***Cyber-physical systems - Advances and Applications, 2022,* 3-32 3**

**CHAPTER-7**

**CYBER-PHYSICAL SYSTEM: ADVANCES AND APPLICATIONS IN CYBER SECURITY**

**Sindhu Rajendran\*, Shilpa S P, SaiPriya L, Ramavenkateswaran N**

*Department of Electronics and Communication, R. V. College of Engineering Bangalore-560059*

**Abstract**: A cyber-physical system is a computer system that operates or monitors a mechanism using computer-based algorithms. Due to the rapid evolution of CPS in today's world, a greater range of services and applications involving e-Health, smart homes, e-Commerce, and industry automation may be easily realized, affecting numerous parts of people's lives. Smart grid, autonomous underwater, and UAVs, gas and oil pipeline monitoring and control, smart factory and manufacturing, pollution control, and HEVs are among the most prominent applications in this domain.

Interconnecting the cyber and physical worlds, on the other hand, introduces new security threats. Security attacks can result in trouble to essential infrastructure and business continuity, including production-performance deterioration, severe commercial risks, unavailability of critical services, and regulatory violations. Cybersecurity attacks are one of the most serious dangers to CPS due to the system's complexity and interdependencies, owing to which risk management is difficult considering recent attack trends. The first section of the manuscript discusses the evolution of CPS and its wide range of applications in different areas, followed by in-depth insights into the industrial sector. Types of cyber and physical threats, as well as examples, various system components, related algorithms and models, attack characteristics, and defense measures, are explained. Current study classifications are assessed and summarized using various system modeling and analytic approaches along with the benefits and drawbacks of various techniques. The chapter is concluded by stating future research topics on secure CPS and potential solutions.

***4 Cyber-physical systems -Advances and Applications Rajendran et al.***

**Keywords**: Cyber security, physical threats, Safety and Security, Cyber-physical system, Industry 4.0, security model, Denial of services, binary hypothesis, deception attack, reply attack, threat modelling, privacy, Bayesian detection, weighted least square, threat model, digital twin, RNN based security, FACT graph, security algorithm, cryptography.

**INTRODUCTION**

Smart data operation, data analysis, and processing capability that leads to the growth of cyberspace; advanced integration that gives significant data access from the material world and knowledge feedback from cyberspace. A cyber-physical system (CPS) regulates or controls a medium using computer-based algorithms. Because of their possible significant effect on society, geography, and thriftiness, CPS is present of attention in academia, assiduity, and government [1].

CPS is used to improve large-scale system implementation by boosting adaptation, functionality, autonomy, efficiency, dependability, safety, and usability. CPS research is divided into two main categories: conceptual foundations and applications for meeting business requirements impacted by software architecture. CPS research is still in its early stages, despite some success in system structure, product innovations, and practical applications. CPS is employed in many different industries, including health, manufacturing, energy, transport, agriculture, and ambient intelligence [2].

CPSs are powered by three types of computer systems: desktop servers, laptops. To conduct business, every desk has a computer, and embedded computing is altering industries and becoming an unseen component of the environment. CPS's primary features are communication, intelligence, corporation, network, and cloud solutions. Functionality and usability are important considerations. These are the distinguishing features: Computer and physical processes, according to CPS, are inextricably linked. Wireless sensor networks are used in CPS networks, and software is incorporated into physical systems.

**Evolution of CPS:**

Though William Gibson is attributed with inventing a new term "cyberspace" in his work Neuromancer, the term CPS has longer and deeper roots. It would be more accurate to regard the terms "cyberspace" and "cyber-physical systems" to be

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications* 5**

derived from the same origin, "cybernetics," which has been introduced in the book Cybernetics by American mathematician Norbert W. Deutsch. The term is derived from the Greek word Kubernetes, which also refers to a helmsman, ruler, pilot, or rudder. The comparison works well with control systems. The terms "CPS" and "cybersecurity," which both refer to data privacy, accuracy, and availability yet have nothing to do with physical phenomena, are sometimes used interchangeably.

As a result, the phrase "cybersecurity" refers to the safety of cyberspace which has little to do with cybernetics. Although CPS has a variety of difficult security and privacy concerns, they are far from alone. According to Stipanovic, Cyber-Physical Systems are a brand-new field of research at the intersection of either the physical, biotechnological, engineering, or information sciences. They supply the integrated whole with abstractions, modeling design, and analytic approaches. In a nutshell, they combine physical process dynamics with software and communication dynamics. As a result of the interactions, thoughts become physical and virtual forms, resulting in novel emergent scenarios, also known as emergence, necessitating the development of new design techniques. Computing, embedded devices, and networking are all examples of these technologies [3].

By merging the 3Cs of computation, communication, and controls, the CPS builds an intelligent circuit between both the physical and information worlds. Though the field is rapidly expanding to support systems throughout their lifecycle, the initial use cases were mostly focused on virtual reality Technology, Computer Vision, and Immersive experiences. When Michael Storage originally established the concept of standard mode in 1999, he described one of the fundamental pieces in the discipline. The two books that go into great length on CPS are those which go into considerable detail about the 5C Framework, describes how Cyber-Physical Systems and their layers work as transformational technologies for managing network connections and defines CPS in great detail [4].

***Benefits of CPS:***

In fields as wide-ranging as energy, health care, aerospace, emergency relief, industry, automotive, and city management, the skill to design and construct efficient CPS will solve many ambitious priorities of nation. The exploration, compatibility, and compilation of the components required to form these cyber-physical systems will be supported by standard, protocol, and test methodologies, which will support innovation, increase financial viability, and enable technologies to become more resource-efficient. Some of the advantages are mentioned below

***6 Cyber-physical systems -Advances and Applications Rajendran et al.***

**i. Agriculture**

CPS technology, also known as smart agriculture and digital farm, has resulted in advancements that help increase farm efficiency. Smart sensors on tractors or harvesters, as well as drones and satellites, broadcast plant health photos and provide information on soil type and condition

**ii. Smart city management**

### A smart city, according to Tech Target, is "a municipality that employs information and communication technology to boost operating effectiveness, share information to the public, and improve quality of both service delivery and citizen satisfaction. "The utilization of cyber-physical systems technology is essential in smart city design, implementation, and optimization. A smart urban ecosystem is complicated, with systems such as smart traffic control, emergency reaction strategies, and public security solutions integrated.

### iii. Automotive

### IoT and CPS technology have made significant advances in smart car innovations that can end up making vehicular transport services as safe as possible; "blind-spot surveillance, carriageway alerting, and forward automated driving" are just three major features that, if installed in all vehicles in the Country, could decrease the number of collisions and save huge amounts of money each year.

**iv. Safety**

Smart technology has improved security in a variety of ways. CPS technology has enabled smart security to progress and improves, from mobile application development for real-time monitoring systems to fully-fledged smart surveillance systems.

### v. Sustainability

CPS technology is regularly used to push these options, which include public electric transport, low-cost energy storage, accessible solar power, and sustainable recycling activities. More answers to today's enormous need for sustainable practices in the workplace, medical services, and many other fields are being sought by society.

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications* 7**

**vi**. **Health care**

Smart technology development has increased security precautions in numerous ways. As a consequence, cybernetics is the integration of physical, computational, and informational processes. He used analog circuitry and mechanical systems, but his control system was mostly computer-based. Smart security has advanced and improved thanks to CPS technology, from the creation of mobile apps for authentic remote monitoring to fully develop intelligent surveillance systems.

**vii. Infrastructure**

### Smart technology development has increased security precautions in numerous ways. As a consequence, cybernetics is the integration of physical, computational, and communicative processes. Because of CPS technology, smart security has advanced and improved, from the development of a mobile application for an authentic monitoring system to fully developed smart surveillance systems. The country's infrastructure scored a C- on the American Society of Civil Engineers' Report Card for America's Facilities in 2021. Infrastructure improvement begins with technology. The smart infrastructure uses IoT sensors and video recorders, as well as many other cutting-edge digital technologies, to enable smart city initiatives to enhance the experience of people, businesses, and city operators [5].

