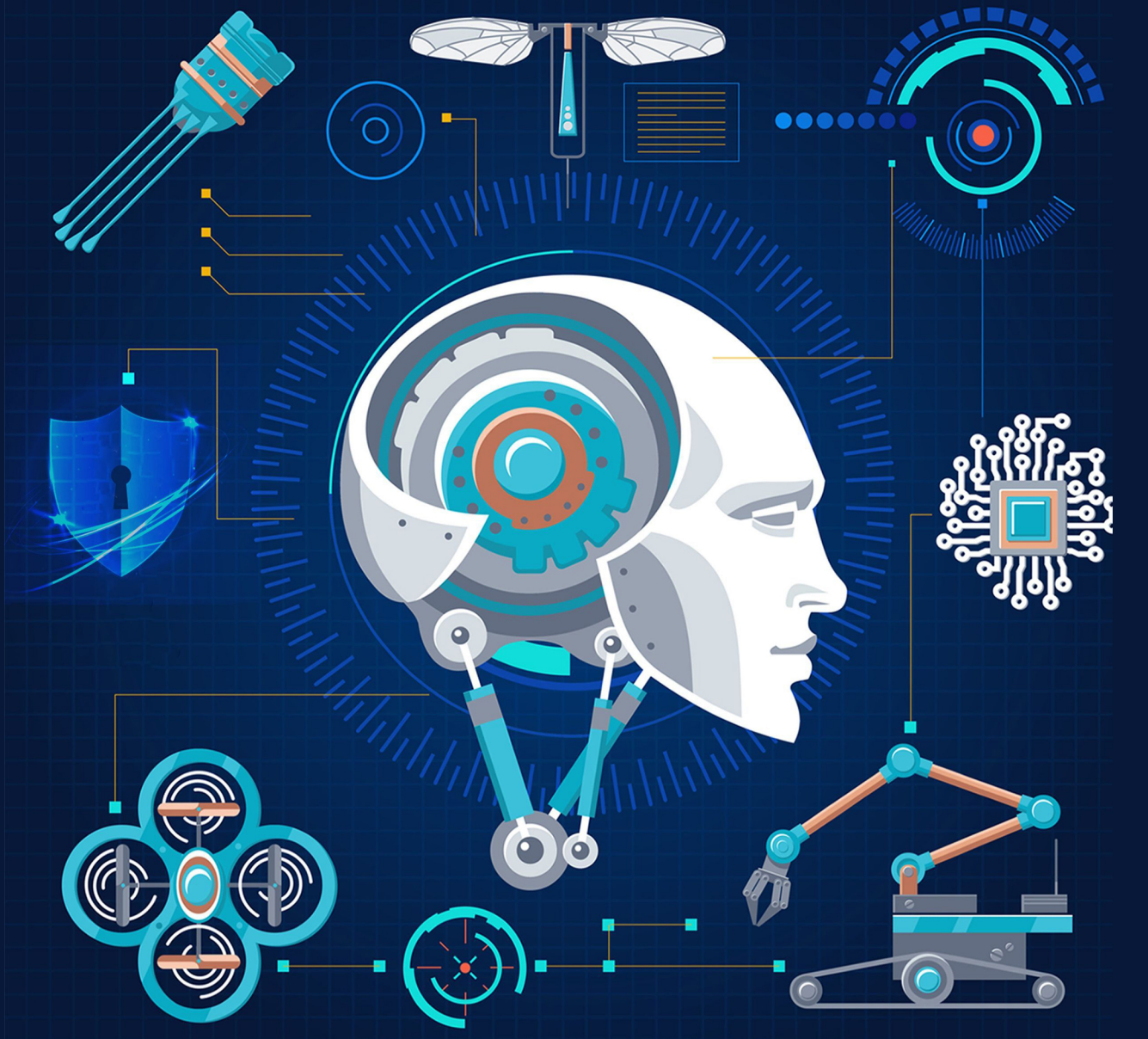
CYBER PHYSICAL SYSTEMS

ADVANCES AND APPLICATIONS



Editors:
Anitha Kumari K.
Avinash Sharma

Bentham Books

Cyber Physical Systems - Advances and Applications

Edited by

Anitha Kumari K.
Department of Information Technology
PSG College of Technology, Coimbatore
TN, India

&

Avinash Sharma
Chandigarh Engineering College, Jhanjeri, Mohali
Punjab 140307, India

Cyber Physical Systems - Advances and Applications

Editors: Anitha Kumari K. and Avinash Sharma

ISBN (Online): 978-981-5223-28-6

ISBN (Print): 978-981-5223-29-3

ISBN (Paperback): 978-981-5223-30-9

First published in 2024.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
80 Robinson Road #02-00
Singapore 068898
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE

This book aims to address the challenges prevailing in Cyber-Physical Systems by providing promising solutions through innovative techniques and thereby safeguarding the digital environment. A computer system that uses computer-based algorithms to control or monitor a mechanism is notoriously known as a Cyber-Physical System (CPS). A broader range of services and applications are available due to the rapid development of CPS in recent years including e-Health, e-Commerce, UAV, game theory, smart grid, and industry automation that influences people's lives in various ways.

The information in this book offers numerous techniques and methods that address various security concerns in the field of automation and cyber-physical world. Precautionary and preventive measures are discussed with organized examples. Analytical approach to Rescue Automation from External Assaults, Analysis of Various Threat Detection and Prevention Techniques in IoT Environment, Security in Smart Grid Cyber-Physical System, Cyber Physical Systems in Clinical Setting, Cyber Physical Systems and Game Theory Integration, Cyber-Physical Systems in HealthCare, Augmented reality in Cyber-Physical System: Challenges and Concerns, Comprehensive Study on Network and Computer Forensic Framework and A Review on Industrial Critical Infrastructure Perspective have all been thoroughly covered. By enabling readers to understand and use Cyber Physical Systems technology in a safe manner in an insecure environment, we the editors think that this book will undoubtedly be useful to academics, researchers, students, and industry professionals.

We would like to sincerely thank our reviewers for their assistance despite their busy schedules. We sincerely appreciate each and every one of our authors for their diligent chapter preparation and on-time submission. We pay a deep sense of gratitude to Bentham Science Publishers from the bottom of our hearts for accepting our proposal to edit this book and for their unwavering support throughout the editing process. We owe a debt of gratitude to everyone who assisted in the successful editing of this book.

We believe that this book creates a good impact and plays a quintessential role in every reader’s life to imagine and develop smart systems for the betterment of the community. This satisfaction will spur us on to create more edited works that will benefit society.

