Confidentiality, integrity, authenticity, and availability are security considerations. The terms confidentiality, integrity, authenticity, and availability describe how to ensure that systems and services are available and work as expected. Confidentiality is the prevention of unauthorised access to sensitive information, while integrity refers to safeguarding data from unauthorised modifications. Encryption, digital signatures, access control, and redundancy are the associated security measures for each security feature. With particular attack designations like denial of service (DoS), man-in-the-middle (MITM), and social engineering assaults, the attack categories for CPS include physical attacks, cyberattacks, and human-related attacks [3], [16-18]. There are various sorts of attacks that may be launched against CPS, including

Table 1.1: Security aspects for CPS

Security Aspect	Reference	Description	Security Mechanism	Attack Category	Attack Names
Confidentiality	[3], [15-18]	Protecting sensitive data from unauthorized access and disclosure.	Encryption, access control, data obfuscation	Disclosure	Eavesdropping, data interception, data theft, Data sniffing, data capturing, side channel attack
Integrity	[3], [15-18]	Ensuring data is not tampered with or modified without authorization.	Hashing, digital signatures, version control	Deception	Data manipulation, injection attacks, man-in-the-middle attacks
Authenticity	[3], [15-18]	Ensuring data is genuine and has not been tampered with or forged.	Digital certificates, biometrics, two-factor authentication	Disruption	Spoofing, identity theft, replay attacks
Availability	[3], [15-18]	Ensuring the availability of systems and data, and preventing denial-of-service attacks.	Redundancy, backup and recovery systems, load balancing	Authentication Bypassing	DoS, DDoS attacks, network congestion, system overload

Denial of Service (DoS) attacks that try to disable the system by flooding it with requests or messages. Man-in-the-Middle (MitM) attacks intercept and modify communications between two parties. Injection attacks take the use of system weaknesses to insert malicious code or data. Spoofing attacks entail imitating a genuine user or device to obtain unauthorised access to a system [19-21].

Physical assaults entail physically messing with the system or its components to impair its operation. Preventing attacks in the first place is the goal of prevention mechanisms. Among these mechanisms, access control is the process of restricting system access to authorised individuals or devices through authentication and permission. Encryption is the use of encryption to protect data in transit or at rest. Security protocols, using secure communication protocols such as SSL/TLS to safeguard data while it is in transit [5], [9]. Using firewalls to filter traffic and prevent unwanted system access. Patching and updating software regularly to address known vulnerabilities and flaws. Aiming to identify assaults as soon as they take place, detection measures are used. Among these mechanisms are Intrusion detection systems (IDS), these systems monitor network traffic to detect suspicious activities and notify system administrators. Security information and event management (SIEM) is the process of collecting and analysing log data from multiple system components to detect aberrant behaviour. Auditing and monitoring include evaluating system logs and activity regularly to uncover unusual patterns or behaviours. Mitigation/Isolation Mechanisms, Mitigation/isolation techniques are designed to reduce the impact of an attack once it has been discovered. Among these mechanisms are, Containment is Isolating affected system components to prevent the spread of the assault Recovery is putting disaster recovery procedures in place to get the system back up and running after an attack backup systems and redundancy are used to guarantee that key activities can continue in the event of an attack [3-5].

Challenges and Threats in CPS. CPS systems need the seamless interplay of several hardware and software elements, each with specialised capabilities. The potential for conflicts and inconsistencies that might arise during the interaction must be thoroughly understood to achieve this cohesiveness. This necessitates a proactive and innovative approach to problem-solving that aims to capitalise on each component's strengths while reducing any potential risks. There are many challenges and applications of CPS and a few of them are discussed in Figure 1.3. Security flaws in CPS are flaws or vulnerabilities that an attacker may use to undermine the system's confidentiality, integrity, and availability. These problems can be caused by human factors, programming errors, configuration issues, or design defects.

Unauthorized access, data breaches, malware infections, denial-of-service attacks, and physical tampering are a few examples of security flaws in CPS. Design flaws in CPS relate to the discrepancy between the system's actual performance or behaviour and its planned functionality. These flaws may result from poor modelling

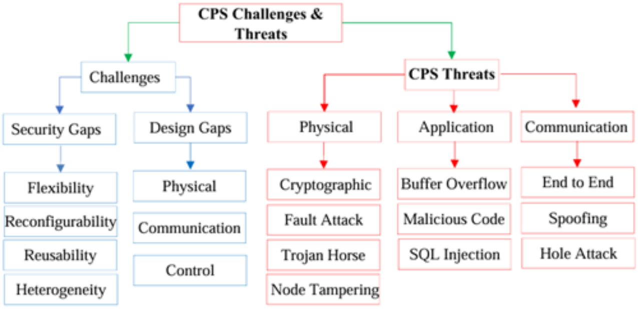

Fig. 1.3: CPS Challenges

or simulation, inadequate testing, or inconsistent or incomplete requirements. Unexpected or undesirable outcomes, such as system problems, failures, or inefficiencies, can result from design flaws. Smart manufacturing, autonomous vehicles, smart grids, medical gadgets, and robotic systems are just a few of the many applications for CPS. In many businesses, CPS may increase effectiveness, productivity, and quality, but it can also present new risks and obstacles. For instance, CPS in the healthcare industry must guarantee patient safety and privacy while giving medical personnel accurate and timely information[. When it comes to transportation, CPS must guarantee the protection and safety of both people and cargo while enhancing traffic flow and cutting pollution. Perception hazards are connected to the sensors and perception systems of the CPS. Sensor failures, erroneous readings, and data misinterpretation are examples of such dangers. Perception hazards can lead the system to make wrong judgements or perform improper actions, posing a danger to the system's safety or security. Communication hazards are dangers to the communication networks that connect the CPS components. Network outages, data manipulation, and eavesdropping are examples of such hazards. Communication hazards may lead to data loss or corruption or illegal system access, which may jeopardise the system's safety and security. Application risks: These are dangers to the software applications that operate on CPS. These dangers might include software defects, malware, or unauthorised application access. Application risks can cause system failures, data breaches, or unauthorised system access. While planning and implementing CPS, it is critical to handle these sorts of hazards. This is possible by employing security mechanisms like authentication, encryption, and intrusion detection.

2. CPS Architectures. CPS architecture are vital and critical in nature and are used at very critical places or places of high secrecy or privacy, hence keeping these architectures or installations is priority of all the undertaking authorities. SCADA, ICS,DCS are some cases The study has taken into account in this paper for security purposes.

2.1. SCADA (supervisory control and data acquisition). It is a network control system made up of sensors, actuators, and other hardware stored in several network levels and segments. SCADA is a software package deployed on top of the hardware with which it must interface via PLCs or other commercial hardware modules. SCADAs are used to collect data, monitor, and control vital infrastructure such as power grids, dams, and industries[22], [23], [24]. The study has come up with a very simple working of SCADA in Figure 2.1. SCADA systems are run in isolation to protect them from internet risks and assaults. Now, as the need for linking SCADA systems to the internet grows, we are in an unprecedented scenario where we must only research and discover methods of safeguarding SCADA systems. A significant amount of money and brainpower is being put into the field of SCADA security and privacy while keeping it online. The exchange of data between the field devices and the central controller is carried out by certain protocols that are designed for industrial applications. according to the authors of SCADA (Supervisory Control and Data Acquisition) systems are now networked. Since these networks are so intertwined, controlling these systems remotely is tough. As a result, robust security techniques are critical since a vulnerability in the SCADA system has the potential to cause financial and/or safety consequences.