***Applications of CPS***

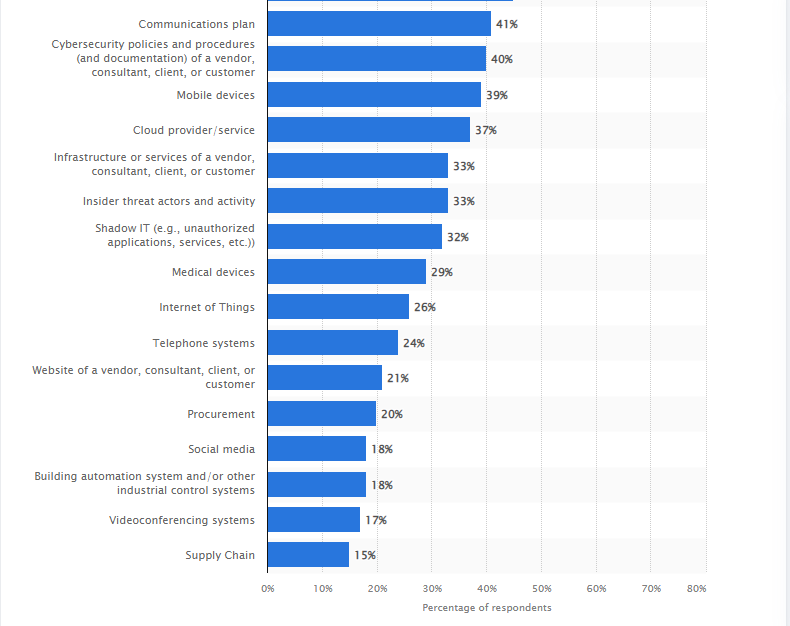
Cyber-physical systems are now widely used in almost every field of science domain. All the systems or devices that can be incorporated with smart technologies find the application of CPS. Some of the domains which have the applications of cyber-physical systems include aerospace engineering, smart architecture, mechanical vehicle and robot manufacturing, implantable medical devices, planes that can fly on their own in controlled airspace, and driverless cars. Figure 1 gives the Share of components of cyber security risk assessments in U.S. healthcare organizations as of 2020.The health care industry is most famous for now widely adapting to the applications of cyber-physical systems. Several innovations like using sensors in the home for detecting health conditions and how they are changing will help give suggestions and recommendations on personalized medical care for the residents. Aeronautic developments include pilot training, aircraft telephony, structure surveillance systems, in-flight diagnostics, in-flight leisure, cordless cab, and flight landing, among many others.

***8 Cyber-physical systems -Advances and Applications Rajendran et al.***

Sustainability is also improved several folds with the use of CPS in environment-related industries. They help detect fires, regulate underwater oil spills, and aid in improved and efficient agricultural practices. By integrating computing, networking, and physical processes the rates of production of goods in the industry can be increased several folds this shall aid in the economy-boosting, which shall be credited to the CPS systems. Old buildings consume 70% of generated electricity and contribute to global warming, which causes climate change. We can realize Zero Net Energy by connecting the Internet of Things, cognition supervision, and controllers. Smart grids are employed in power generation, transmission, and distribution, as well as at the customer level. It will regulate the network connection and also the operational aspects of the electricity generated. CPS monitors and maintains the transmission and distribution networks that connect end users to the smart grid. It will enable two-way control and monitoring between the electricity grid and consumers. Cyber-Physical Systems offer a means to increase the performance of traffic security.

The Cyber-Physical System creates an environment that occurs in both the geographical and the artificial environment, like bridges across rivers, long and large tunnels, high-risk slopes, urban raised bridges, and so on, but also a tremendous range of cars, people, and products in the complicated driving environment. ITS may achieve traffic control by installing many advanced digital equipment and data management to the road traffic system, boosting efficiency, productivity, and safety levels. Traffic management and this information is integrated into the transportation process via CPS, which functions through coordination to make transportation safer. Smart learning spaces can profit from including Cyber-Physical Systems. CPSs can be used in the smart learning to collect adequate information about physical contexts, convert recorded values to experience and ideas, and yield timely and reliable services to students, faculty, and the institution. Smart learning environments will absolutely affect how people learn and work at universities [6].

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications* 9**

****

**Figure 1:** Share of components of cyber security risk assessments in U.S. healthcare organizations as of 2020

**CHALLENGES IN TERMS OF SECURITY IN CPS**

A vulnerability is a flaw in security that can be used for industrial espionage. A vulnerability evaluation determines the necessary preventive and corrective steps to lessen, relieve, or even completely eradicate any risk. Identifying and analyzing the existing CPS issues.

In reality, CPS vulnerabilities fall into three broad categories:

i. **Network Vulnerabilities:** Compromise of insecure wi-fi and cellular connections, and also eavesdropping, probing, replay, spoofing, and

***10 Cyber-physical systems -Advances and Applications Rajendran et al.***

communications, are examples of security flaws. Backdoors in the networks, transportation, and access layer some of them include DoS/DDoS attacks and packet manipulation.

**ii. Platform Vulnerabilities:** These can be found in software, hardware, configuration, and databases.

**iii. Management Vulnerabilities:** Leave out security protocols, regulations, and policies. A variety of events could result in vulnerabilities.

**a) Assumption and Isolation***:* It are based upon that CPS design approach known as "security through obscurity. "Rather than expecting that systems are separated from the outside community, the emphasis, in this case, is on designing a safe and dependable platform while integrating the installation of vital security services.

**b) Increasing Networking***:* As connectivity expands, so does the number of attack surfaces. As CPS facilities have become more interconnected in recent years, producers have enhanced CPS through the adoption and utilization of the wireless site and open wireless communications. Till 2001, the bulk of ICS attacks was carried out internally. That was before the internet's rise, which converted internal attacks into external ones

**c) Diversity**: CPS systems include a variety of third-party parts that are used to create CPS solutions.

**iv. USB Usage:** As with the Stuxnet attack on Iranian power plants, the virus included within the USB is a substantial contributor to CPS flaws. When the malware was plugged in, it was used to replicate and exploit to spread to a large number of devices.

**v. Bad Practice**: This is usually due to poor development practices or a lack of programming skills, which causes the programs to run forever thus becoming too basic for a specific attacker to edit.

**vi. Spying**: The bulk of spying/surveillance attacks on CPS systems employ malware types that attempt to access silently and run for years without detection to collect sensitive data.

**vii. Homogeneity**: can corrupt and change the code, provide hackers with remote access by opening a restricted port or introducing an infected USB/device, inflicting harm or damage to CPS devices

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications 11***

**viii. Suspicious Employees**: can corrupt and change the code, provide hackers with remote access by opening a restricted port or introducing an infected USB/device, inflicting harm or damage to CPS devices.[6]

**CPS IN INDUSTRY**

CPS includes embedded devices that use the internet as a massive network. Cyber-physical systems are now being used to make processes smarter, simpler, faster, and more efficient in all segments of society, like engineering, medicine, transportation, and business. Industry 4.0 is a new German technology that largely relies on big data and CPS. Industrial, automobile, healthcare, mobile, connectivity, transport, leisure, and electronics can all benefit from Industry 4.0. Industry 4.0, a CPS and cloud programming technology, focuses on data interchange with every link within the value chain of the industry. It accelerates the process of setting up due to the experience and understanding high-tech approach it employs and the idea that manufacturing complication is reduced [7].

Business technology and big data 4.0 is largely concerned with data exchange from across the entire industry value chain and are associated with cloud technology and CPS. It allows for the faster establishment of a new firm's production due to its experience and understanding, high-tech approach, and reduced manufacturing complexity. Individuals, things, and systems will be linked by the platforms' services and applications. Cyber-physical systems are critical in industrial production for meeting customer needs. Production processes can be improved, altering the environmental balance sheet. Future products should have a standardized network adapter that plays a major role in data sharing, as well as a distinct character and remembering by birth for recognizing and managing the product [8].