Anitha Kumari K.
Department of Information Technology
PSG College of Technology, Coimbatore
TN, India

&

Avinash Sharma
Chandigarh Engineering College, Jhanjeri, Mohali
Punjab 140307, India

List of Contributors

Avinash Sharma	Chandigarh Engineering College, Jhanjeri, Mohali, Punjab 140307, India
A.S. Rakseda keerthi	PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India
Alaska Tengli	Department of Electronics and Communication, R. V. College of Engineering Bangalore Mysore Rd, RV Vidyaniketan, Karnataka-560059, India
Anitha Kumari K.	Department of Information Technology, PSG College of Technology Coimbatore TN, India
D. Priya	Department of Computer Networking, PSG Polytechnic College, TN, India
Geeta Rani	Department of Computer Science and Engineering APEX, Chandigarh University, Haruan, Punjab, India
L. Latha	Kumaraguru College of Technology, Coimbatore-641022, India
M. Karthigha	Sri Ramakrishna Engineering College, Coimbatore-641022, India
M. Revathy	PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India
P.S. Pavithra	SRM Institute of Science and Technology, Chennai, India
Puninder Kaur	Institute of Engineering and Technology, Chitkara University, Punjab, India
P. Durgadevi	SRM Institute of Science and Technology, Chennai, India
Ramavenkateswaran N.	Department of Electronics and Communication, R. V. College of Engineering Bangalore Mysore Rd, RV Vidyaniketan, Bengaluru, Karnataka-560059, India
R. Madhumathi	Sri Ramakrishna Engineering College, Coimbatore, India
S. Brindha	Department of Computer Networking, PSG Polytechnic College, Coimbatore, India
Sindhu Rajendran	Department of Electronics and Communication, R. V. College of Engineering Bangalore Mysore Rd, RV Vidyaniketan, Bengaluru, Karnataka-560059, India
Shreya S.	Department of Electronics and Communication, R. V. College of Engineering Bangalore Mysore Rd, RV Vidyaniketan, Bengaluru, Karnataka-560059, India
Shilpa S.P.	Department of Electronics and Communication, R. V. College of Engineering Bangalore Mysore Rd, RV Vidyaniketan, Bengaluru, Karnataka-560059, India
Sai Priya L.	Department of Electronics and Communication, R. V. College of Engineering Bangalore Mysore Rd, RV Vidyaniketan, Bengaluru, Karnataka-560059, India
T.P. Kamatchi	Department of Computer Networking, PSG Polytechnic College, TN, India

CHAPTER 1

A Comprehensive Analysis of Various Threat Detection and Prevention Techniques in IoT Environment

P.S. Pavithra[1,*] and **P. Durgadevi**[1]

[1] *SRM Institute of Science and Technology, Chennai, India*

Abstract: The Internet of Things (IoT) has become one of the most widely used technologies in recent times. IoT devices can be enabled to collect, and exchange information in a highly efficient manner *via* the network. A smart object with technology and devices builds a network infrastructure that is used in a variety of areas such as mechanical, building, medical, manufacturing, entertainment, and transport. The major security issues such as confidentiality, authentication, confirmation, security systems, system configuration, data storage, and administration are the main challenges in an IoT environment. To overcome these security issues, various techniques are addressed. Initially software called an Intrusion Detection System (IDS) was used that monitors a network of malicious activity using valuable tools in IoT devices. Then, the machine technique was used to detect the attacks from the intrusion detection system to provide embedded intelligence in IoT devices and networks. Finally, Blockchain (BC) technology is gaining traction in modern IoT devices to address security and privacy challenges to provide reliable communication in an IoT environment. The aim of this work is to provide a detailed review of ML and BC techniques that can be used to develop revamped IoT security devices.

Keywords: Attack, IoT Layers, Protocols, ML Techniques.

1. INTRODUCTION

IoT is a network of sensors and objects that can communicate with one another without human intervention. The “things” in the IoT are hardware objects such as wearable sensors, that detect and collect different types of data about technology and human social activity. The Internet of Things keeps people, objects, devices, and services all interconnected at all times.

[*] **Corresponding author P.S. Pavithra:** SRM Institute of Science and Technology, Chennai, India;
E-mail: pp2616@srmist.edu.in

Anitha Kumari K. & Avinash Sharma (Eds.)

The primary objective of the Internet of Things is to create a broadband network with interrelated communication systems and applications that help physical/virtual sensors, home computers (PCs), digital phones, motorcars, and items such as fridges, washing machines, household appliances, food, and medications to be connected and embedded anywhere at all possible time and on any network. The requirements for large-scale IoT deployment are rapidly growing and eventually pose a serious security issue. Privacy, authorization, authentication, security systems, system configuration, data storage, and monitoring are the primary issues in the IoT environment [1]. IoT devices are linked to complex devices, interact with the environments, and are deployed on a wide range of unmanaged systems. They confront a number of security concerns and challenges. The Internet of Things layer is separated into four layers; its architecture is based on a standard Online communication network, and it is primarily for information transit between IoT devices. In recent years, IDS has shown to be a more reliable and efficient strategy. IDS is a technology that analyses a network for unexpected IoT device performance [2]. IDS can be set up on a single system or on multiple machines in a network. IDS provides several advantages to businesses, including the ability to detect security threats. An IDS (Fig. **1**) can aid in the identification of threat types and numbers. This paper outlines a strategy for developing an IDS that employs Machine Learning (ML) approaches to detect data-based threats in order to defend against attacks in the IoT. The hostile devices carry out attacks, where data is collected in two ways: benign information during normal flow and traffic seized during threats. Machine learning techniques are built using a number of approaches to detect malicious behaviour in an IoT infrastructure. Blockchain is a distributed technology with numerous advantages, including increased security and transparency. As a result, blockchain can spearhead itself be a strong platform for payment and communication apps. Thus by using blockchain as a database to keep records of how things communicate, what state they're in, and how they connect with other IoT systems, blockchain can help to solve the majority of IoT privacy and tracing issues.

The detailed review of this paper is carried out as follows: Section 2 shows the classification of IoT layers and their protocols. Section 3 shows security issues in IoT Layers. Section 4 shows security issues occurring with the use of IDS. Section 5 discusses security issues that occur using ML techniques and Section 6 explains security issues that occur using Blockchain technology.

2. CLASSIFICATION OF IOT LAYERS

The IoT can be divided into four layers namely: Application, Middleware and Sensor Layer, as shown in Fig. (**2**).

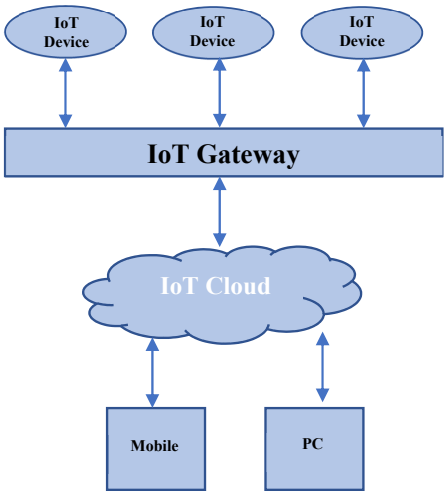


Fig. (1). IoT architecture.

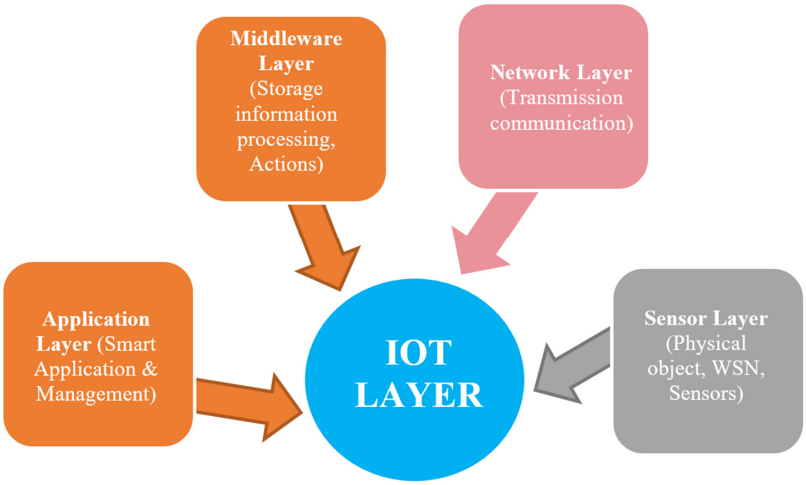


Fig. (2). IoT layers.