According to the authors of where they have proven using the experiments, upon embedding an OPC server

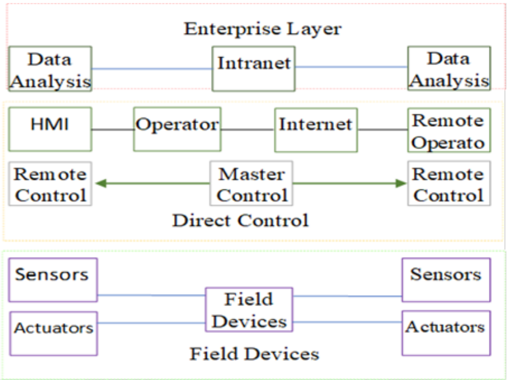

Fig. 2.1: SCADA Architecture

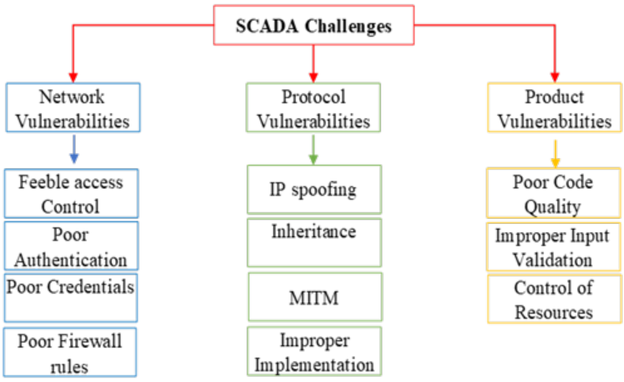

Fig. 2.2: SCADA Challenges

based application that is embedded into the SCADA. Which monitors a quasi-general process of industries, that is defined by the 2nd Order transfer function. It is used to identify transfer functions and manage the client-server transmission or communication based on quantities of interest by viewing online and using TDMS to create records plus a MySQL server. The Authors of have summarized the SCADA systems as well as the OPC Client-server communication. Furthermore, they suggest the following functionalities of a main software module. According to the authors of a function for main software is written in the OPC-UA, MySQL, Web servers, and Web servers. It also shows the evolution of the acquired values, transports are achieved automatically, the solution is stored in a database, and email addresses are sent to automatically manage alarms.to achieve integration in SCADA and to allow the data to be displayed wherever it is required internet or intranet using a web server that is embedded in the application. The Authors of have also discussed the problem that can arise in SCADA practical monitoring and industrial applications, which is data communication, can develop at any moment and become a pain for the operators; this problem can only be handled and investigated by reducing the provision of software modules for data transmission and actual data management. The Authors of contrasted the needs of an IT system and a SCADA system. Any vulnerability can have serious consequences in terms of data loss, money loss, energy loss, and even life-threatening situations for those who operate at the hazardous level of critical infrastructure. The study has shown some major challenges faced by SCADA in Figure 2.2. based on three major categories that are, network vulnerabilities, protocol vulnerabilities, and product vulnerabilities.

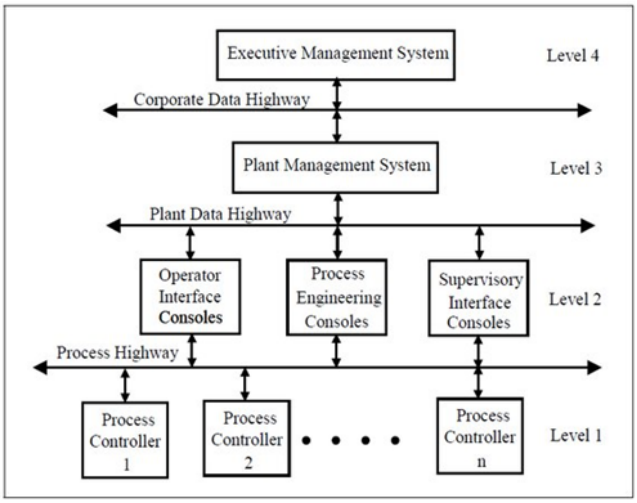

Fig. 2.3: Distribute Control System Architecture

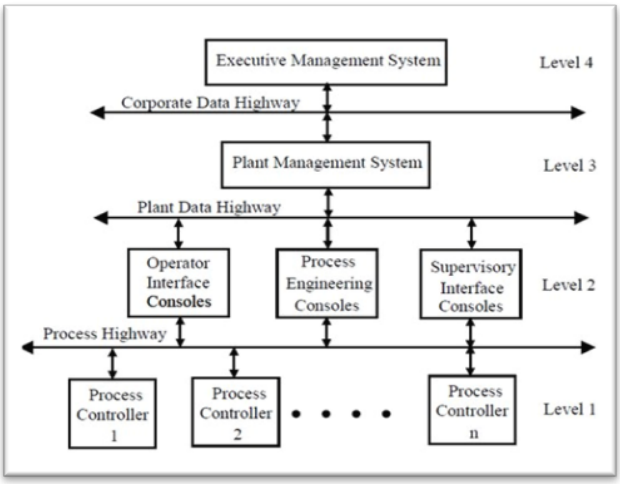

Fig. 2.4: DCS Architecture

2.2. Distributed Control System (DCS). Distributed Control System (DCS) is a custom-built control system and automatic, consisting of scattered control units located across various geographic locations and the facility or zone where it is controlled from. Unlike centralised control systems, in which a single controller at a single location controls the control function, each process element, machine, or collection of machines in a DCS is controlled by a distinct controller [25], [26]. Sensors and actuators in the field are linked to dispersed individual automated-controllers. Communication between controllers is accomplished using different field buses or industry-standard communication protocols. These controllers may communicate with supervisory terminals, operator terminals, historians, and other controllers, as well as with each other. DCS's architecture is distinguished by three major features. Modbus, HART, Profibus, and arc net are a few examples [12], [16].

The separation of many control functions into small groups of semiautonomous subsystems linked by a high-speed communication bus. The second feature of DCS is the use of cutting-edge control techniques in the industrial process. DCS organises the whole control structure as a single automation system, with distinct

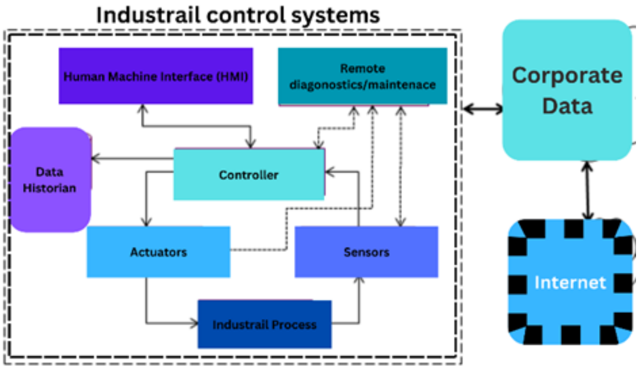
Industrail control systems
Human Machine Interface (HMI)
Remote diagonostics/maintenace
Data Historian
Controller
Actuators
Sensors
Industrail Process
Corporate Data
Internet

Fig. 2.5: Industrial Control Systems Architecture

subsystems linked together by a suitable command structure and information flow. The third characteristic is the object's systematic organisation. The study has shown this in Figure 2.3. The data collection, data presentation, process management, and monitoring. It might be a PC or another device equipped with engineering software. Its control, process and communication systems. The comprehensive configuration capabilities of the engineering station allow the user to undertake engineering activities such as adding additional loops and modifying sequential and continuous control logic.

A distributed control system (DCS) employs several components to monitor and manage physical processes. Input/output (I/O) modules, controllers, human-machine interfaces (HMI), communication networks, software, redundancy systems, and field devices are the essential elements of a DCS. I/O modules link the DCS to out-of-thebox equipment like sensors and actuators that monitor and regulate physical processes. I/O module data is processed by controllers, who also make choices and issue orders to field devices. An interface for system monitoring and control is provided by the HMI for operators. All of the DCS components are connected via communication networks, which enable real-time data transmission using different protocols. The system's functioning is controlled by DCS software, which also includes algorithms for monitoring and control that may be tailored for certain operations. systems for redundancy, like backup controllers and power supplies, ensure system availability and reduce downtime. Field devices, such as sensors and actuators, measure and control physical processes and communicate with the DCS through I/O modules. Do not adjust line and character spacing to fit your paper to a specific length.