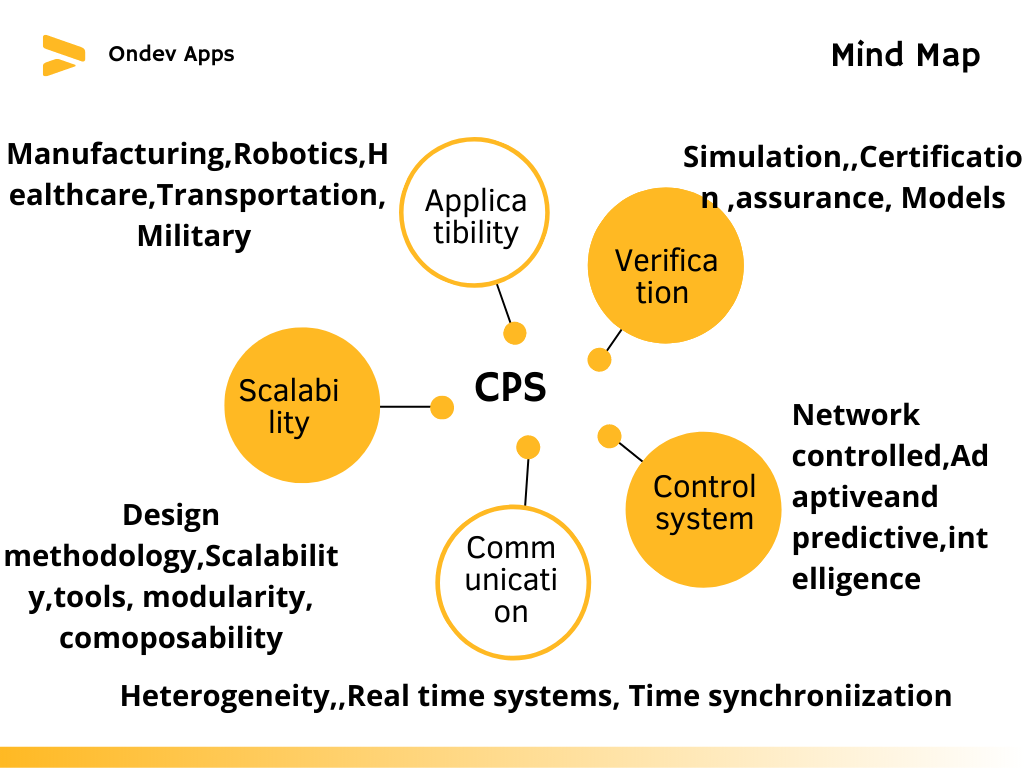
Because traditional data analysis has evolved for such analysis of large amounts of information, the volume of data has grown from unorganized to structure to carry out tedious scheduling activities. To carry out manufacturing activities such as clouding, connecting, and monitoring lower and upper controlling stations synced into complicated shop floor scheduling, a smart economy has been suggested. As a result, computer systems, material-handling devices, commodities, and framesets, as well as their automation deployment and customizable coordination among smart objects, have been produced.

***12 Cyber-physical systems -Advances and Applications Rajendran et al.***

The depiction of the 5C systematic architecture is beneficial to the growth of industrial data analytics with the integration of CPS in the manufacturing company in the creation of smart devices and smart workstations. The idea of multiple data capture is offered for the digital twinning of industrial processes.

This enables the framing of digital twins and multiple terminals with task execution optimization to avoid data gathering delays. This enables the development of smart manufacturing infrastructure. As a result, more will be added to the big data environment to generate dynamic information from data. Developing technologies have embraced the IoT, decision analytics, and industry 4.0 decision-making approaches to boost production efficiency in more controlled and plentiful ways. An enterprise CPS for the development of computational paradigm has been offered to support the incorporation of programmed machine learning methods into industrial processes and improve the exploitation of Industries 4.0. Following this in the design phase will be data privacy, data integrity, consistency of data, and data decentralization [9].

**CPS Management System**



**Figure 2:** CPS integrated production and management systems [10]

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications 13***

The cyber-physical management system is a combination of both cyber and physical systems it has different types of operational methods. Giving the system clear instructions is the best way to guarantee that an operation is completed to the intended level. The three categories of these models are passive, autonomic, and active. These models are made up of the processing, monitoring, physical element, cyber element. In particular, actuation in the active model is direct, whereas actuation in the autonomic model is indirect. The cyber-physical systems, also known as smart factories or smart manufacturing, are what this new technology uses to link the virtual and real worlds as shown in Figure 2. [10].

***Types of Threats***

The most common types of cyber-physical attacks can be summarized as follows [11]

**i. Zero Attacks**

Zero-day attacks aim to exploit a security flaw that has not been made public. Likely, only a select few people who have managed to identify such a weakness have been aware of it because the existence of such a weakness has not been made public.

**ii. Attacks on Spying**

Attackers can illegally get sensitive data through eavesdropping on communication lines used by persons or organizations to transmit such essential information.

**iii. Denial of Service attacks**

Attacks known as denial of service (DoS) attempt to shut down the targeted systems by limiting their access to any kind of computational resources, hence transferring control of the system’s-controlled process to the attacker.

**iv. Data Injection attacks**

Control system networks that are not protected by effective authentication procedures are subject to false data injection attacks that introduce malicious code and commands.

***14 Cyber-physical systems -Advances and Applications Rajendran et al.***

**v. Replay attacks**

An authenticated data packet that has been altered with malicious instructions can be retransmitted, even though authentication measures can assist stop targeted equipment from executing damaging commands.

**vi. Side-Channel Assaults:**

Unauthorized data capture via data leakage in manufacturing machinery is a distinguishing feature of side-channel attacks. An attacker, for example, can collect useful knowledge about how a system works by analyzing variations in power utilization while processing data. It addresses five types of threats (criminal, financial, political, private, and structural) and how each one impacts the cause,

targeted, purpose, vector, and outcome in five different ways. Other malware attacks are described in this section [12].

**SYSTEM MODELLING OF CPS**

A CPS can be modeled as a hybrid system in which computations are defined using state machines, dataflow models, and synchronous and DE models, while physical processes are represented as continuous-time models of dynamics. Solvers for continuous-time models use numerical approximations of differential equation solutions.[13]

A system model is critical in building system control theory on CPS because of its capacity to reflect the dynamic behavior of a CPS. A CPS under attack, per the literature, can be described as one of two types of systems: time-driven or event-driven. In CPS modeling, time-driven systems, which encompass consistent and distinct systems, have garnered a lot of attention. We note that the LTI system is the most extensively used model for both.

Consider a discrete-time LTI as an example.



 **(1)**

** **(2)**

 represents the state of the system, process noise, system measurement, and measurement noise at time, respectively. Furthermore, and  are covariant

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications 1*5**

uncorrelated zero-mean Gaussian noises. and , respectively. A variety of threat models have been developed based on such models. A fundamental concept

for describing availability attacks. Let  represent the threat signal or strength. andbe the attacking forces' decision at moment . An availability attack is defined as

= **(3)****

The sensor-measured values or controlling devices are the targets of integrity attacks. If we consider  to be an entry point, the best measure under attacks is

, where A similar model, i.e., where and are input when attacks are happening or not respectively [14].

**CPS SECURITY REQUIREMENTS**

CPS must possess the resilience to withstand mishaps and harmful assaults. Therefore, from a security perspective, Systems within CPS, both logical and physical, are susceptible to cyber security issues.

**1. Privacy:** The majority of individuals are unaware that CPS constantly engages in a massive data collection procedure. As a result, each individual has the opportunity to examine his or her own data, as well as the chance to ensure what kind of information is being gathered from them by data providers and for whom it is being shared or sold. Nevertheless, doing so also necessitates stopping illegal access to the client's personal information dissemination.

**2.Dependability:** The Intelligent Physical World ensures that the CPS adaptive behavior is obtained to give greater dependability and ensure the right Quality of Service by swiftly adopting fault-tolerance mechanisms (QoS) [15].

**3.Durability:** To withstand mishaps and harmful assaults, CPS must possess resilience. Each CPS element in the Base Architecture, in which each

***16 Cyber-physical systems -Advances and Applications Rajendran et al.***

communicative and wired network path between components is given access to BA's connectors from a security perspective, achieves resilience.