2.1. Application Layer

The advantages of IoT in our daily lives are prominent. Security was not a significant design when the IoT was first introduced in the late 1960s since security risks were not properly accommodated. Security has become crucial for the IoT's long-term viability and widespread adoption. IoT applications and sensors have infiltrated every part of our lives [3]. IoT has become a critical component of many healthcare contexts. IoT sensors have made their way into our living environments by paving ways to create smart home which includes Possible sources, led lights, thermostats, and other home equipment are now equipped with

CHAPTER 2

Security Concerns in Smart Grid Cyber-Physical System

S. Brindha[1,*] and **Anitha Kumari K.**[2]

[1] *Department of Computer Networking, PSG Polytechnic College, Coimbatore, India*

[2] *Department of Information Technology, PSG College of Technology, Coimbatore, TN, India*

Abstract: A smart grid cyber physical system (SG-CPS) is an optimal fusion of a power network infrastructure and cyber system based on a communicating network. The SG-CPS employs advanced technologies to deliver energy supply and provide flexible choices for prosumers. The SG-CPS uses multiple components in different units and this has given rise to more complexity in managing them. The reliable operation of any smart grid is necessary to enjoy uninterrupted services. As many smart devices are being used, more cyber-attacks are also targeted on smart grid cyber physical systems. The different types of attacks necessitate a broad security perspective to ensure safe services in the smart grid. The countermeasures for securing the smart grid have to be designed in all layers encompassing the cyber physical power system. If the power system is targeted then all the dependent devices will be at risk. A blackout scenario will cause more damage to industrial and household applications. Emerging technologies like Blockchain, AI, ML and IoT present a promising trend in the smart grid cyber-physical system. By predicting the power demand, supply can be adjusted automatically. Many such power system-related issues have smart solutions. In this chapter, we will first review the security challenges and attacks in the context of smart grid cyber-physical systems. Then the potential vulnerabilities to cyber-attack threats and risks in smart grid cyber-physical systems have been outlined. Finally, countermeasures for the security attack scenarios in SG-CPS are outlined.

Keywords: Cyber-Physical power system, Cyberattacks, Smart grid.

1. INTRODUCTION

In the past few years, advancements in Information and Communications Technology (ICT) systems have shown the strategy for the adoption of the Cyber-Physical System (CPS) for various applications. The cyber physical system is made up of three components namely the physical parts of the system, the data

[*] **Corresponding author S. Brindha:** Department of Computer Networking, PSG Polytechnic College, Coimbatore, India; E-mail: hod.dcn@psgpolytech.ac.in

Anitha Kumari K. & Avinash Sharma (Eds.)

and information-related cyber system and the communication network for the network between the two systems.

CPS is an embedded system, controlled and managed by computer algorithms with communicative network components.

The various components of CPS are the foundation for emerging innovations and automated services in building tools and technologies. The world changed a lot due to the advent of the internet. As a result of the internet, the communication methodologies through which people communicate among themselves changed. As shown in Fig. (**1**), cyber physical systems combine sensors, computing devices, actuators, and communicating networks to connect them to the Internet and to each other. CPS has the capability to reinvent things with more smart components and redesign the world with more responsive, sustainable, and reliable systems.

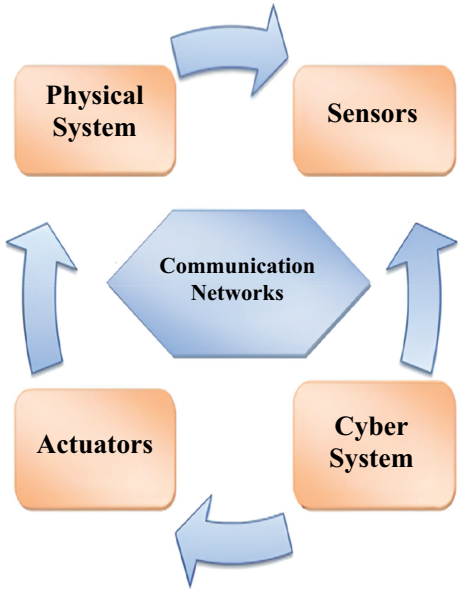


Fig. (1). Cyber physical system.

One of the most application-oriented CPSs is the smart grid CPS (SG-CPS) that aims to provide a power supply to modern-age consumers in a better way. The smart grid is an upcoming technology that has immense potential to cater to the changing demands of the industry with respect to power consumption. Smart Grid enables monitoring, controlling, and managing the power grid in real-time. Cyber-Physical System (CPS) is an upcoming technology that can tackle many challenges in smart grid systems. Smart grids are electric grid networks using

monitoring tools and controlling components to deliver an uninterrupted and reliable power supply. Conventional electrical machines like generators, transformers, and distribution devices have been made smart by attaching the cyber components with them, thereby managing the large physical systems that have been made automatic and easier.

Smart Grids (SGs) are such a boon for smart energy supply and they open the door for a modern and automated use of the electric power supply system. The stakeholders involved in the electric energy supply chain have to collaborate and establish new standards for smart grid energy supply. The main criteria for the deployment of SGs are the flawless combination and interoperability obtained from physical components belonging to the conventional power grids and the latest cyber field components involving computing capabilities. This cyber-physical system integrated with the power system is called a cyber-physical power system (CPPS). Smart systems integration will provide accurate estimation, power demand forecasting, fault diagnosis, and self-healing power to the smart grid environment. The new-age producer and consumer called the prosumer will benefit largely by adopting this cyber-physical system. A sustainable and economically feasible power system would be available for the prosumers. The application of SG-CPs will be diverse in nature and based on the feedback, many corrections can be initiated in the system. The security aspects of smart grid are to be carefully examined as it is very important.

2. SMART GRIDS

The smart grids are more intelligent when compared to conventional power grids. Smart grids [1] are the ones that use computing devices along with the power system components for better monitoring and management of the electric power supply system. It employs the sensors, actuators, and control equipment in all stages of power supply like generation, transmission, and distribution. In this way, the prosumers are more aware of the happenings of the power system network and can interact in real time.

As prescribed by the National Institute of Standards and Technology [2], the smart grid model can have seven functional units: generation, transmission, distribution, customers, service providers, operations, and markets. Having mentioned the above developments, this new age can witness the transformation of a centralized power industry into a consumer interactive smart grid network. In a smart grid [3], the activities can be monitored and feedback actions can be initiated for better performance.