2.3. Industrial Control System (ICS). The collection of all types of control systems in cyber-physical systems comprising SCADA, Distributed Control Systems (DCS) and Programmable logic Controllers (PLC) is known as Industrial systems [1], [2], [26], [27], [28]. ICS has become an essential part of critical infrastructures and industries. It generally consists of electrical, mechanical, hydraulic, and pneumatic brought together to perform an action and achieve a common goal which can be manufactured in the manufacturing industry and transportation in transportation and logistics, matter or energy in the energy industry. Control can be automated or may be manual in the loop and the part of the system used to control must have specifications of the desired results. The systems operate in three modes of loops; open loop, closed loop and manual loop, when the system is in the open loop it is controlled by established settings, when the system is in the closed loop the output impacts inputs to maintain the desired output, while as when the system is in manual mode, the control lies with the humans. The controller is part of the system which has concerned with maintaining conformance with the specifications of the system.

The authors of [16] have presented the widely used industrial communication protocols with a focus on the inherent security features and have offered security expansions of each protocol. The authors of [16] also provide a comprehensive overview of the current ICS state of the art, where they have analysed various testbeds, datasets, and IDS based on the availability of ICS literature available, the authors of also offer a The Authors have described the IDS generated for the offered datasets based on performance after conducting a thorough

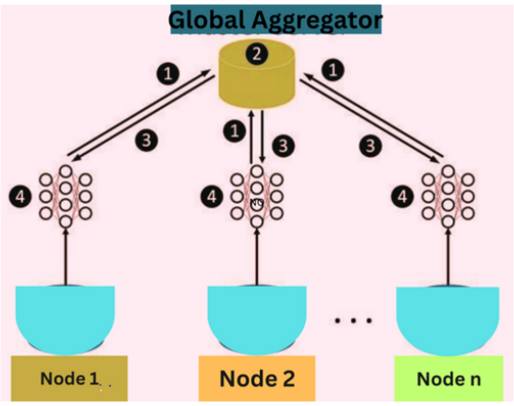

Fig. 3.1: Federated Learning Architecture

investigation of the various testbeds and datasets utilised for security research in ICS. As soon as the writers of were working on this program they found out that there is a need to well define testing detection frameworks. The authors of [16] made sure that they provide us with the best practices for designing a very efficient test bed in ICS. Dataset for ICS, IDS for ICS. The study has also shown the working diagram of industrial control systems in Figure 2.5. Where The study has shown all the components, their place, and their connectivity with the network.

3. FL Architectures for CPS. Federated learning is one of the most recent, advanced, critical advancements in the field of AI (Machine Learning, Deep Learning). Federated learning can be defined as the approach where all the traditional methods of machine training algorithms or techniques where a huge amount of data was required to train the machine, this process of collecting samples was problematic since many countries or organisations are hesitant of sharing the private information of citizens, customers [29], [30], [31]. Hence traditional machine learning techniques needed some relief which they got in the form of Federated Learning. Federated learning doesn't require a huge amount of data to train its models, and unlike ml models where data is shared with the server of the model and then the model is trained, in federated learning, we train data models at the local nodes and then the results or features (Parameters) are shared with the actual or global model which is then trained (aggregation takes place) based on these features. Federated learning provides far better security than traditional machine learning techniques since no exchange of actual data takes place, now if we need data from countries where data sharing is prohibited, we can train the model locally and then, share the results outside for training the global model. The regulations by many countries and organisations the reluctance to share the data of citizens for any purpose the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR) of the European Union, and the California Consumer Privacy Act (CCPA)). These were some of the first states and organisations that brought stringent laws for data protection which ultimately led us to the discovery of federated learning. Hence federated learning solved the problem of movement of data between jurisdictions by just allowing the training of data models at the local nodes and then sharing the results with the actual model for further computations with improved security on the privacy of data and efficient models where we need less time and less storage hence less costly. Now with the help of federated learning researchers and companies can build federated learning models for mutual benefits without sharing the data [32].

Vertical Federated Learning (VFL). Vertical Federated Learning (VFL) partitions training data horizontally across multiple parties and vertically partitions features for each party. This allows participants to retain ownership of their data while contributing to a broader model. Challenges include communication overhead, non-IID data, and privacy concerns. In VFL, collaborators within the same jurisdiction share encrypted data to ensure privacy. The global model is updated through a trusted third party. Solutions for VFL challenges include differential privacy, compression for communication efficiency, and resource allocation design. VFL is used for various applications like fraud detection, personalized advertising, and health modeling. Mitigation approaches against attacks include differential privacy and outlier detection [33].

Horizontal Federated Learning (HFL). Horizontal Federated Learning involves training machine learning models across multiple devices with similar feature spaces but distinct samples. It allows for collaboration among data owners without sharing raw data, enhancing model accuracy and privacy. Google proposed an HFL solution for updating Android phone models, where local updates are aggregated centrally. Secure aggregation schemes protect aggregated user updates, and additive homomorphic encryption ensures server security [34]. Challenges include communication costs, data heterogeneity, and potential attacks like Byzantine assaults.

Federated Transfer Learning (FTL). Federated Transfer Learning operates across diverse clients, transferring features from various feature spaces to train models. It encrypts gradient updates for security and privacy [35]. FTL is used in medical diagnosis and offers improved accuracy and reduced loss. It involves components like Guest, Host, and Arbiter for encryption, computation, and gradient collection. Challenges include data format variability, privacy concerns, communication overhead, and uneven data distribution. Mitigation strategies include differential privacy, secure aggregation, robust algorithms, and detection methods.

Centralized Federated Learning (CFL). Centralized Federated Learning involves a central server coordinating model training among multiple devices without sharing raw data. Local updates are aggregated centrally, and the global model is sent back to devices for updating [32], [36], [37]. CFL addresses data privacy concerns and communication overhead. Applications include healthcare, IoT, banking, and fraud detection. Challenges include single-point failure, data volume, and potential attacks like model poisoning. Mitigation strategies include federated averaging, differential privacy, secure aggregation, and outlier detection.

Decentralized Federated Learning (DFL). Decentralized Federated Learning operates without a central server, with nodes sharing updates among themselves. It's used in blockchain and cryptocurrency applications [34], [38]. Challenges include addressing heterogeneity and ensuring security. Applications include various industries like healthcare, finance, and smart cities. Mitigation strategies involve differential privacy, secure aggregation, and federated learning with adversarial defense (FLAD).

Multi-class Vertical Federated Learning (MMVFL). MMVFL enhances traditional vertical federated learning by allowing multiple clients to share label information while dealing with varied sample and feature spaces[39]. It aims to overcome challenges associated with horizontal FL and provides customized learning processes. Applications include computer vision datasets and industries requiring multi-class classification.

Table 3.1 summarizes various FL architectures used in different applications. Vertical FL (VFL) handles different feature spaces with similar sample spaces, facing security risks and high costs, while Horizontal FL (HFL) deals with varying sample spaces within the same feature space, encountering data distribution inconsistency. Federated Transfer Learning (FTL) efficiently manages diverse sample and feature spaces, applied in image classification and speech recognition. FL offers solutions to CPS challenges, with centralized FL facing single-point failure issues and decentralized FL offering a distributed approach for blockchain and cryptocurrency applications.

FEDF Architecture. The FEDF architecture enables parallel training with privacy preservation, allowing model training in geographically distributed locations [40]. It includes a master server and multiple nodes, facilitating remote training processes. Applications include various sectors needing distributed training data.

PerFit. [30], [35] is a cloud-based FL framework designed for IoT, addressing device and statistical heterogeneity, model variation, and privacy concerns. It offloads computing tasks from IoT devices, ensuring efficiency and low latency. Applications include healthcare and smart environments.

Framework of FADL. FADL is an architecture focused on the medical industry, utilizing a federated-autonomous deep learning approach [41]. It trains model elements using all data sources while ensuring security and privacy. Applications include ICU hospital data analysis.