**4.Interaction and Coordination:** To keep the CPS secure at all times, interaction and coordination are crucial. The methods rely on "cyberizing" the physical by incorporating cyber-properties and connections into real system and "physicalizing" the cyber which entails representing real-time cyber-software components.

**5.Operational Security:** Its main responsibility is to ensure operational efficacy by preventing any opponent from accessing public or private information; as a result, it is in charge of monitoring information and detectable behaviors regarding a specific cyber-physical system, especially in hostile circumstances.

**6.System Hardening: A** larger spectrum of risks can be protected against by system hardening. To increase the IoCPT and CPT security, it is therefore strongly advised to separate important applications of any OS that cannot be trusted, and lacks the required security protections. Its main job is to protect a given cyber-physical system's operational efficacy by preventing any adversary from accessing sensitive information. This is incredibly significant in hostile circumstances and locations. Therefore, in order to raise the security level, it is crucial to create the appropriate privileges (role-based, task-based, rule-based, etc.) and strict password complexity restrictions. To lessen the risk of distant wireless attacks, this also entails closing any open ports and removing any outdated accounts.

**VARIOUS APPROACHES OF CPS SECURITY**

**Binary hypothesis and Bayesian detection:**

In deception attacks on sensor networks, one popular detection technique uses a hypothesis test with the prior probabilities of two hypotheses. Byzantine attacks, which increase the possibility of inaccurate sensor output when the fusion center is subjected to misleading data, are taken into account in the estimation of the cooperative spectrum sensing performance limit. A simple regression analyzer based mostly on binary supposition is presented to come to terms with the predicted restricted error in detector network data for smart grid security.

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications* 17**

An analyzer based on an augmented probability value revealed to hued Probability distribution noises under misleading information violent attacks is presented including both observable and non - observable conditions in SCADA systems [16].

**Weighted least square approaches:**

For measurement data, a weighted least-squares (WLS) technique provides an effective and reliable assault detection tool. As a result, it's widely employed, especially in network and power systems. It can ascertain whether a poor assessment occurs by comparing the constructed measure residual to a predetermined threshold.

Consider the following linear system:

 were,  **(4)**

When, the measurement's entire column ranked Jacobian matrix can be determined, where and  are indeed the measuring and state vectors, accordingly, and e is the disturbance influencing the measurement. The estimation problem's goal is to get the estimate of a variable  that correlates most accurately to the meter readings  regarding equation. The remnant is described as the variation between the predicted observations  and the actual measurements.

**(5)**

The WLS set of criteria challenge attempts to find an approximation of that minimizes the performance index. , which is established by the formula below [16].

**(6)**

**DoS Attack strategies:**

Attacks called denial-of-service (DoS) are regularly used to dominate channels of communication to prevent the delivery of measuring and/or control data and to

***18 Cyber-physical systems -Advances and Applications Rajendran et al.***

noticeably impair system performance. The most hazardous DoS attack, often known as a planned assault or dispersed DoS (DDoS), makes use of numerous

infected workstations to execute it. DDoS attacks are extremely frequent since they are straightforward, inexpensive, and have severe negative impacts on systems, including the capacity to entirely cut off an organization. It has been demonstrated that this assault may lead to power system instability and that NCS packets may jitter with a significant delay [17].

**Deception Attack strategies:**

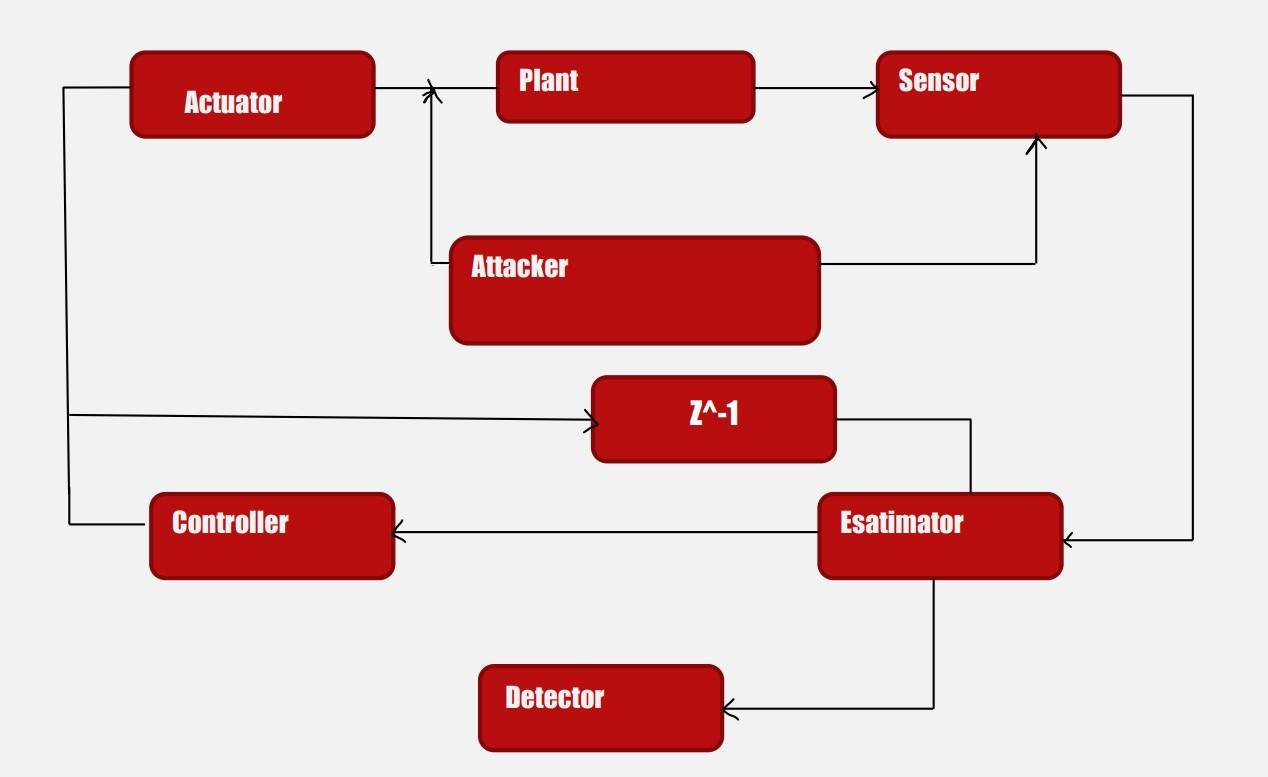
The alteration of the data security for transmissions among particular cyber parts of a CPS is referred to as a deception attack. Other names for it include malicious attacks and fake data injection assaults. To give an example, the very well-known computer virus Stuxnet can alter the code that is running in PLCs through SCADA systems resulting in a deviation from the expectation. Another example is seen in

the power grid's transmission systems, where attackers might start attacks by hacking RTUs that are comparable to the sensors found in substations. A hierarchically oriented attack that included multiple attacks with various cyber levels and goals was used to show this type of attack.