In every home and industry in the future, we can expect a producer and a consumer *i.e.*, prosumer [4], and the power system setup must be geared up to

CHAPTER 3

Cyber Physical Systems in Clinical Setting

T.P. Kamatchi[1,*], Anitha Kumari K.[2] and **D. Priya[1]**

[1] *Department of Computer Networking, PSG Polytechnic College, TN, India*

[2] *Department of Information Technology, PSG College of Technology, Coimbatore, TN, India*

Abstract: Cyber Physical Systems (CPS) is a new generation of systems with integrated control, communication, and computation capabilities in the modern world. Just as the Internet changed the way people interacted with one another, cyber physical systems will change how people engage with the real environment. Currently, CPS research is in its infancy, and numerous research concerns and obstacles exist in areas such as electricity, health care, transportation and smart construction, agriculture, and others. The architecture of CPS and Wireless Sensor Networks (WSNs) for cloud computing for life support or healthcare and its application for monitoring and decision support systems are introduced in this article. The suggested CPS architecture is made up of three primary components: 1) communication, 2) computing, and 3) resource management for healthcare. Industry, agriculture, and hospitals are all being transformed by this type of integration, known as Cyber-physical Systems. CPS enables the systematic transformation of large amounts of data into information, revealing previously unseen patterns of degradation and inefficiency and resulting in an optimal decision-making system. This article focuses on current trends in hospital big data analytics and CPS development. Relevant concepts such as cloud computing, real-time scheduling, and security models are thoroughly examined and explained. Finally, a healthcare application section is offered, which is based on our long-running practical test bed. Many businesses and hospitals are confronting new opportunities and problems as Information and Communication Technologies (ICT) improve and advanced analytics are integrated into manufacturing, goods, and services. Finally, a case study using the CPS to construct intelligent machines is provided.

Keywords: Cyber-Physical systems, Clinical setting, CPS architecture, CPS challenges, CPS characteristics, Smart sensors, Service-oriented architecture, Security challenges.

[*] **Corresponding author T.P. Kamatchi:** Department of Computer Networking, PSG Polytechnic College, TN, India; E-mails: tpk.dcn@psgpolytech.ac.in, kamatchiperi@gmail.com

1. INTRODUCTION

1.1. Cyber Physical Systems

Systems that combine computing, networking, and physical operations are known as cyber-physical systems (CPS). There are feedback loops where the physical processes influence the computations and *vice versa*. Embedded computers and networks are utilized to monitor and control physical processes, and their potential economic and societal impact exceeds current recognition. Worldwide investments are being made to advance this technology. Embedded systems, which focus on computers and software within objects like cars, toys, medical equipment, and scientific instruments, form the foundation for this technology. Cyber-Physical Systems (CPS) combine the dynamics of physical processes with software and networking, employing modeling, design, and analytical methodologies. Moreover, CPS provides abstractions for integrated systems.

1.2. Definition of Sensor

Any type of input from the physical world can be detected by a sensor, which then responds to it. Light, heat, motion, moisture, pressure, or any of the many other environmental phenomena could be the specific input. Typically, the output is a signal that can be read or processed further after being translated into a human-readable display at the sensor position.

1.3. Classification of Sensors

Different writers and professionals have categorized sensors in a number of different ways. Some are relatively straightforward, while others are intricate. An expert in the field may already use the classification of sensors that follows, although it is fairly straightforward.

The sensors are separated into Active and Passive categories in the first classification. **Active sensors** are those that need an external [1] power signal or an excitation signal. On the other hand, **passive sensors** produce an output response without the need for any external power signals. The other classification method is based on the sensor's method of detection. **Electric, biological, chemical, radioactive**, and other methods of detection are some examples.

The following classification is based on the input and output of conversion processes. **Thermoelectric, photoelectric, thermoelectric, electrochemical, electromagnetic**, and other frequent conversion processes are only a few.

Analog and **digital** sensors make up the last two categories of sensors. Analog sensors generate an analogue output, often known as a continuous output signal, in proportion to the quantity being measured (often voltage but occasionally other quantities like resistance *etc*.). In contrast to analogue sensors, digital sensors operate on discrete or digital data. Digital sensors contain data that is digital in nature and is utilized for conversion and transmission.

1.4. Usage of Sensors

Several industries, including automotive, medical, aerospace, defense, and agriculture, use sensors for various purposes.

• **Position sensors** are employed to measure rotational or linear movement, displacement, and position. These are employed for steering angle measurement, wind direction measurement, ramp and bridge location, flight simulation, and throttle control.

• Pressure is measured with **pressure sensors**, which can be differential, gauge-style, or absolute. Transducers, commonly referred to as pressure switches or pressure transmitters, are the most widely used types of pressure sensors. Oil pressure, tyre pressure, car braking systems, oil pressure, fans, filters, and applications for diesel and engines are just a few of the applications for pressure sensors.

• The **force sensors**, sometimes referred to as load cells or weight sensors, are employed in scales for weighing purposes.

• By monitoring the amount of force being applied, **weight sensors** are renowned for providing an accurate weight measurement. The load sensors are utilized in tank weighing, on-boarding weighing, hopper weighing, and platform weighing, and counting scales.

• Temperature sensors are employed in the monitoring and detection of liquid, solid, and gas temperatures. It is the most often used sensor in houses and comes in a variety of sizes and shapes to serve diverse needs. This kind of sensor is utilized in home appliances, computers, electrical radiators, industrial equipment, motors, and surface plates. Sensors are quite useful and are utilized in many pieces of technology that can be utilized every day.

1.5. How Do the Sensors' Function?

It is well known that sensors change their electrical characteristics in response to changing physical conditions. Electronic systems have been shown to be the most common means by which artificial sensors analyze, record, and transmit

CHAPTER 4

Cyber Physical Systems in Autonomous and Unmanned Aerial Vehicles

Sindhu Rajendran[1,*], **Shreya S.**[1], **Alaska Tengli**[1] and **Ramavenkateswaran N.**[1]

[1] *Department of Electronics and Communication, R. V. College of Engineering Bangalore Mysore Rd, RV Vidyaniketan, Bengaluru, Karnataka-560059, India*

Abstract: In today's world, the demand for autonomous and unmanned aerial vehicles is rapidly growing with applications in many domains. These autonomous vehicles have potential advantages like – a reduction in traffic deaths by 90%, a drop in harmful emissions by 60%, an improvement in fuel economy by 10%, an increase in lane capacity by 500%, a reduction in travel time by 40%, an increase in transportation accessibility and a reduction in transportation costs. Similarly, UAVs have advantages like- traffic monitoring, moving objects in seemingly dangerous environments, payload delivery and surveillance. Cyber-Physical Systems (CPS) are combinations of networking, computation and physical systems. The three interacting components of CPS - communication, computation, control and their coupling effects are necessary for improving the performance of the UAV network. Control mechanisms, performance and safety of autonomous and unmanned aerial vehicles are the important factors to be considered while designing them.The major concern for any fully or partially autonomous system is safety, the other challenges faced are: mechanical failure, communication bandwidth shortage, cyber-hacking, communication delay, *etc*. Various designs are proposed and tested to overcome these challenges, few of them are: a framework for software - ReMinds in addition to the extensions implemented in the Dronology system; for Dronology, researchers have proposed and designed incubators for safety-critical CPS. The chapter emphasizes the role of CPS in autonomous and unmanned aerial vehicles, framework of CPS for UAVs, the challenges with respect to CPS and is concluded with the state of art of the present autonomous vehicles.