FL-based Framework with Blockchain Integration. This architecture integrates FL with blockchain technology to address security and privacy concerns, especially in the industrial IoT sector. It uses a blockchain module for safe data links and supports transactions for data retrieval and sharing [42], [43], [44]. Applications include industrial IoT and sectors requiring secure data exchange.

4. FL for CPS. Security and computational efficiency are the most important aspects of CPS and FL has been a real booster to both of these aspects while resolving the privacy issues it also takes care of computational

Table 3.1: A summary of federated learning applications, mechanisms, and challenges

Architecture	Mechanism	Challenges	Applications
Vertical FL	Data partitioned vertically among devices	Limited data availability, data heterogeneity, communication overhead	Banking, insurance, e-commerce, privacy
Horizontal FL	Data partitioned horizontally among devices	Limited data availability, privacy concerns, communication overhead, imbalanced data distribution	Health, IoT, Security
Federated Transfer Learning	Transfer knowledge between device sets in FL setting	Model and data heterogeneity, communication overhead, privacy concerns	Image and text classification, speech recognition, loss prevention
Centralized FL	Central server coordinates training among devices	Privacy concerns, security risks, scalability, communication overhead, data heterogeneity	Text prediction enhancement (Gboard)
Decentralized FL	Devices communicate directly for model training without central coordinator	Privacy concerns, security risks, scalability, communication overhead, data heterogeneity	Blockchain, cryptocurrency
MMVFL	Multiclass model training with many parties collaboration	Privacy concerns, security risks, scalability, communication overhead, data heterogeneity	Multi-class classification
FEDF	Federated Ensemble Deep Learning Framework	Privacy concerns, security risks, scalability, communication overhead, data heterogeneity	Privacy preservation, parallel training
PerFit	Personalized FL Framework	Privacy concerns, security risks, scalability, communication overhead, data heterogeneity	IoT implementation
FedHealth	FL framework for healthcare applications ensuring patient data privacy	Privacy concerns, security risks, scalability, communication overhead, data heterogeneity	Healthcare

efficiency simultaneously. Lets take a look at some use cases of FL in CPS already in place [45].

4.1. Federated Learning-Based Explainable Anomaly Detection for Industrial Control Systems. A new method for identifying anomalies in industrial control systems (ICS) that makes use of federated learning and explainability is presented in the research article ”Federated Learning-Based Explainable Anomaly Detection for Industrial Control Systems”. While standard anomaly detection approaches can be successful, the authors contend that they frequently lack transparency and interpretability, which limits their usefulness in crucial applications such as ICS. The suggested method makes use of a federated learning architecture to allow the training of anomaly detection models across various ICS devices while protecting data privacy. Local models are trained on specific devices, and their parameters are pooled to build a global model capable of detecting abnormalities throughout the ICS[2], [46], [47]. The authors also present a unique technique for explaining identified anomalies based on individual features and device contributions to the global model. This helps ICS operators to have a better understanding of the nature of reported abnormalities and take necessary mitigation measures. The authors do tests on a real-world dataset of ICS network traffic to assess the effectiveness of the suggested technique. The findings show that the federated learning-based strategy detects abnormalities well and beats standard centralised approaches in terms of accuracy and communication efficiency. The explainability component also improves the system’s interpretability and usefulness. The suggested method makes an important addition to the field of ICS anomaly identification. The use of federated learning provides a distributed and effective technique for training anomaly detection models while maintaining data privacy, and the explainability component improves the system’s interpretability and utility. This method can improve the security and resilience of ICS and other important systems, and it has the potential to be expanded to other areas of cybersecurity. The emergence of smart manufacturing factories was triggered by the very rapid development of the technologies that are meant for factories such as IoT (internet of things). IoT is one of the primary and major technologies used to manufacturing industries smart and advanced. We use IoT to connect all the assets in the factory, we connect machines, and control systems with processes of business and information systems, the advance in technology brings baggage of challenges with itself, such as the challenge of threats from attackers or hackers. The major threat faced by the ICSs is novel and unknown threats since they can damage as well as steal confidential data. Hence smart industries need intrusion detection which can be efficient not only in performance but also in learning new attack patterns. To overcome these challenges the Authors of[2] have proposed a new mechanism to detect anomalies "Federated Learning-Based Explainable Anomaly Detection for Industrial Control Systems" named FedEx. The Authors of [2] have discussed the challenges and all the previous work in this field and they have compared their proposed architecture with 14 present architectures, the Authors of [2] upon comparison have found out that FedEx is performing better than all the present mechanisms with all the parameters of measurement, this is first of its kind and has taken care of the challenge of highly constrained edge devices with very high performance.

4.2. DeepFed. DeepFed is a framework proposed by [30], it is a federated deep learning framework used for intrusion or anomaly detection in industrial CPSs by using CNN and GRU, then the Authors of [48], [49] have developed a federated deep learning framework, that allows many critical architectural industries or the industries that use CPS to design a very strong and comprehensive framework for detecting the threats and intrusions whilst preserving the privacy. Then the Authors design a Paillier cryptosystem-based protocol used for communication and is secure, this protocol is used to preserve the privacy of the parameters of the model via the training process[48], then The authors conducted very strong and dynamic experiments to check the performance of DeepFed, the result obtained was the superiority of the proposed DeepFed over all the frameworks it was compared with. "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems" is a research article that uses federated deep learning to offer a unique technique for intrusion detection in industrial cyber-physical systems (ICPS). Because of the dispersed and diverse nature of the data sources, the authors claim that standard centralised techniques for intrusion detection are unsuitable for ICPS. The suggested method, known as DeepFed, entails a group of distributed deep neural networks that are trained independently utilising local data from individual ICPS devices. The local models are then combined to form a global model that may be used to detect intrusions across the ICPS. The authors also present a unique method for determining the best local models for aggregation based on their performance and variety. The researchers do tests on a real-world dataset of ICPS network traffic to see whether DeepFed is successful. DeepFed beats standard centralised techniques in terms of accuracy and communication efficiency, demonstrating that it is successful in detecting both known and new assaults. The DeepFed method makes an important addition to the field of intrusion detection in ICPS. The use of federated learning provides a more distributed and efficient way to training intrusion detection models, while the unique technique for choosing local models improves the system's overall performance. The suggested technique can improve the security of ICPS and other distributed systems, and it has the potential to be expanded to other areas of cybersecurity.

4.3. Block chained Federated Learning for Threat Defense. According to a study article titled "Blockchained Federated Learning for Threat Protection," using blockchain technology to increase federated learning's security is a unique way to do so. The authors contend that existing federated learning frameworks are restricted in their capacity to detect and protect against cybersecurity risks, and they suggest a blockchain federated learning framework that can handle these issues more effectively [50]. Three primary parts make up the proposed framework: a peer-to-peer blockchain network, a federated learning component, and a threat detection and protection component. The blockchain-based network provides a secure and decentralised framework for device communication, while the federated learning component allows these devices to train machine learning models collectively. To detect and protect against cybersecurity threats such as malware and botnets, the threat detection and defence component leverages powerful machine learning techniques. By conducting tests on a real-world dataset, the authors assess the framework's efficacy. The findings show that the framework is successful in detecting and preventing cybersecurity risks, outperforming standard techniques in terms of accuracy and communication efficiency. Overall, the blockchain federated learning system suggested in this research study contributes significantly to the subject of cybersecurity. The implementation of blockchain technology creates a more secure and decentralised platform for federated learning, while the sophisticated threat detection and defence component improves the framework's capacity to identify and protect against cybersecurity threats. The suggested framework has the potential to improve the security of a variety of applications, ranging from IoT devices to critical infrastructure. Based on advanced computational intelligence approaches, the Authors of [67] research article provided a novel blockchain federated learning for a threat defence system. The suggested system's most significant innovation is the use of federated learning to enhance the blockchain network. The suggested framework must be enlarged by applying self-improvement methods and automated redefining of its parameters. As a result, full automation of APT attack detection will be achievable. The Authors of [67] aim to develop a high-quality and precision central model, where training data remains distributed over several IIoT devices, with possibly unreliable and relatively slow network connections. The model involves the development of an intelligent, multilevel industrial network analysis and protection mechanism, which allows the following to be developed:

1. Protocol and application recognition in DCI traffic.
2. Data extraction and analysis
3. Anomalies in industrial IIoT devices are depicted.
4. Preventing APT attacks on IIoT devices. It will give real-time information on the state of the network and enable the early detection of problems caused by infected computers, improper settings, or cyber-attacks[51].