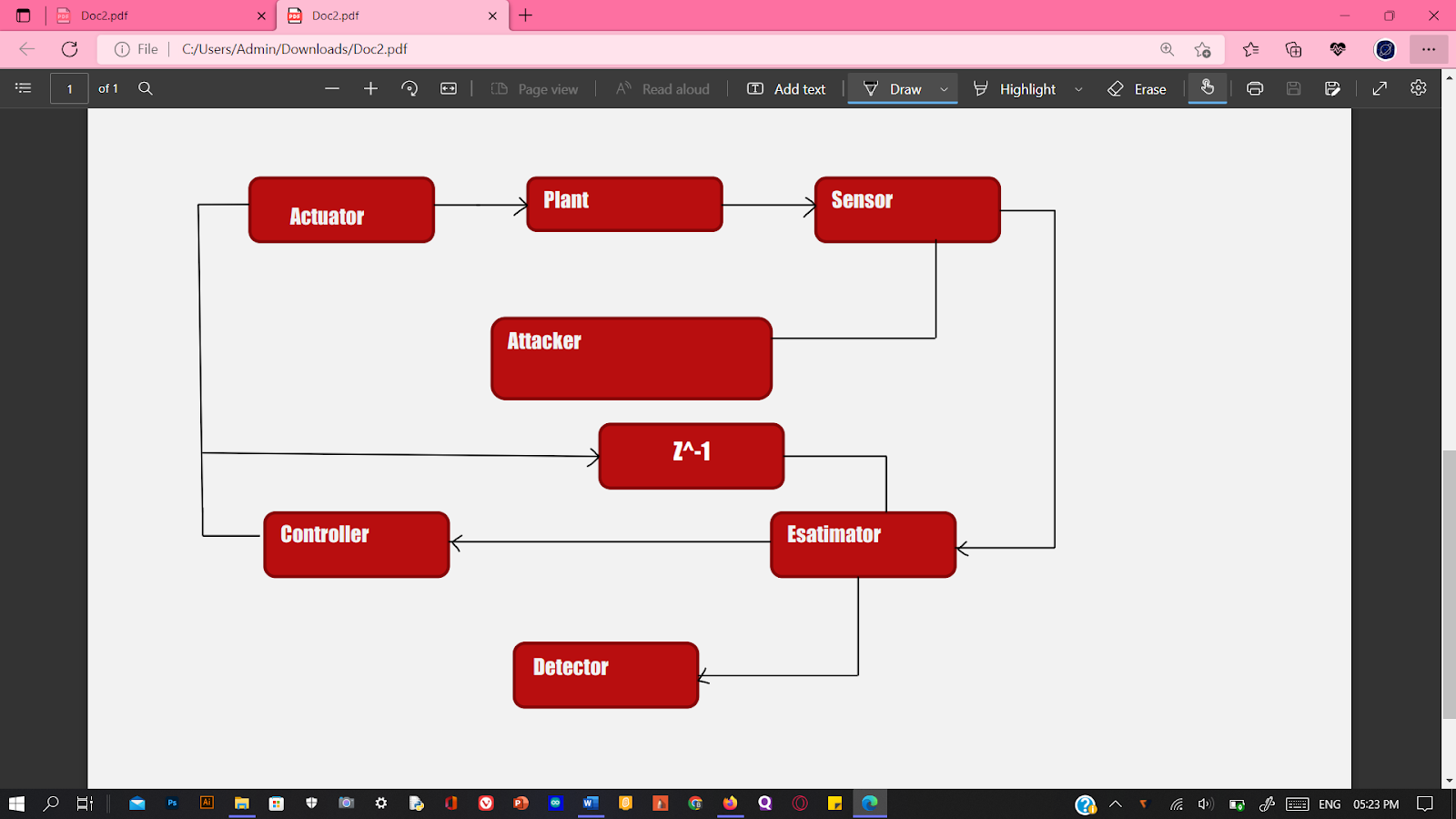
**Replay Attack strategies:**

Replay assaults, a particular kind of deception attack, take place when the opponent is effective in intercepting parts of the data transmission, like sensing data and injecting it into the CPS. The attacker is believed to collect information from the system in the first step of such an attack, and then insert this information into the network (Figure 3) and in the second phase, (Fig 4) which may be directed at the physical process. In some of the popular wormhole topologies used in wireless sensor networks, the attacker can, for example, create a communication link between two endpoints and inject replay messages.

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications* 19**

****

**Figure 3:** First stage of replay attack [16]

****

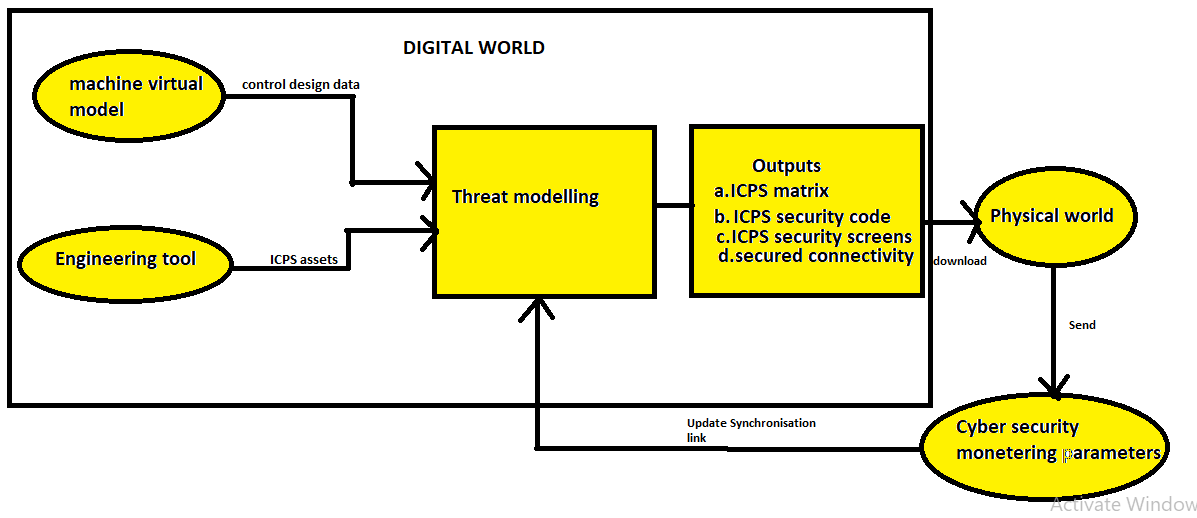
**Figure 4:** Second stage of replay attack [16]

***20 Cyber-physical systems -Advances and Applications Rajendran et al.***

**DIFFERENT ALGORITHMS FOR CPS SECURITY**

**Algorithm For Threat Modeling Approach**

The methodology suggests a final threat modeling that results in a thorough framework that takes the complete ICPS lifetime into account.





**Figure 5:** The Methodology for threat modeling approach [18**]**

The first stage, "Asset Scoping," defines the ICPS target assets as mentioned in outputs of digital world in Figure 5; this is a crucial step because the end goal is to defend these assets against cyberattacks. Assets scoping can be done manually by removing the targeted assets from the engineering drawings and ICPS system architecture, or programmatically by incorporating the resources from engineering tools. Assets are classified based on the Purdue Model to reflect asset values in both situations.

By analyzing threat actors' TTP with the use of ICS ATT&CK, Step 2's "Attack Models" tries to create potential attack situations for scoped assets. This stage results in a collection of assault trees that describe every scenario in which ICPS assets might be attacked.

Attack vector & attack likelihood are measured for each modeled attack in step three under the heading "Attack Vector (AV) versus Attack Likelihood (AL)".

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications 21***

Threat actors use AV as their window of opportunity to launch a cyberattack. Based on data model characteristics, AV relies on threat actor capabilities and

resources, vulnerabilities related to target resources, capital appreciation, attack detection and impact, and asset-related flaws. AL determines if the modeled attacks have ever been carried out on an ICPS-related industry sector or whether they are likely to occur in the future. This step's outcome gauges the characteristics of the modeled attacks.

The goal of Step 4 "Risk Matrix Definition" is to create a matrix listing all hazards associated with the attacks being modeled. The zoomed ICPS resources, assaults modeled, AV & AL numbers, security threats, risk levels, their severity, and mitigating controls are all displayed in the risk matrix.