Keywords: Autonomous vehicles, Computation, Component based design, Controller area network, Cyber physical system (CPS), Cyber security, Data-driven strategy, Dronology, Embedded systems, Model based design, Networking, Physical Processes, ReMinds, Safety, Sustainability, Transportation, UAVs.

[*] **Corresponding author Sindhu Rajendran:** Department of Electronics and Communication, R. V. College of Engineering Bangalore Mysore Rd, RV Vidyaniketan, Bengaluru, Karnataka-560059, India;
E-mail: sindhur@rvce.edu.in

Anitha Kumari K. & Avinash Sharma (Eds.)

1. INTRODUCTION

A cyber-physical system (CPS) combines computing with physical processes, and the behavior of the system is determined by both the computational and physical components. Embedded communications and devices continuously track mechanical phenomena, which typically involve feedback where computations are impacted by physical processes and *vice versa*. The Internet of Things and the industrial Internet are examples of embedded systems. Modern cars, fly-by-wire airplanes, medical gadgets, electricity production and dissemination techniques, robots, building control systems, distribution systems, and many more are examples.

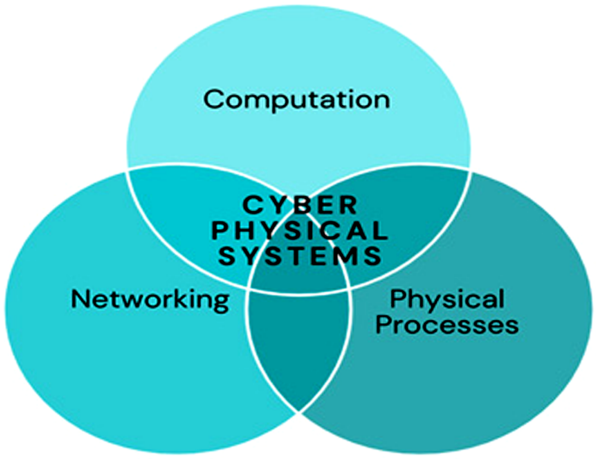


Fig. (1). Venn diagram depicting cyber physical system [1].

The junction of the physical and digital worlds—not their union—represents the conceptual challenge of CPS. Separately designing, analyzing, and comprehending the computational and physical components, and then connecting them, is insufficient. We need to comprehend and plan for the interplay of various components, such as computing, connectivity, and physical processes, in order to enable their integration. Fig. (**1**) illustrates a Venn diagram representing the cyber-physical system.

Although cyber-physical systems have been present for a while, the field has just lately come together as an academic study. Because of this, there aren't currently established design methodologies for CPS that are backed by tools as there are, say, digital circuit design, even if there are methods and tools for automating CPS design in some domains.

CPSs are also multidimensional and more complicated than integrated circuits. There is no unique "design space" for Cyber physical systems like there is for digital systems. The CPS of today bridges the real and virtual worlds, equipment and software, actuators and sensors.

They are also frequently large-scale, increasingly dispersed systems. They must be adaptable since they must function in extremely dynamic contexts and for constantly changing goals. Finally, because many CPSs work alongside human operators, the human element of their design must be carefully taken into account. For the community of design automation, this demand represents a substantial potential. Every stage of the design process is covered by some factors, including specification, designing, language layout, software, simulation, testing and evaluation, analysis equivalence and precision verifying, surveying, performance process optimization, user interfaces, routing algorithms, testing, bug fixing, treatment plan, as well as fixing, and other.

We believe that each of these examples need further development in conceptual model, methods, and equipment where there is a need to make the architecture of CPS as regular and their conduct as expected as the planning and installation of digital circuits are at the moment. We demand new design methods for CPS that have an effect equivalent to the register transfer level(RTL) design flow for digital systems. Additionally, the rising accessibility of data on system design and field usage increases the possibility of developing new design techniques for CPS. In this work, we place more emphasis on an explanation of a fundamental approach that has been thoughtfully chosen than outlining the various specific prospects for systems engineering of CPS.

1.1. Evolution of Autonomous Vehicles

Numerous industrial sectors, including the automotive industry, mining, machinery, *etc*., are actively researching the development of automated driving technology. New autonomous driving assistance system features and functions are continually being developed by the car industry. By the end of this decade, completely autonomous driving is the general goal. Many automakers, like Tesla, Ford, and others, have stated recently that they would have completely autonomous driving vehicles very soon, but they frequently have had to push back their stated timelines. The most well-known autonomous driving projects are Apple's self-driving vehicle project and Waymo from Google [1]. However, the problems involved have been more than first anticipated, and as a result, their efforts have been hindered and the deadlines are prolonged. Fig. (**2**) shows the expected Global Autonomous Car Sales Projection (2019-2030) sold worldwide.

CHAPTER 5

Cyber-Physical System: Advances and Applications in Cyber Security

Sindhu Rajendran[1,*], **Shilpa S.P.**[1], **Sai Priya L.**[1] and **Ramavenkateswaran N.**[1]

[1] *Department of Electronics and Communication, R. V. College of Engineering Bangalore Mysore Rd, RV Vidyaniketan, Bengaluru, Karnataka-560059, India*

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.

However, interconnecting the cyber and physical worlds 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: Bayesian detection, Binary hypothesis, Cyber security, Cryptography, Cyber-physical system, Denial of services, Deception attack, Digital twin, FACT graph, Industry 4.0, Privacy, Physical threats, Reply attack, RNN based security, Safety and Security, Security model, Security algorithm, Threat modeling, Threat model, Weighted least square.

[*] **Corresponding author Sindhu Rajendran:** Department of Electronics and Communication, R. V. College of Engineering Bangalore Mysore Rd, RV Vidyaniketan, Bengaluru, Karnataka-560059, India; Tel: +91-9538351009; E-mail: sindhur@rvce.edu.in

Anitha Kumari K. & Avinash Sharma (Eds.)

1. INTRODUCTION

Smart data operation, data analysis, and processing capability lead to the growth of cyberspace; advanced integration 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 a present focus 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: desktops, servers, and 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.

1.1. 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 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 that go into considerable detail about the 5C Framework, describe how Cyber-Physical Systems and their layers work as transformational technologies for managing network connections, and define CPS in great detail [4].

1.1.1. 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 the 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:

1.1.1.1. 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.

1.1.1.2. Smart City Management

A smart city, according to Tech Target, is “a municipality that employs information and communication technology to boost operating effectiveness,

CHAPTER 6

Cyber-Physical Systems in HealthCare

M. Revathy[1,*] and **A.S. Rakseda keerthi**[1]

[1] *PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India*

Abstract: Cyber-Physical Systems (CPS) are being developed with the integration of computational capabilities and communication with physical systems. Recent technologies like WSN (Wireless Sensor Networks), Communication Networks, Cloud Computing, Big Data, and many more use CPS. Applications include Smart Grid, Healthcare, Transportation, and Smart Buildings. CPS has made a huge impact on increasing the efficiency of medicines and life span in many developed countries. This has drawn researchers and the government's interest in Medical Cyber-Physical Systems (MCPS), especially during Covid times. Many models were developed during the pandemic. One of them is a Machine Learning (ML) integrated X-ray device called Covilearn. In this chapter, an introduction to CPS in health care, its current trends, and a device called e-stocking has been discussed. It is being used to treat leg venous insufficiency. The motive of the application of CPS is to reduce power consumption for long-term usage. This system is based on a model-driven energy-aware approach. There are three approaches - Mechanical, Software, and Communication. False alarm is one of the major issues as it is a pressure on both patients and caretakers. A model aimed at resolving this problem is proposed and discussed here. Also, the existing challenges and prospective opportunities in the domain of CPS have been explored.