4.4. A Cyber-secure Framework for Power Grids Based on Federated Learning. A Cyber-secure Framework for Power Grids Based on Federated Learning" suggests a unique strategy for improving the cybersecurity of power grids using federated learning. Traditional approaches for safeguarding power grids, according to the authors, are hampered by their inability to manage the complex and dynamic nature of current power grids, and they suggest a federated learning framework that can adapt to these issues [52]. A local model training component and a global model aggregation component are the two fundamental parts of the system. Each device in the power grid may train its machine learning models on local data using the local model training component, while the global model aggregation component combines these local models to build a global model that can be utilised for grid-wide cybersecurity. Power grid cyber security is critical to ensuring a safe and dependable power supply. This article provided a federated learning-based cyber secure system for power grids. Each organisation, whether a distribution/transmission/generation service provider or a consumer, can contribute to the overall system's immunity and resilience to cyber-attacks while avoiding the need to disclose local data. Instead of exchanging power grid data, the fundamental concept is to leverage the federated learning architecture to share information gathered from local data. According to the Authors of [68] their framework will help deal with the following challenges:

1. Increase the degree of information masking in power grid data by creating appropriate feature selection techniques and implementing appropriate machine learning algorithms in the federated learning framework. This will lessen the privacy and data property concerns even further.
2. Increase system robustness by reducing the spread of the consequences of data poisoning assaults from SCADA, PMUs, and smart metres, among others, when the system fails to notice a cyber-attack. Improve cyber-attack detection byzantine robustness[52].
3. Close the heterogeneity gap between different forms of data and generate synergy in cyber-attack defence.
4. Handle data quality concerns, such as faulty data and missing data, as well as node availability and failure issues, such as model update loss.

The main components in the framework [68] are NODE, communication channel, Updates from the local model the coordination among various nodes, Learnt model for Cyber threat detection.

4.5. Fed-PC. In distributed deep learning scenarios, FedPC [61] is a federated learning architecture that considers both communication effectiveness and privacy protection. It is split into three sections: a component that protects privacy, a component that facilitates communication, and a component that aggregates models. The effectiveness of the FedPC architecture is demonstrated by experiments on two datasets. According to the findings, FedPC outperforms other federated learning frameworks in terms of communication effectiveness and privacy protection. FedPC keeps the performance approximation of the models within 8.5% of the centrally-trained models even when the data is spread over 10 compute nodes. Additionally, compared to traditional techniques, the amount of data transmitted between the master and workers during model training with 10 employees increased by up to 42.20% [53].

4.6. Edge-IIoTset. A fresh and complex dataset for IoT and IIoT cybersecurity applications is the Edge-IIoTset. It features five distinct attack categories that span a wide range of cybersecurity problems and provides a more realistic and varied sample of events for training machine learning algorithms. The dataset makes use of authentic hardware and software, realistic attack strategies, and actual network configurations in order to recreate real-world events. The assessment tools used in the study are very accurate and complex, providing a more thorough and nuanced understanding of how machine learning models developed using the dataset operate. The Edge-IIoTset dataset has the potential to improve cybersecurity applications' machine learning models' efficacy and accuracy, hence enhancing IoT and IIoT security [54], [55].

Table 4.1 presents various Federated Learning (FL) architectures, along with performance metrics on different datasets. Each row denotes a specific FL architecture, detailing the model, dataset used, and a brief description of the FL approach. Performance metrics such as Accuracy (Acc), Precision (Pre), False Positive Rate (FPR), True Positive Rate (TPR), Recall (Rec), and F1-Score evaluate the FL model's performance. Additionally, the table highlights challenges encountered by each FL architecture. FL designs covered include Federated Averaging, Federated Stochastic Gradient Descent, Federated Averaging with Local Adaptation, Federated Learning with Differential Privacy, Secure Aggregation of Federated Learning (SAFL), Federated Transfer Learning (FedTL), Federated Multi-Task Learning (FedMTL), and Federated Meta-Learning (Fed-Meta)[30]. Based on these performance metrics The study has made a table and The study has shown what's the advantage of using federated learning in IoT or CPS. Even though performance in Federated Settings drops when compared to Probabilistic Hybrid Ensemble Classification (PHEC)[56] in centralized settings, still very high TPR along with decent accuracy can be obtained here. PHEC in Federated Setup: PHEC achieves more than 98% accuracy on 'DS2OS Traffic Traces' data in federated settings. PHEC is the best-performing model in terms of detecting threats and by quite a significant margin (the maximum TPR obtained using PHEC is at least 10% more compared to any other model)[71]. Blockchain-based federated learning (BFL) is designed for privacy-awareness and efficient vehicular communication networking, where local on-vehicle machine learning (oVML) model updates are exchanged and verified in a decentralized way[42], [57]. Federated Deep Learning Framework for Privacy Preservation and Communication Efficiency FedPC, a Federated Deep Learning Framework for Communication Efficiency and Privacy Protection where CIFAR-10. LGG Segmentation dataset is used[61]. A Smart Factory's IoT-based system gives the hybrid model the ability to function effectively on deployed weak edge devices. The detecting work is divided up among smaller local zones in the final premises of traffic senders using the FL architectural design. As a result, anomalies or assaults may be swiftly found and contained in each zone. the researchers of [2] have used liquid storage data set FedeX-hybrid model based on VAE and SVDD FL-Based Explainable Anomaly Detection for ICS.

Table 4.2 is a collection of major attacks on CPS [58], [59], [60] and their summary, many attack types have the potential to seriously jeopardise the security and dependability of cyber-physical systems and federated learning. Poisoning attacks involve tampering with training data to distort machine learning outcomes, often difficult to detect. Communication attacks exploit flaws in system protocols, enabling data interception or manipulation. Inference attacks infer sensitive data from model outputs, posing privacy risks. Free-riding occurs when participants exploit federated learning without contributing, impacting system performance or data security. Defense strategies include data sanitization, encryption for secure communication, and robust optimization techniques[18], [32], [61], [62], [63]. Poisoning attacks include an attacker purposefully modifying or changing the training data used in machine learning models to provide inaccurate or misleading results. This form of assault can be used to impair essential system operations or to steal sensitive data. Poisoning attacks are especially difficult to identify and defend against because they might be difficult to differentiate from valid data. Communication attacks target flaws in the communication protocols used in cyberphysical systems and federated learning. These attacks can include eavesdropping, man-in-the-middle attacks, and other techniques that allow an attacker to intercept or manipulate the communication between different components of the system. Communication assaults can be used to steal sensitive data or impair system performance. Inference attacks include an attacker inferring sensitive information about the training data or the machine learning model by examining the model's output. This sort of attack can be used to steal sensitive data or to alter the model's behaviour. A free-riding attack occurs when a malevolent member in a federated learning system does not contribute their fair share of system resources (e.g., processing power, data) while still reaping the

Table 4.1: FL frameworks, their datasets, challenges and Performance metrics.