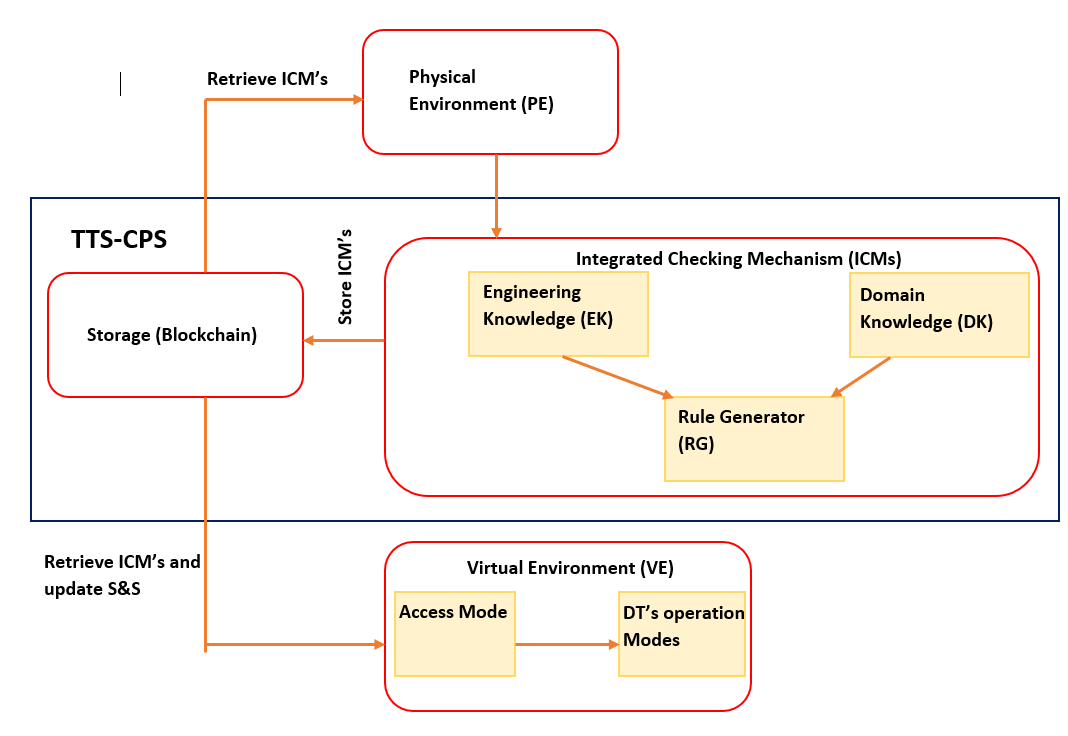
The threat modeling process ends with step 5, "Mitigation Controls," when each identified risk is addressed. Technical and managerial controls are the two types of mitigation controls that are suggested. For this reason, a library of mitigation controls is created to offer potential risk-reduction strategies that may be put into practice [18].

**Digital Twinning Algorithm**

The design of the Trusted Twins for Securing Cyber-Physical Systems DT framework is based on block chain technology (TTS-CPS). The TTS-CPS framework is first introduced in its overall form. After that, we go to great length about the TTS-primary CPS's elements, including comparisons with existing frameworks, digital-physical mapping, and block chain-based DTs.

***Overview of the proposed framework:***

***22 Cyber-physical systems -Advances and Applications Rajendran et al.***

**Figure 6:** CPS security framework using Digital Twinning [19]



The Physical Environment is the first to depict the physical process (PE). Second, the twinned process is explained using a virtual environment (VE). Finally, the layer connects the physical and virtual environments through behavioral data. The behavioral data can be static (like the sensor information) or accommodative (like real-time sensor information). The specification-based artifacts provide process knowledge to the Decision tree. Fourth, depending on data from frequent trials and user-specified criteria, the storage layer maintains the data in the knowledge base and makes it accessible to subsequent layers.

We use the governed, supportive virtual environment as a portion of our regular responsibilities as information analysts when trying to replicate (usually record and

recapping happenings and designed to simulate (trial and error) methods, as well as (ii) detecting deviations from a predetermined or learned benchmark to alert systems. We use DTs as just an exceptional case detection method in addition to other safety applications such as vulnerability scanners, incident management, and automated security. To be more specific, the goal of DT is to find discrepancies

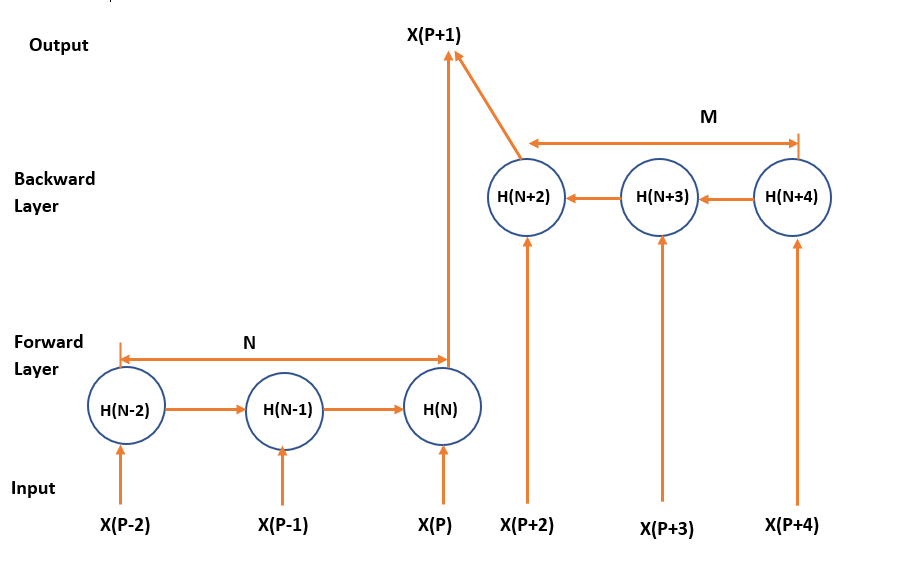
***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications* 23**

between PE and VE. Storage of data, PE and VE, and ICMs are three of the framework's most important elements (block chain-based DTs). Additional to the

implicit S&S requirements, the ICMs provide design requirements of the CPS required to construct the configuration settings of the virtual environment as shown in Figure 6.

The simulation results, reproduction, and data analytics modes of the DT are used for CPS event surveillance, action recognition, and replay. The block chain network ensures secure data management by information retrieval or events. The suggested TTS-CPS framework is compared to other approaches that are pertinent to our field of interest in the sections that follow, specifically leveraging specification-based knowledge of the process for DTs and securing CPS [19].

**Bidirectional RNN-Based Network Anomalous Attack Detection for Cyber-Physical Systems with 1-Based Power System Security Algorithm**

****

**Figure 7:** BRNN based attack detection system [20]

Even though advanced cyber-attacks such as Crashoverride as well as TRITON targeted CPS, few network-based intrusion detection solutions have been used in CPS situations. Korea Electric Power Corporate entity, Korea Alternative Energy Evaluation as well as Making plans, and Korea Power Exchange collaborated on the study. CPS managers from many industrial automation and grids conducted a poll, and they noted that intrusion prevention technology is not used for CPS due

***24 Cyber-physical systems -Advances and Applications Rajendran et al.***

to repeated false positives and difficulty in understanding the sensing data. A rate of false regularity of 0.1 percent, for example, indicates exceptionally high accuracy. On the other hand, a huge CPS network can give millions of packets every day, while a general-sized CPS network could send at least 100,000. Although if 100,000 packets are sent, with a false alarm rate of 0.1 %, 100 false alarms occur daily.

Security administrators' understanding of threats may be reduced by the prevalence of false positives. In the TRITON case, it appears that at least two intrusion detection alarms were disregarded, which allowed hackers to successfully install malware.

However, this same difficulty in analyzing detection data limits progress in reducing false positives. The detection findings are generated at a black box level by the methodologies of the detection techniques used in previous studies. It is not suggested how to perceive the detection results. As a result, determining whether an abnormal behavior discovered as a sensing consequence is a truthful identification of unusual behavior or untrue sensing for a typical practice may be difficult. This makes it hard to use and limits the ability to produce superior detection results.

The development of graph-based automata is one approach to tackling this problem that enables quick visual inspection of the result values as compared to analysis just at the black box level. One strategy for solving this issue that permits quick visual evaluation of the result values as compared to research at the black box level is the construction of graph-based automata. The practical implementation shows that the automata-based detection method only performs identification once, which is an issue. In the automata, for instance, If the ground has been required to determine whether the prospective abnormality selection would be put in place as a 4-statement following a normal 3 state or as a 1 state again following a normal 4 state (1234). The ground must assess if a package of a kind signifying 5 after 123 has been transmitted and judged to be abnormal if the following abnormality determination would still be carried out as a 1 state once one 4 states have been reached. Particularly, common network traffic trends longer than 100 are shown by

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications 2*5**

the data used to validate the suggested technique. According to analysis, the time required for the system to return to normal operation after anomalous behavior varies. As a result, we chose an RNN algorithm that, after abnormal behavior

occurs, can predict the next abnormality by comprehending the pattern of data input. A helpful model for finding patterns in a set of input data is the RNN stack.