Keywords: Biosensors, Databases, Data management, Cloud computing, Communication, Computation, Covi-learn, Closed loop systems, Cyber-physical systems, E-Stocking, Machine learning, Medical cyber-physical systems, Networks, Taxonomy, Transfer learning, Networks, Security.

1. INTRODUCTION

Cyber-physical systems are the integration of the cyber world and the physical systems through a network. In this era of automation, CPS has gained attention for its diverse applications. CPS was considered a key research area in 2008 by the US National Science Foundation (NSF) and was listed as the US President Council's top priority [1]. CPS relies on sensing, processing, storing, and networking. The three main components are software for computation, physical systems for sensing, and a network for the flow of data.

[*] **Corresponding author M. Revathy:** PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India; E-mail: manireva1975@gmail.com

Anitha Kumari K. & Avinash Sharma (Eds.)

As far as the cyber side is concerned, it is used for computations and wireless communications. It includes technologies such as the Internet of Things intelligence, machine learning, and many more [1]. It plays an important role as it consists of software for the analysis, diagnosis categorization, and storage of information. It collects the data from physical systems and stores it as a database in the cloud. These data can be retrieved for future reference.

By considering its physical characteristics, it consists mostly of sensors and actuators. It senses various environmental factors and sends the data to the software through the network. Environmental factors may vary depending on the use. The type and characteristics of the sensors also vary. For example, for agricultural use, temperature sensors and moisture sensors can be used. In healthcare, very sensitive sensors are used to detect very minute changes in biomedical sensors. [2].

The third main component is the network. It may be wired or wireless based on the use. The wired one is used when the patient is monitored in the hospital. But wireless is more convenient as it is more portable. The patients can be monitored even from their homes. It makes both the device and the patient in movement. The device is easy to carry to remote places by physicians.

CPS is applied in a wide range of fields. this includes agriculture, transportation, education, environmental control, smart building, smart grid, smart home, and smart manufacturing. In this chapter, CPS in Healthcare, namely, the Medical Cyber-Physical systems (MCPSs), is discussed.

MCPS is considered a powerful solution for healthcare. The traditional Healthcare method has doctors as controllers and medical devices as sensors. MCPS provides more types of sensors for computation. The advantages include faster results and accuracy. However, building the intricate devices is a complex and tedious process. This is due to the insufficient understanding of the human body. And the difference in patients due to their age, medical history, and environment. Fig. (**1**) outlines the components of Cyber-Physical Systems (CPS).

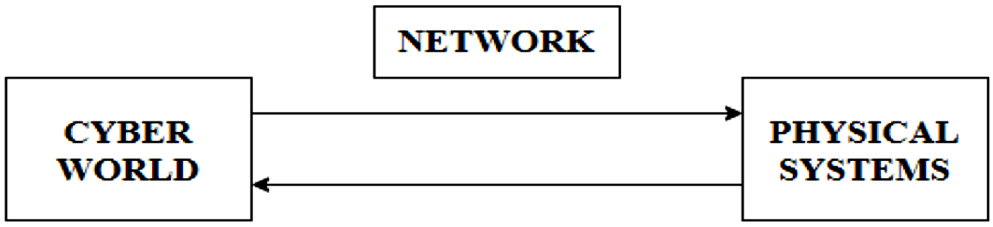


Fig. (1). Components of cyber-physical systems [1].

2. CURRENT TRENDS

The ongoing trends in the development and the security of the devices are discussed below. Also, the trends developed for the usage and storage of data and networks are given below.

2.1. Software Based

The new devices are largely based on software-driven technology. An apt example is software surgery, which requires real-time monitoring and control of the devices based on high-resolution images [2]. Another example used for cancer treatment is the proton therapy treatment in radiotherapy. High-intensity proton beams from the cyclotron have been applied to the patients. It requires precise guidance as it also takes the small movement of patients into account. Compared to conventional radiotherapy, it allows high radiation to be passed. Hence, there are stringent requirements on patients' safety and timing for precise application. Another function is to process real-time images for the placement of beams and to calculate the small movements of the patients.

2.2. Increased Connectivity

The other advantage of MCPS is the network. The networking is done more to develop an interconnected large device with integrated functionality. The network is mainly used in monitoring the patients from a distance and in storing patients' data.

Medical device Plug and Play (MD PnP) is a good initiative in networking [2]. It allows the interoperability of devices. One of them is the connection between the X-ray machine and the ventilators. X-ray images were taken during the operations. The patient who is in general anesthesia cannot hold their breath. As a result, only a blurred image of the lungs can be taken. So, the ventilator has to be stopped before the image is taken. But sometimes, ventilators cannot be used at the correct time, which may lead to the death of the patient. Hence, the X-ray machine can be connected to the ventilator. The machine will turn on and off the ventilator before and after an operation. The high-risk but good alternative is to let the ventilator control the X-ray machine. As there will be a pause during the breathing cycles, this pause can be used to take the image.

2.3. Continuous Monitoring

There has been an increase in demand for home care, assisted living, and sports activity monitoring.

CHAPTER 7

Journey from Data Warehouse to Data Lake

Geeta Rani[1,*], **Puninder Kaur**[2] and **Avinash Sharma**[3]

[1] *Department of Computer Science and Engineering APEX, Chandigarh University, Haruan, Punjab, India*

[2] *Institute of Engineering and Technology, Chitkara University, Punjab, India*

[3] *Chandigarh Engineering College, Jhanjeri, Mohali, Punjab 140307, India*

Abstract: With the increase in high volume, velocity, and variety of data, the traditional data analysis approaches are not adequate to handle diverse analysis challenges. Traditionally, a data warehouse is being used which is an integrated repository from various sources used for management and decision-making in business. Data is already in a transformed and structured format stored in a costly but reliable storage device. The data warehouse does not include all the data that may be not required at the time of construction of the data warehouse. With the advent of big data and to handle the data silos problem, the concept of Data Lake is introduced to handle data analysis. Data lakes have not replaced the data warehouse but rather complement it. In this chapter, firstly Data Lake is introduced and compared with predecessor technologies, then various tools and techniques are discussed to implement Data Lake.

Keywords: Big data, Data warehouse, Data lake, Data analysis, Hadoop.

1. INTRODUCTION

Data is a key to the success of a business and it keeps on mounting day by day. Huge amounts of data are produced from social platforms [1], IoT devices, digital devices, e-commerce, *etc*. Organizations want to understand customer choices to facilitate them with better service and earn maximum market share. It can be possible by customer data collected from various sources. To draw valuable inferences, data must be organized and analyzed systematically.

Traditionally, a file system was used to handle a large pool of data. Then IBM introduced the concept of a centralized Database Management System in 1966 and provided a three-level architecture to handle the problems of replication, accuracy, concurrency, recovery, *etc*.