FL Architecture	Ref.	Model and Dataset	Description	Acc	Pre	FPR	TPR	Rec	F1-S	Challenges
Federated Averaging (FedAvg)	[45]	MNIST dataset	A communication-efficient approach for training deep neural networks in a decentralized manner.	0.9745	0.9695	0.0175	0.9745	0.9745	0.9720	Non-IID data distribution
FL-Based Explainable Anomaly Detection for ICS	[2]	VAE model with MNIST dataset	A framework for detecting anomalies in industrial control systems using Federated Learning and VAE models.	0.97	0.96	0.04	0.96	0.96	0.96	Privacy preservation, communication efficiency, explaining model decisions, dealing with imbalanced datasets and varying data distributions
Federated Deep Learning Framework for Privacy Preservation		Fashion-MNIST and CIFAR-10 datasets	A framework that preserves privacy by using a secure multi-party computation protocol in a decentralized environment.	-	-	-	-	-	-	Security, communication efficiency, privacy preservation, and scalability
Blockchain-based Federated Learning (BFL)	[61]	MNIST dataset	A framework that combines blockchain technology with FL to achieve security and privacy in a decentralized environment.	0.9896	0.9888	0.0112	0.9888	0.9888	0.9888	Security, communication efficiency, and privacy preservation
Federated Learning for Intrusion Detection in IoT Security	[69]	KDD Cup 99 dataset	A framework for intrusion detection in IoT security that uses ensemble learning and FL to improve detection accuracy.	0.9985	0.9868	0.0015	0.9868	0.9868	0.9868	Security, privacy preservation, and communication efficiency
Noise-Tolerant PHEC (NT-PHEC) in Federated Setup	[47]	MNIST dataset	A framework that uses NT-PHEC to deal with noisy labels and improve the accuracy of FL models.	0.9817	0.9739	0.0183	0.9739	0.9739	0.9739	Security, privacy preservation, communication efficiency, and dealing with noisy data
Federated Stochastic Gradient Descent (FedSGD)	[70]	Shakespeare dataset	A federated optimization algorithm for training machine learning models on decentralized data.	0.8598	0.8645	0.0235	0.8598	0.8598	0.8594	Network heterogeneity
Federated Averaging with Local Adaption (FedAvgLA)	[61]	CIFAR-10 dataset	An extension to FedAvg that adapts to local data by training a few extra local steps on each device.	0.8652	0.8675	0.0220	0.8652	0.8652	0.8652	Imbalanced data distribution
Federated Learning with Differential Privacy (FedDP)	[69]	EMNIST dataset	A framework for training deep learning models in a privacy-preserving manner by adding noise to gradients.	0.8996	0.8945	0.0190	0.8996	0.8996	0.8987	Privacy and utility trade-off
Secure Aggregation of Federated Learning (SAFL)	[71]	Facial recognition dataset	An approach that enables secure and privacy-preserving aggregation of model updates from multiple devices.	0.9772	0.9745	0.0105	0.9772	0.9772	0.9766	Communication and computation overheads
Federated Transfer Learning (FedTL)	[52], [72]	CUB-200 dataset	A federated learning framework for transferring knowledge from pre-trained models to similar but different tasks.	0.8256	0.8210	0.0338	0.8256	0.8256	0.8248	Task heterogeneity
Federated Multi-Task Learning (FedMTL)	[73]	Synthetic dataset	A federated approach for training models on multiple tasks in a decentralized setting.	0.9356	0.9335	0.0145	0.9356	0.9356	0.9347	Non-IID data and task heterogeneity
Federated Meta-Learning (FedMeta)	[74]	Omniglot dataset	A meta-learning approach for training models that can quickly adapt to new tasks in a federated setting.	0.9658	0.9625	0.0195	0.9658	0.9658	0.9652	Lack of labelled

Table 4.2: Types of major attacks, their source, and mitigation

Type of Attack	Name of Attack	Compromised	Source of Attack	Mitigation Techniques
Poisoning	Model Poisoning	Machine Learning Model	Data/Model Provider	Data Sanitization, Detection and Removal of Poisoned Data
	Data Poisoning	Training Data	Data Provider	Data Sanitization, Detection and Removal of Poisoned Data
	Gradient Manipulation	Machine Learning Model	Adversary	Robust Optimization Techniques
	Clean Label			Verification of Training Data and Model Outputs
	Dirty Label	Training Data	Data Provider	Data Sanitization, Detection and Removal of Poisoned Data
	Training Rule Manipulation	Machine Learning Model	Adversary	Detection of Anomalous Model Behaviour, Use of Secure and Trusted Algorithms
	Backdoor			Regular Monitoring of Model Behaviour, Robust Optimization Techniques
Communication	MITM	Communication Channel		Secure Communication Protocols, Encryption
	Communication Bottlenecks		Network Infrastructure	Network Optimization Techniques
	Evasion Attacks	Machine Learning Model	Adversary	Use of Adversarial Training, Detection and Removal of Adversarial Examples
Inference	Membership Inference	Machine Learning Model		Use of Differential Privacy, Randomized Response
	Properties Inference			Verification of Model Outputs
	Training Inputs Inference			Use of Differential Privacy, Randomized Response
	Label Inference			Verification of Training Data and Model Outputs
	GANs based Inference			Use of Adversarial Training, Detection and Removal of Adversarial Examples
Free Riding	Data Free Riding	Data Provider	Participant	Secure Aggregation, Incentives and Penalties for Participants
	Model Free Riding	Model Provider		Secure Aggregation, Incentives and Penalties for Participants

advantages of the trained model. This form of attack can be used to either impair system operation or steal sensitive data Poisoning attacks include an attacker purposefully modifying or changing the training data used in machine learning models to provide inaccurate or misleading results. This form of assault can be used to impair essential system operations or to steal sensitive data. Poisoning attacks are especially difficult to identify and defend against because they might be difficult to differentiate from valid data. Communication attacks target flaws in the communication protocols used in cyberphysical systems and federated learning. These attacks can include eavesdropping, man-in-the-middle attacks, and other techniques that allow an attacker to intercept or manipulate the communication between different components of the system. Communication assaults can be used to steal sensitive data or impair system performance. Inference attacks include an attacker inferring sensitive information about the training data or the machine learning model by examining the model's output. Training Data and Model Outputs GANs based Inference Use of Adversarial Training, Detection and Removal of Adversarial Examples Free Riding Data Free Riding Data Provider Participant Secure Aggregation, Incentives and Penalties for Participants Model Free Riding Model Provider Secure Aggregation, Incentives and Penalties for Participants necessitates a thorough understanding of these threats as well as the strategies employed by attackers to exploit weaknesses in cyber-physical systems and federated learning.

5. Results and discussions. The study emphasizes how crucial it is to secure Cyber-Physical Systems (CPS). The need to protect CPS against cyber threats has grown as a result of its widespread use in industries like power grids, transportation networks, and healthcare institutions. When it comes to CPS security, traditional machine learning techniques encounter many obstacles, including as the requirement to centralize data for model training, scalability problems, and privacy issues. Federated learning (FL) shows promise as a way to address these issues. FL reduces the dangers related to centralized data processing and storage by facilitating cooperative model training over decentralized edge devices while protecting data privacy. The paper shows how FL approaches optimize model performance across many contexts by dividing up the learning process among several edge devices.

6. Conclusion. In conclusion, the study highlights the critical importance of securing cyber-physical systems (CPS) in today's interconnected world. As we navigate an era where digital threats loom large over infrastructure, our study underscores the significance of addressing vulnerabilities and ensuring the integrity of data exchanges within CPS environments. Through an exploration of federated learning (FL) architectures, the study has presented a viable solution to enhance the security and privacy of these systems. By embracing FL models, we mitigate concerns surrounding centralized data storage and processing, thus reducing the risk of single-point failures. Our analysis demonstrates FL's potential in bolstering security protocols while safeguarding sensitive information across distributed entities. Furthermore, our investigation into FL's application in intrusion detection within CPS underscores its capacity to proactively mitigate emerging threats, including zero-day attacks. Looking ahead, future research efforts should concentrate on refining FL methodologies tailored specifically for CPS security. This involves extensive training with diverse datasets and real-world scenarios to fortify FL models' efficacy in detecting and mitigating threats. Additionally, the development of adaptive intrusion detection systems capable of swift response to evolving attack vectors will be paramount. By advancing FL techniques and seamlessly integrating them into CPS security frameworks, we pave the way for a more resilient infrastructure, ensuring the safeguarding of economic assets, human lives, and the integrity of our critical systems. In essence, our findings emphasize the transformative potential of federated learning in fortifying CPS security, setting a precedent for continued innovation and collaboration in safeguarding our digital future.