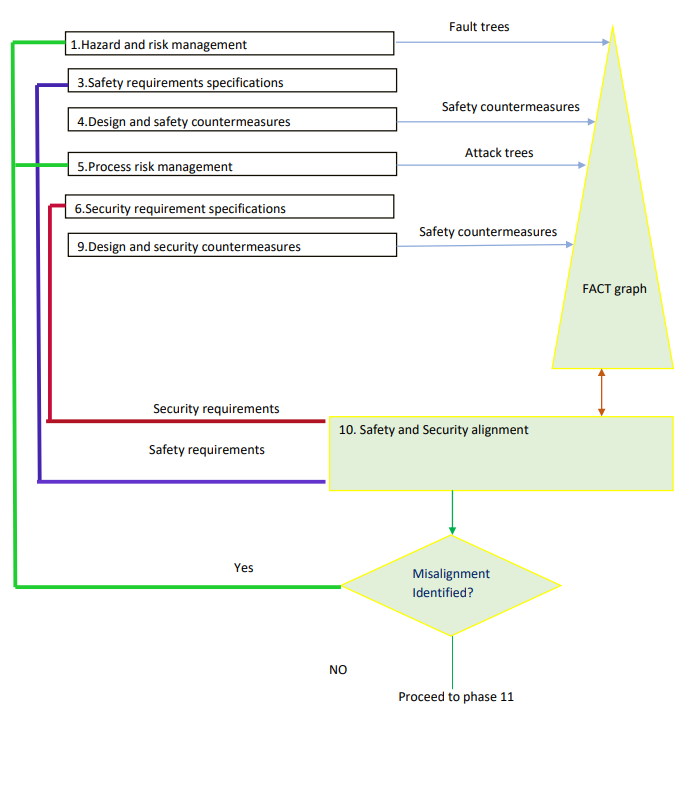
The broad "many to many" RNN model isn't appropriate because it generates all of the following prediction data for every input over a series of inputs to measure accuracy. Therefore, we use a "many to one" RNN model that can only predict one future event. details on projections for different inputs. However, the results of our a priori analysis showed that the linear RNN model had been unable to forecast unusual data. Consider two instructions, the first of which has a cycle of five seconds and the second of which has a period of 5 minutes. For greater accuracy in this situation, the linear RNN model tends to anticipate just 5-s periodic instructions and disregard 5-min periodic commands. This study uses a "many to one" bilateral RNN structure as a result.

Contrarily, conventional "many to one" bidirectional RNNs use (P+1) th to (P+q) th input as the backward layer to forecast the (P+1) th input, and P series input as the forward layer. The (P+1) th input significantly increased the weight of the backward layer, making it difficult to carry out the required training. We recommend a novel many-to-one bidirectional RNN as a consequence. Given M traffic patterns, this structure produces the (P+1) th prediction data. The M data from the (P+2) data are then used to correct the (P+1) th prediction data as shown in Figure 6. A model with a smaller M is more effective for real-time detection since M data are also used to identify improper behavior in the corrective delay [20].

**Alignment of CPS Security and Safety Using Failure Graph of Attack-Countermeasure (FACT)**

The FACT graph is formed as a result of stages 1 through 9 of a combined protection and stability lifecycle process. Only a few of the artifacts from these stages are used as resources for the Fact graph. Security protocols, safety regulations, and the FACT graph are also inputs for the analysis of protection and stability alignment. The FACT graph is built in four steps, as shown in Figure.8. The steps are as follows:

***26 Cyber-physical systems -Advances and Applications Rajendran et al.***

**Figure 8:** FACT graph [21]

**Step 1:** After the safety risk identification and risk analysis, fault trees are shipped to begin going to generate the graph (phase 1). Interconnected fault trees have been linked using AND or OR gates whenever possible to provide a comprehensive view of potential system faults. These fault trees are located all around the FACT graph.

**Step 2:** Once the safety measures have been described and designed, they are added to a FACT graph (phase 4).

They have had an emotional stake in the catastrophes they are trying to avoid.

This mapping enables us to see how safety remedies have addressed flaws in safety.

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications 27***

**Step 3:** The FACT graph is updated to attack trees established during the procedure risk assessment's fifth section. Attacks linked to FACT graph failures are linked to

security flaws. The OR gate manages to combine assault trees into fault trees, indicating that rejection can be prompted by either accidental or intentional failures. Security preventative measures are added to the FACT graph after the protective prevention and mitigation design method (phase 9) is completed.

**Step 4:** We can now apply the FACT approach, which allows us to connect protective measures to any danger tree node. The FACT graph, which was built during phases 1-4, is a holistic system safety and defense model that shows safety and stability relationships between objects. It could be used to perform security and protection alignment evaluations (phase 10). Safety analysts must collaborate with security analysts during this phase to identify any mismatches, duplication, as well as missing components.

To achieve this goal, the integrative lifecycle's phase [iii] safety regulations and phase 6 security requirements are combined [21].

The FACT graph is evaluated and discussed to the protection and safety conditions in phase 10 to determine if the needs are met, i.e., whether the suggested quality and security FACT graph can also be used in subsequent CPS development and maintenance phases, such as phases 11 and 13 for software oversight and evaluation, as well as security and safety verification and validation. To determine whether the existing countermeasure set is adequate for safeguarding CPS, newly discovered failures and attacks should be included in the FACT graph. To determine whether the current preventative measure set is adequate for safeguarding CPS, newly discovered failures and threats that were consistently reported will be included in the FACT graph [22].

**FUTURE ASPECTS OF IMPROVEMENT**

 Keeping in mind the key challenges in CPS with track of the current advancement of technology, CPS technologies and applications have following areas of improvements:

**Upkeep of Security Services**: To safeguard CPS in authentic processes while needing the lowest amount of processor complexity, new lightweight

***28 Cyber-physical systems -Advances and Applications Rajendran et al***

***.***

cryptographic techniques are necessary. The mentioned security services can be supported by these cryptographic solutions:

**ii. Confidentiality**: To secure real-time communications using CPS resources, a special type of light block or stream cipher algorithms is required. Early this year, a completely fresh strategy was introduced. It is founded on the key generation cipher structure and only needs two or one repetitions. At the physical layer, a mix of these approaches can be used.

**iii. Integrity of Message/Device:** This refers to preventing logical or physical alterations to CPS data and devices (s). This can be accomplished by ensuring that the apps, and software are safely signed, error-free, and equipped with powerful cryptography.

**iv. Device and data accessibility**: To recover quickly from various types of availability attacks, computing resources, substantiated backup, as well as a self-healing capability of CPS, are required. Furthermore, it is crucial to maintain data access, and one approach to do this is by designing a multi-secure connection.

**v. Authentication of Devices and Users:** To enable non-repudiation, increased accountability, and improved identification and verification processes due to these unique access-control privileges, a powerful hardware mutual multi-factor authentication mechanism is required (least-privilege).

**vi. Digital Evidence Protection:** This is important since the majority of sophisticated attacks, including those launched by viruses like Shamoon, Duqu, Flame, and Stuxnet, focus on eliminating any trace that can be used to pinpoint the attack's origin. New defenses for maintaining digital forensics records should be offered by contemporary digital forensics technologies.

**vii. Improving Security Policy:** Insiders were regularly involved in CPS attacks (on purpose or by accident). Therefore, before being employed, all employees must undergo a screening process, have their privileges revoked outside of work hours, and also have their behavior scrutinized for advanced responsibilities. This suggests that new regulations be added to the CPS security strategy to limit access and reduce the likelihood of harm.

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications* 29**

viii. **Intelligent collaborative effort with non-cryptographic solutions:** To function properly, intrusion detection systems (ids should be synergistic in every manner and incorporated with a firewall as well as adaptive honeypot systems.