[*] **Corresponding author Geeta Rani:** Department of Computer Science and Engineering APEX, Chandigarh University, Haruan, Punjab, India; E-mail: geeta@chitkara.edu.in

Anitha Kumari K. & Avinash Sharma (Eds.)

In the 1980s, Relational databases became more popular due to their simplicity and user-friendly language *i.e*., Structured Query Language (SQL). In 1990, there were major cultural and technological changes that took place in the business world. Globalization and expansion of business in 2000 required exhaustive decision-making to survive and excel. The conventional systems were good enough to handle the operational databases as data is stored as per the business processes but not sufficient for decision making.

So, to complement the operational database, an enterprise-wide data warehouse [2] came into existence, which is primarily equipped for decision-making. A data warehouse [3] is stuffed with a historical, non-volatile collection of data in the pre-processed (summarized) form as per the subjects of interest [36]. However, building a data warehouse for every enterprise is not feasible. It is because the data warehouse contains all the data of the organization as a whole which is a costly affair. So, a mini-warehouse or data mart is being built that focuses on selective departments or subjects of interest.

With the advent of big data, the cloud, IoT, and social media, there is a rapid increase in the volume of data. Every second, millions of data are produced in different formats which contain a huge value for business. This huge amount of data cannot be stored by the traditional techniques because it requires a lot of preprocessing and even all data is not required every time. So, a new concept of Data Lake is required which complements the earlier approaches and stores all the data in raw format for future reference, and only that data is processed which is required at that time. It is just like that we store a lot of water in lakes for future reference in an unprocessed form and only the required amount of water is filtered for use at home for drinking [4]. In section 2, the concept of Data Lake has been introduced with its advantages. The data warehouse and Data Lake are distinguished in Section 3. Sections 4 and 5 describe the Data Lake architecture and Hadoop Ecosystem. Challenges and recommendations are discussed in Section 5 and then Section 6 concludes the paper.

2. DATA LAKE AND ITS BENEFITS

There is a rapid increase in data with the development of the internet, Cloud, and web technologies. Thus, more sophisticated business Intelligence tools are required as they play a vital role in the growth of any organization. Business Intelligence improves business decision-making by revealing the potential threats and opportunities [5, 6]. Initially, business Intelligence focused on organizational data only. Organizations build the data warehouse [7] which is an integrated, subject-oriented, time-variant, and non-volatile collection of data that is used explicitly for decision-making. Data is stored already in processed (structured)

form on a reliable media so that information can be extracted for decision-making whenever required. But with the emergence of Big Data [7], it became a requirement to consider the broad view of data. It became a challenge to analyze big data as it deals with volume and variety of data. It contains not only structured data but also semi-structured and unstructured data. There is a requirement to convert all variety of data to a structured form to store it in the data warehouse. It is not practically feasible for organizations to increase their storage and processing capabilities to analyze the large volume of dynamic data. Moreover, other forms of data cannot be ignored as they contain the major part of important organization data (70%-80%). So, to handle the current needs of businesses, a practical solution is Data Lake.

Data Lake is a lake (big repository) of data for an organization. Data is loaded from diverse [8 - 10] resources and stored cost-effectively [11]. Data Lake can possess structured, unstructured, semi-structured, or binary data in the raw form as shown in Fig. (**1**) and processed when required for decision-making. It can be said that Data Lake contains big data for an enterprise that is used for advanced data analytics.

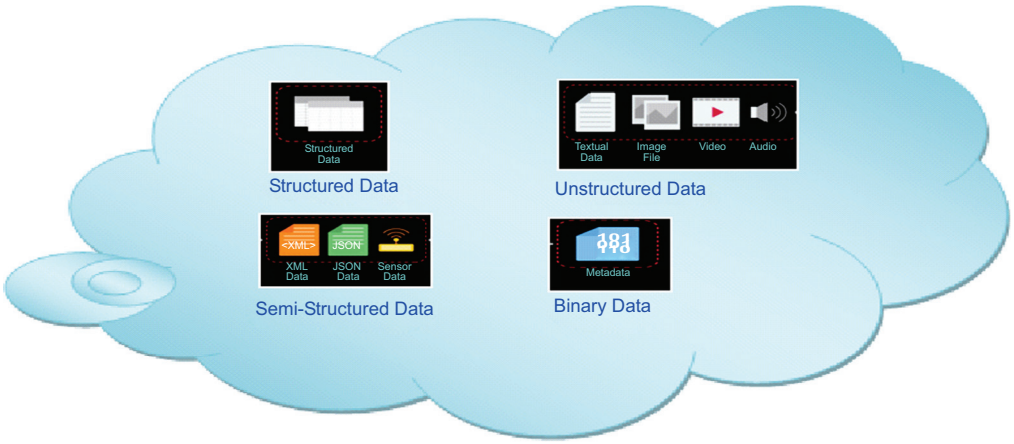


Fig. (1). Types of data in data lake.

Data Lake [12] can be stored within the organization or on the cloud. But generally, companies like to store Data Lake on the cloud due to availability, scalability, cost, and reliability. Cloud services are provided by several vendors like Amazon, Google, and Microsoft.

CHAPTER 8

Feature Selection and Classification Models of Intrusion Detection Systems -A Review on Industrial Critical Infrastructure Perspective

M. Karthigha[1,*], L. Latha[2] and **R. Madhumathi[1]**

[1] *Sri Ramakrishna Engineering College, Coimbatore-641022, India*

[2] *Kumaraguru College of Technology, Coimbatore-641022, India*

Abstract: It is self-evident that recently, humanity has entered the fourth industrial revolution. With the advent of the Internet of Things, cloud computing, and Artificial Intelligence, industrial critical infrastructures such as power plants, oil and gas plants, heavy industries, nuclear plants, and water treatment facilities are experiencing disruptive growth. This era of industrialization, nevertheless, has carried with it its new myriad of issues, notably regarding cyber security threats. Nowadays, industrial processes are openly connected to the internet, and internet-connected machines are almost always highly susceptible to security breaches by adversaries despite sufficient cyber security safeguards. Intrusion detection systems (IDS) are designed to employ classification models to detect malicious attacks such as service attacks, probing attacks, *etc*. In intrusion detection, the phase that reduces the number of similar traffic attributes while sustaining the accuracy of classification is a requirement that considerably improves an intrusion detection system's overall efficacy. This chapter focuses on (i) various feature selection methods in IDS, (ii) ML&DL classification models in IDS of industrial systems, (iii) Various ensemble feature selection models are analyzed, and a novel ensemble feature selection model for IDS is proposed.

Keywords: Classification, Feature selection, Intrusion detection systems, Machine learning.

1. INTRODUCTION

An Intrusion Detection System (IDS) can be a network monitor system that detects suspicious behavior and sends notifications. IDS plays a crucial role in maintaining the security and integrity of digital environments. IDS identifies potentially harmful activities, such as unauthorized access attempts, malware, and

[*] **Corresponding author M. Karthigha:** Sri Ramakrishna Engineering College, Coimbatore-641022, India; E-mail: karthighamohan@gmal.com

Anitha Kumari K. & Avinash Sharma (Eds.)

abnormal network behavior. When suspicious activity is detected, IDS generates alerts or notifications to inform system administrators or security personnel [1].