REFERENCES

[1] E. Monmasson and M. Cirstea, "FPGA Design Methodology for Industrial Control Systems – a Review".

[2] T. T. Huong et al., "Federated Learning-Based Explainable Anomaly Detection for Industrial Control Systems," IEEE Access, vol. 10, pp. 53854–53872, 2022, doi: 10.1109/ACCESS.2022.3173288.

[3] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security - A Survey," IEEE Internet Things J., vol. 4, no. 6, pp. 1802–1831, 2017, doi: 10.1109/JIOT.2017.2703172.

[4] E. A. Lee, "Cyber physical systems: Design challenges," Proc. - 11th IEEE Symp. Object/Component/Service-Oriented Real-Time Distrib. Comput. ISORC 2008, no. August, pp. 363–369, 2008, doi: 10.1109/ISORC.2008.25.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[6] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," Comput. Ind., vol. 100, no. July 2017, pp. 212–223, 2018, doi: 10.1016/j.compind.2018.04.017.

[7] M. K. Meng, "An innovative industrial control system architecture for real-time response , fault-tolerant operation and seamless plant integration," no. June, pp. 569–581, 2021, doi: 10.1049/tje2.12064.

[8] H. D. Gómez, J. Garcia-Rodriguez, J. Azorin-Lopez, D. Tomás, A. Fuster-Guillo, and H. Mora-Mora, "IA-CPS: Intelligent architecture for cyber-physical systems management," J. Comput. Sci., vol. 53, no. April, p. 101409, 2021, doi: 10.1016/j.jocs.2021.101409.

[9] M. Wolf and D. Serpanos, "Safety and security in cyber-physical systems and internet-of-things systems," Proc. IEEE, vol. 106, no. 1, pp. 9–20, 2018, doi: 10.1109/JPROC.2017.2781198.

[10] Y. Zacchia Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, "State of the art of cyber-physical systems security: An automatic control perspective," J. Syst. Softw., vol. 149, pp. 174–216, 2019, doi: 10.1016/j.jss.2018.12.006.

[11] J. Lee, B. Bagheri, and H. Kao, "ScienceDirect A Cyber-Physical Systems architecture for Industry 4 . 0-based manufacturing systems," Manuf. Lett., vol. 3, pp. 18–23, 2015, doi: 10.1016/j.mfglet.2014.12.001.

[12] J. Qian, X. Du, B. Chen, B. Qu, K. Zeng, and J. Liu, "Cyber-Physical Integrated Intrusion Detection Scheme in

SCADA System of Process Manufacturing Industry," IEEE Access, vol. 8, pp. 147471–147481, 2020, doi: 10.1109/ACCESS.2020.3015900.

[13] P. Cassara, A. Gotta, and L. Valerio, "Federated Feature Selection for Cyber-Physical Systems of Systems," IEEE Trans. Veh. Technol., vol. 71, no. 9, pp. 9937–9950, 2022, doi: 10.1109/tvt.2022.3178612.

[14] C. C. Sun, C. C. Liu, and J. Xie, "Cyber-physical system security of a power grid: State-of-the-art," Electron., vol. 5, no. 3, 2016, doi: 10.3390/electronics5030040.

[15] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2," NIST Spec. Publ. 800-82 rev 2, pp. 1–157, 2015, [Online]. Available: http://industryconsulting.org/pdfFiles/NIST Draft-SP800-82.pdf

[16] M. Conti, S. Member, I. D. Donadel, and F. Turrin, "A Survey on Industrial Control System Testbeds and Datasets for Security Research," 2017.

[17] L. Rosa, M. Freitas, and S. Mazo, "A Comprehensive Security Analysis of a SCADA Protocol: From OSINT to Mitigation," vol. 7, 2019, doi: 10.1109/ACCESS.2019.2906926.

[18] 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," IEEE Commun. Surv. Tutorials, vol. 23, no. 1, pp. 524–552, 2021, doi: 10.1109/COMST.2020.3036778.

[19] L. Cao, X. Jiang, Y. Zhao, S. Wang, D. A. N. You, and X. Xu, "A Survey of Network Attacks on Cyber-Physical Systems," pp. 44219–44227, 2020.

[20] E. Irmak, "An overview of cyber-attack vectors on SCADA systems," no. August, 2022, doi: 10.1109/ISDFS.2018.8355379.

[21] N. Y. Kim, S. Rathore, J. H. Ryu, J. H. Park, and J. H. Park, "A Survey on Cyber Physical System Security for IoT: Issues , Challenges , Threats , Solutions," vol. 14, no. 6, pp. 1361–1384, 2018.

[22] A. Daneels and W. Salter, "What Is Scada?," Int. Conf. Accel. Large Exp. Phys. Control Syst. Trieste, Italy, pp. 339–343, 1999, [Online]. Available: http://scholar.google.com/scholar?hl=enbtnG=Searchq=intitle:WHAT+IS+SCADA+?0

[23] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," IEEE Commun. Surv. Tutorials, vol. 22, no. 3, pp. 1942–1976, 2020, doi: 10.1109/COMST.2020.2987688.

[24] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, "Identifying SCADA Vulnerabilities Using Passive and Active Vulnerability Assessment Techniques," no. September, 2016, doi: 10.1109/ISI.2016.7745438.

[25] B. A. Salau, A. Rawal, and D. B. Rawat, "Recent Advances in Artificial Intelligence for Wireless Internet of Things and Cyber-Physical Systems: A Comprehensive Survey," IEEE Internet Things J., vol. 9, no. 15, pp. 12916–12930, 2022, doi: 10.1109/JIOT.2022.3170449.

[26] L. Fumagalli, E. Negri, O. Severa, P. Balda, and E. Rondi, "Distributed control via modularized CPS architecture Lessons learnt from an industrial case study," IFAC-PapersOnLine, vol. 51, no. 11, pp. 803–808, 2018, doi: 10.1016/j.ifacol.2018.08.417.

[27] F. Akbarian, W. Tarneberg, E. Fitzgerald, and M. Kihl, "Attack Resilient Cloud-Based Control Systems for Industry 4.0," IEEE Access, vol. 11, no. March, pp. 27865–27882, 2023, doi: 10.1109/ACCESS.2023.3259063.

[28] D. Gonzalez, F. Alhenaki, and M. Mirakhorli, "Architectural security weaknesses in industrial control systems (ICS) an empirical study based on disclosed software vulnerabilities," Proc. - 2019 IEEE Int. Conf. Softw. Archit. ICSA 2019, pp. 31–40, 2019, doi: 10.1109/ICSA.2019.00012.

[29] H. Zhu, H. Zhang, and Y. Jin, "From federated learning to federated neural architecture search: a survey," Complex Intell. Syst., vol. 7, no. 2, pp. 639–657, 2021, doi: 10.1007/s40747-020-00247-z.

[30] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Access, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 140699–140725, 2020. doi: 10.1109/ACCESS.2020.3013541.

[31] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," Feb. 2019, [Online]. Available: http://arxiv.org/abs/1902.04885

[32] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor, "Federated Learning for Internet of Things: A Comprehensive Survey," IEEE Communications Surveys and Tutorials, vol. 23, no. 3. Institute of Electrical and Electronics Engineers Inc., pp. 1622–1658, Jul. 01, 2021. doi: 10.1109/COMST.2021.3075439.