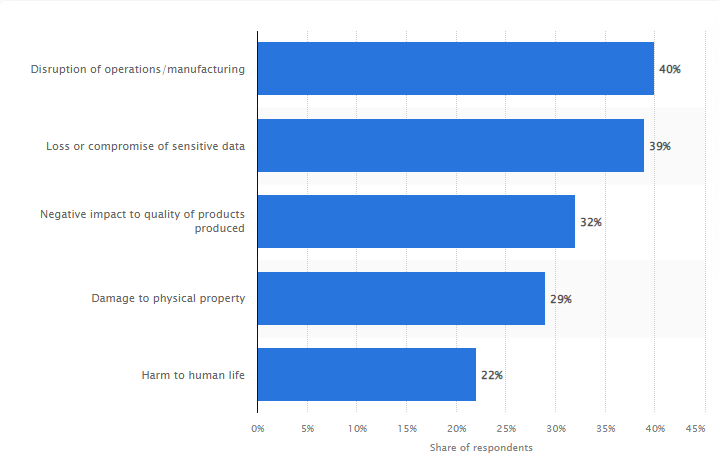
ix. **Compliance Enforcement:** When analyzing CPS's big data through the cloud, particularly when the data is kept by utility companies (Trusted Third Party (TTP)), it is possible to protect user privacy and maintain compliance with data access regulatory standards. Maintaining a proper balance between system security and functionality, user privacy, and the security and features of systems, as well as setting more stringent accountability criteria.

x. **Obtaining a Trade-Off:** is crucial for preserving the availability, security, and safety of systems. These three fundamental elements must be merged while taking into consideration the existing budget and financial needs for risk assessment in order to accomplish such a trade-off.

xi. **Availability**: Because their availability is crucial for all authentic CPS operations, protecting them is a top responsibility. As a result, a compromise must be made between security and availability (such as protection from efforts at wireless jamming) (Signal-to-Noise Ratio, Frequency Hopping/Shifting, Backup Devices, Firewalls, Traffic Monitoring, etc.).

xii. **Safety and Security:** Even if a CPS is secure, its safety cannot be guaranteed. In fact, to maintain both security and safety in any CPS domain, a compromise must be made, with a security measure (Firewalls, Artificial Intelligence (AI), etc.) assuring defense against intentional cyber-physical attacks, and a safety feature designed to protect the CPS from every accidental failure or dangers (system failure, abnormal activities, miscalculations, etc.) .

***30 Cyber-physical systems -Advances and Applications Rajendran et al.***



**Figure 9:** Anticipated results of successful cyber-attack against automation and/or robotics systems worldwide as of 2017

**CONCLUSION**

By merging the physical and digital worlds, CPS systems—essential elements of Industry 4.0—are already altering how people engage with the former. The objectives of installing CPS systems, whether utilized within or out of the IoT, are to increase system availability and reliability as well as product quality. The dependability, safety, and effectiveness of CPS systems could be impacted, and there are a variety of privacy and security issues that could prohibit their broad usage. This chapter initially provides an overview of all the elements that make up CPS systems and how they communicate with one another, including IoT systems. Its next focuses on the primary security concerns, vulnerabilities, and attacks that pertain to these elements and the communication protocols that are in use. Then, an

***Advances and Applications in Cyber Security Cyber-physical systems: Advances and Applications* 31**

insight about and evaluate the most recent CPS security options, which fall into two categories: cryptographic and non-cryptographic options. To create resilient and safe CPS systems while preserving necessary performance and reliability, we offer suggestions and guidance on the many security features, applications, and best

practices that should be adopted. Then, we emphasize the key takeaways from the entire experience.

**ABBREVIATIONS**

CPS - cyber-physical system

IoT - Internet of Things

AI -Artificial Intelligence

TTP - Trusted Third Party

FACT -Failure Graph of Attack-Countermeasure

RNN - Recurrent Neural Network

DT - Decision tree

PE -Physical Environment

VE - Virtual Environment

ICM - Integrated Checking Mechanism

TTS-CPS -Trusted Twins for Securing Cyber-Physical Systems

**REFERENCES**

[1] A Afrizal, B Mulyanti and I Widiaty,” Development of Cyber\_Physical System (CPS) implementation in industry 4.0”,*IOP Conference Series: Materials Science and Engineering* ,2020.

[2] Amit Kumar Tyagi, N. Sreenath, “Cyber Physical Systems: Analyses, challenges and possible solutions”, *ScienceDirect* ,2021

[3] Edward A. Lee, Albert M. K. Cheng,” The Past, Present and Future of Cyber-Physical Systems: A Focus on Models”, *Sensors* ,2015

[4] Kyoung-Dae Kim, P. R. Kumar, “Cyber–Physical Systems: A Perspective at the Centennial”, *IEEE* ,03 April 2012

[5] *Vanderbilt Engineering Graduate Admissions Team*, “What are the Impacts and Benefits of Cyber-physical Systems?”, May 18 2022

[6] Jean-Paul A. Yaacouba, Ola Salmanb, Hassan N. Nouraa, Nesrine Kaanichec, Ali Chehabb, Mohamad Malli,” Cyber-physical systems security: Limitations, issues and future trends”, *Elsevier*,2020

[7] Seungmin Rhoa, Athanasios V. Vasilakos b, Weifeng Chenc,” Cyber physical systems technologies and applications”, *Elsevier*, 2016

***32 Cyber-physical systems -Advances and Applications Rajendran et al.***

[8] Magdi S. Mahmouda, Mutaz M. Hamdana, Uthman A. Barudib, “Modeling and control of Cyber-Physical Systems subject to cyber attacks: A Survey of recent advances and challenges”, *Elsevie*r,21 April 2019

[9] Lidong Wanga, Guanghui Wangb,” Big Data in Cyber-Physical Systems, Digital Manufacturing and Industry 4.0*”, I.J. Engineering and Manufacturing*, 2016, July 2016

[10] Harpreet Singh,” Big data, industry 4.0 and cyber-physical systems integration: A smart industry context”, *Elsevier* ,9th July 2020

[11] *Konverge Technologies*, Types of cyber physical attacks.

[12] Rasim Alguliyev, YadigarImam verdiyev, Lyudmila Sukhostat,” Cyber-physical systems and their security issues”, *Elsevie*r ,2018

[13] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo,” Cyber-Physical Systems Security – A Survey*”, IEEE Internet of Things Journal PP (99),* January 2017

[14] Wenli Duo, MengChu Zhou, Abdullah Abusorrah, “A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges*”, IEEE*,26th April 2022

[15] Miklós Biró, Atif Mashkoor, Johannes Sametinger, “Safe and secure cyber-physical systems”, *Wiley online library* ,16 March 2021

[16] Caiming Zhang, Xiaojun Xu, Hong Chen, “Theoretical foundations and applications of cyber-physical systems: a literature review”, *Emerald Insights*, 3 January 2020

[17] Dan Zhang, Qing-Guo Wang, Gang Feng Yang Shi Athanasios, V. Vasilakos, “A survey on attack detection, estimation and control of industrial cyber–physical systems*”, Elsevier*,19th January 2021

[18] Mohammad Jbair, Bilal Ahmad, Carsten Maple, Robert Harrison, “Threat modeling for industrial cyber physical systems in the era of smart manufacturing”, *Elsevie*r,17 January 2022

[19] Sabah Suhaila, Saif Ur Rehman Malikb, Raja Jurdakc, Rasheed Hussaind, Raimundas Matulevičiuse, Davor Svetinovica, “Towards situational aware cyber-physical systems: A security-enhancing use case of blockchain-based digital twins”, *Elsevier*, 26 April 2022

[20] Sungmoon Kwon, Hyunguk Yoo, and Taeshik Shon,” IEEE 1815.1-Based Power System Security with Bidirectional RNN-Based Network Anomalous Attack Detection for Cyber-Physical System”, *IEEE,* April 23 2020

[21] Giedre Sabaliauskaite and Aditya P. Mathur,” Aligning Cyber-Physical System Safety and Security”, *Springer*, 2015

[22] GiedreSabaliauskaite, Geok SeeNg, Justin Ruths, Aditya Mathur, “A comprehensive approach, and a case study, for conducting attack detection experiments in Cyber–Physical Systems”, *Elsevier*, December 2017