Earlier Security Information and Event Management (SIEM) is used in organizations for information security. Any harmful interest is usually reported to gather an SIEM gadget. An SIEM system combines information from many resources and uses alert filtering algorithms to show differences between malicious and fake alarms. Although this keeps an eye fixed on networks for suspicious ports, they may be at risk of fake alarms. Because of this, organizations must first implement IDS and then optimize them. It involves effectively configuring intrusion detection systems to differentiate between valid network site visitors and malicious activities. This technology is used by IT departments in enterprises to get insight into potentially dangerous activities that occur in their technical settings. It also enables information to be shared across departments and organizations more securely and reliably. It is, in many aspects, an advancement over conventional cybersecurity technologies such as firewalls, antivirus, and message encryption. The advantages and disadvantages of IDS are given in Fig. (**1**).

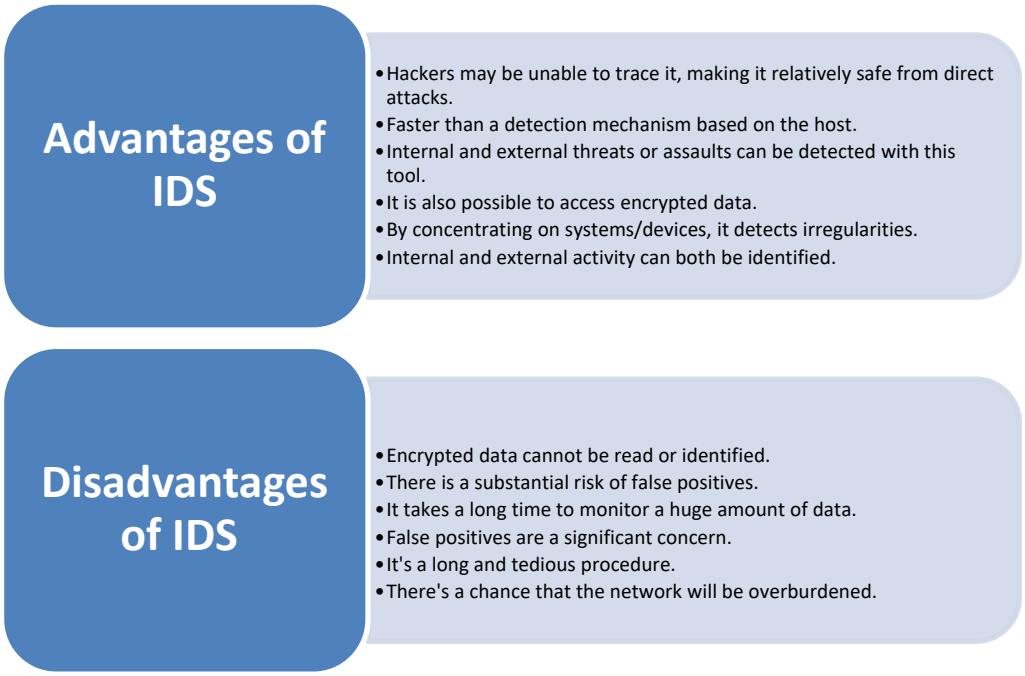


Fig. (1). Advantages and Disadvantages of IDS.

1.1. IDS for Industrial Control Systems

Industrial Control Systems are employed to control industrial processes. Actual-time statistics, gadget tracking, automated manipulation, and management of commercial strategies are the major duties of ICS [2]. Finance, transportation, water storage, manufacturing, and power manufacturing and distribution are just a number of the industries that employ ICS. They are a key element at some point in a country's crucial infrastructure and feature an immediate impact on the financial system. ICS has become smarter and more open as they combine more with PCs and internet technology (IT).

The safety of ICS has sparked big public challenges in recent years, and therefore, the frequency of cyber attacks in opposition to ICS is rapidly developing. In 2010, the infamous Stuxnet malware2 attacked Iran's Natanz nuclear enrichment complex, capturing several important structures and then unnaturally accelerating the uranium-enriched centrifuge, ultimately resulting in the centrifuge's destruction. The plant had no preference, however, to close. BlackEnergy 33 hacked the Ukraine strength device in 2015, infiltrating the power grid management center through VPN, tampering with the relay's control instructions, and separating the circuit. Dr. Staggs established the method to link unmanned wind generators inside the United States of America to compromise the wind farm control gadget at Black Hat 2017. Consistent with a succession of security events, ICS has turned out to be a well-preferred target for hackers. One of the most urgent worldwide demanding situations is a way to protect the security of ICS.

One of the essential components of maintaining the safety of ICS is intrusion detection. Intrusion detection technology for ICS is now a search hotspot that has attracted a lot of interest from academia and businesses. As a result, a range of intrusion detection algorithms for ICS have evolved. IDS are intended to spot harmful attacks routinely. They accumulate and examine community site visitors, safety logs, audit information, and expertise from vital places on a laptop that allows you to decide whether or not the device has any security flaws [3]. The paper provides an explanation for intrusion detection strategies for ICS and proposes a brand-new categorization of ICS IDS that takes into consideration the unique characteristics of ICS.

1.2. Types of Intrusion Detection Systems

Different types of IDS are classified based on different techniques and methods [4, 5], which are depicted in Fig. (**2**).

SUBJECT INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

V

W

Anitha Kumari K.

Prof. Anitha Kumari is working as an associate professor in the Department of IT for more than 13 years in PSG College of Technology, India. As an independent researcher, she had an opportunity to present her UGC sponsored research paper based on quantum cryptography in the USA and visited a few foreign universities. She has a granted patent along with 3 published patents. She published around 110 technical papers in refereed and impact factored international/national journals/conferences published by IEEE, Elsevier, Springer, T&F, etc,. She has published a-book entitled: "Edge Computing: Fundamentals, Advances and Applications", by CRC Press and contributed in several book chapters published by CRC Press, Springer, Bentham, IGI Global, etc., She is the recipient of Shri. P. K. Das Memorial Best Faculty Award. She is also serving as editorial board member for different Scopus-indexed/open-access journals. Besides, she has been an active reviewer for prestigious journals. She has been the mentor for Technovator Projects (2019, 2018 & 2014) and 'MEDROIDZ', an ICICI – Trinity 2014 funded project that was selected as one among the 6 projects in India. She is currently providing guidance to 8 Ph.D. scholars. She serves as PI and Co-PI for funded projects sponsored by AICTE and DST.

Avinash Sharma

Prof. Avinash Sharma is presently the director of engineering at Chandigarh Engineering College Jhanjeri Mohali. Earlier worked as principal with Maharishi Markandeshwar Engineering College, Mullana, Ambala (Haryana), India. He obtained his undergraduate degree with honours in computers (1998) from Mumbai University, India. He received his master's degree in computers from BITS, Pilani, India. He received Ph.D. in computer engineering from Suresh Gyan Vihar University, Jaipur, India. He has previously served as dean of faculty of engineering and technology, member of the board of studies and DRC committee for research, and ex-principal & professor, Rajasthan College of Engineering for Women (the Leading Women's Engineering College in the state of Rajasthan). He has previously served as the founder principal & professor of Advait Vedanta Institute of Technology, Agra Road Campus, Jaipur, Rajasthan, India during the period (2012–2014).