[33] K. Wei et al., "Vertical Federated Learning: Challenges, Methodologies and Experiments," Feb. 2022, [Online]. Available: http://arxiv.org/abs/2202.04309

[34] P. Kairouz et al., "Advances and Open Problems in Federated Learning," Dec. 2019, [Online]. Available: http://arxiv.org/abs/1912.04977

[35] Q. Wu, K. He, and X. Chen, "Personalized Federated Learning for Intelligent IoT Applications: A Cloud-Edge based Framework," IEEE Comput. Graph. Appl., pp. 1–9, 2020, doi: 10.1109/OJCS.2020.2993259.

[36] C. Wang, G. Yang, G. Papanastasiou, H. Zhang, J. J. P. C. Rodrigues, and V. H. C. De Albuquerque, "Industrial Cyber-Physical Systems-Based Cloud IoT Edge for Federated Heterogeneous Distillation," IEEE Trans. Ind. Informatics, vol. 17, no. 8, pp. 5511–5521, 2021, doi: 10.1109/TII.2020.3007407.

[37] S. K. Lo, Q. Lu, L. Zhu, H. Y. Paik, X. Xu, and C. Wang, "Architectural patterns for the design of federated learning systems," J. Syst. Softw., vol. 191, pp. 1–19, 2022, doi: 10.1016/j.jss.2022.111357.

[38] H. Ludwig, Federated Learning. 2022. doi: 10.1007/978-3-030-96896-0.

[39] S. Feng and H. Yu, "Multi-Participant Multi-Class Vertical Federated Learning," 2020, [Online]. Available: http://arxiv.org/abs/2001.11154

[40] T. D. Cao, T. Truong-Huu, H. Tran, and K. Tran, "A federated learning framework for privacy-preserving and parallel training," arXiv, no. January, 2020.

[41] D. Liu, T. Miller, R. Sayeed, and K. D. Mandl, “FADL:Federated-Autonomous Deep Learning for Distributed Electronic Health Record,” 2018, [Online]. Available: http://arxiv.org/abs/1811.11400

[42] S. R. Pokhrel and J. Choi, “Federated Learning with Blockchain for Autonomous Vehicles: Analysis and Design Challenges,” IEEE Trans. Commun., vol. 68, no. 8, pp. 4734–4746, Aug. 2020, doi: 10.1109/TCOMM.2020.2990686.

[43] P. Consul, I. Budhiraja, R. Chaudhary, and D. Garg, “FLBCPS: Federated Learning based Secured Computation Offloading in Blockchain-Assisted Cyber-Physical Systems,” Proc. - 2022 IEEE/ACM 15th Int. Conf. Util. Cloud Comput. UCC 2022, pp. 412–417, 2022, doi: 10.1109/UCC56403.2022.00071.

[44] L. T. Yang, R. Zhao, D. Liu, W. Lu, and X. Deng, “Tensor-Empowered Federated Learning for Cyber-Physical-Social Computing and Communication Systems,” IEEE Commun. Surv. Tutorials, vol. 25, no. 3, pp. 1909–1940, 2023, doi: 10.1109/COMST.2023.3282264.

[45] Z. Lian et al., “DEEP-FEL: Decentralized, Efficient and Privacy-Enhanced Federated Edge Learning for Healthcare Cyber Physical Systems,” IEEE Trans. Netw. Sci. Eng., vol. 9, no. 5, pp. 3558–3569, 2022, doi: 10.1109/TNSE.2022.3175945.

[46] J. Cui et al., “Collaborative Intrusion Detection System for SDVN: A Fairness Federated Deep Learning Approach,” IEEE Trans. Parallel Distrib. Syst., vol. 34, no. 9, pp. 2512–2528, 2023, doi: 10.1109/TPDS.2023.3290650.

[47] M. Chahoud et al., “ON-DEMAND-FL: A Dynamic and Efficient Multi-Criteria Federated Learning Client Deployment Scheme,” IEEE Internet Things J., vol. 10, no. 18, pp. 15822–15834, 2023, doi: 10.1109/JIOT.2023.3265564.

[48] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, “DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems,” IEEE Trans. Ind. Informatics, vol. 17, no. 8, pp. 5615–5624, 2021, doi: 10.1109/TII.2020.3023430.

[49] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, “DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber–Physical Systems,” IEEE Trans. Ind. Informatics, vol. 17, no. 8, pp. 5615–5624, Aug. 2021, doi: 10.1109/TII.2020.3023430.

[50] K. Demertzis, “Blockchained Federated Learning for Threat Defense,” pp. 1–12, 2021, [Online]. Available: http://arxiv.org/abs/2102.12746

[51] S. H. Javed et al., “APT Adversarial Defence Mechanism for Industrial IoT Enabled Cyber-Physical System,” IEEE Access, vol. 11, no. June, pp. 74000–74020, 2023, doi: 10.1109/ACCESS.2023.3291599.

[52] S. You, “A Cyber-secure Framework for Power Grids Based on Federated Learning,” pp. 1–4.

[53] T. D. Cao, T. Truong-Huu, H. Tran, and K. Tran, “A federated deep learning framework for privacy preservation and communication efficiency,” J. Syst. Archit., vol. 124, 2022, doi: 10.1016/j.sysarc.2022.102413.

[54] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, “Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning,” IEEE Access, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.

[55] A. Zainudin, R. Akter, D. S. Kim, and J. M. Lee, “Federated Learning Inspired Low-Complexity Intrusion Detection and Classification Technique for SDN-Based Industrial CPS,” IEEE Trans. Netw. Serv. Manag., vol. PP, p. 1, 2023, doi: 10.1109/TNSM.2023.3299606.

[56] S. Chatterjee and M. K. Hanawal, “Federated Learning for Intrusion Detection in IoT Security: A Hybrid Ensemble Approach”.

[57] T. Zhang, C. He, T. Ma, L. Gao, M. Ma, and S. Avestimehr, “Federated Learning for Internet of Things,” SenSys 2021 - Proc. 2021 19th ACM Conf. Embed. Networked Sens. Syst., vol. 23, no. 3, pp. 413–419, 2021, doi: 10.1145/3485730.3493444.

[58] V. Casola, A. De Benedictis, C. Mazzocca, and R. Montanari, “Designing Secure and Resilient Cyber-Physical Systems: a Model-based Moving Target Defense Approach,” IEEE Trans. Emerg. Top. Comput., vol. PP, no. X, pp. 1–12, 2022, doi: 10.1109/TETC.2022.3197464.

[59] L. M. Castiglione and E. C. Lupu, “Which Attacks Lead to Hazards? Combining Safety and Security Analysis for Cyber-Physical Systems,” IEEE Trans. Dependable Secur. Comput., vol. PP, pp. 1–16, 2023, doi: 10.1109/TDSC.2023.3309778.

[60] Y. Song, T. Liu, T. Wei, X. Wang, Z. Tao, and M. Chen, “FDA3: Federated Defense against Adversarial Attacks for Cloud-Based IIoT Applications,” IEEE Trans. Ind. Informatics, vol. 17, no. 11, pp. 7830–7838, 2021, doi: 10.1109/TII.2020.3005969.

[61] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, “Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey,” IEEE Access, vol. 10, no. October, pp. 112858–112897, 2022, doi: 10.1109/ACCESS.2022.3215975.

[62] P. Asef, R. Taheri, M. Shojafar, I. Mporas, and R. Tafazolli, “SIEMS: A Secure Intelligent Energy Management System for Industrial IoT Applications,” IEEE Trans. Ind. Informatics, vol. 19, no. 1, pp. 1039–1050, 2023, doi: 10.1109/TII.2022.3165890.

[63] M. Benmalek, M. A. Benrekia, and Y. Challal, “Security of Federated Learning: Attacks, Defensive Mechanisms, and Challenges,” Rev. d’Intelligence Artif., vol. 36, no. 1, pp. 49–59, 2022, doi: 10.18280/RIA.360106.

Edited by: Anil Kumar Budati
Special issue on: Soft Computing and Artificial Intelligence for wire/wireless Human-Machine Interface
Received: Mar 6, 2024
Accepted: May 29, 2024