STOCHASTIC NEUROMORPHIC CYBER PHYSICAL SYSTEMS DESIGN

Thesis submitted in fulfilment of the requirements for the Degree of

DOCTOR OF PHILOSOPHY

By

PAYAL THAKUR

Department of Computer Science & Engineering and Information Technology

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY
Waknaghat, Solan – 173234, Himachal Pradesh, INDIA

November, 2024

DECLARATION BY THE SCHOLAR

I hereby declare that the work reported in Ph.D. thesis entitled **"Stochastic Neuromorphic Cyber Physical Systems Design"** submitted at **"Jaypee University of Information Technology, Wakhnaghat, Solan (H.P), India"**, is an authentic record of my work carried out under the supervision of **"Prof. (Dr.) Vivek Kumar Sehgal"**. I have not submitted this work elsewhere for any other degree or diploma. I am fully responsible for the contents of my Ph.D. Theses.

Payal Thakur

Enrolment No.: 196201

Department of Computer Science & Engineering

Jaypee University of Information Technology, Wakhnaghat,

Solan (H.P), India

Date:

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled **"Stochastic Neuromorphic Cyber Physical Systems Design"** submitted by **Ms. Payal Thakur**, Enrollment no. 196201 at **Jaypee University of Information Technology, Wakhnaghat, Solan (HP), India**, is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree or diploma.

Prof. (Dr.) Vivek Kumar Sehgal (Professor)
Department of Computer Science & Engineering and Information Technology
Jaypee University of Information
Technology, Wakhnaghat,
Solan (H.P),
India
Date:

ACKNOWLEDGEMENT

With the providential grace of "**Almighty God**", the expedition of my Ph.D. came to an end and my heart is overflowing with appreciation towards each and every person who has lend a hand in the form of support, believe and efforts to accomplish this journey.

It is an immense pleasure to express my profound gratitude towards my supervisors **Prof.** (**Dr.) Vivek Kumar Sehgal**, **Professor**, Department of Computer Science & Engineering and Information Technology, JUIT, Wakhnaghat, who graciously gave me the opportunity to work under their guidance. I am thankful for his patience, continuous support, optimistic approach, never-ending deliberations, time to time guidance and liberty throughout this course. I will always stay indebted to him for bearing my shortcomings with their immense sense of awareness, maturity, thorough knowledge of the specific field and consistency.

I would like to express my gratitude to our Honourable Vice Chancellor **Prof. (Dr.) Rajendra Kumar Sharma** and Dean (Academics and Research) **Prof. (Dr.) Ashok Kumar Gupta** to promote the research and facilitate resources in the institution. I would also like to pay my gratitude to the DPMC members **Dr. Ekta Gandotra, Dr. Amol Vasudeva, and Dr. Harsh Sohal** for their thought-provoking interactive assessments, queries and opinions. Their valuable motivation, help, suggestion, affirmative vision, magnificent supervision and enormous confidence in my abilities made me face tough circumstances during the progress of the research work.

I am grateful to my parents and my brother for supporting me through all these years in my PhD journey. Their belief in me has kept my spirits and motivation high during this process. I am obliged for all the support received from all the faculty members and staff of Department of C.S.E & I.T for their scholarly support and guidance. I thank my fellow Ph.D. friends for their consistent help and valuable discussions.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BCPS	Blockchain Enabled Cyber Physical Systems
C2B	Customer-to-Business
CHS	Cyber Human Systems
CPPS	Cyber-physical production systems
CPS	Cyber-Physical Systems
CPSI	Cyber-Physical Systems Integration
CPSoS	Cyber-Physical Systems of Systems
CSS	Cloud Storage Service
DaaS	Data as a Service
DBN	Deep Belief Network
DCS	Distributed Control System
DDAI	Distributed and Decentralized AI
DNN	Deep Neural Networks
DoD	Department of Defence
DPoS	Delegated Proof of Stake
DRP	Deep Reinforcement Learning
DT	Digital Twins
DVFS	Dynamic voltage and frequency scaling
FGPA	Field Programmable Gate Array
FSMC	Finite-State Markov Channel
HART	Highway Addressable Remote Transducer
HRI	Human Robot Interaction
IBEC	Integration of Blockchain and Edge Computing
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISA	International Society of Automation
LQD	Linear Quadratic Regulator
LSS	Lean Six Sigma
LSTM	Long Short-Term Memory
LTD	Long-Term Depression
LTP	Long-Term Potentiation

M2M	Machine-to-Machine
MCPS	Medical Cyber-Physical Systems
NVM	Non-Volatile Memory
OaaS	Ownership as a Service
P2P	Peer-to-Peer
pBFT	Practical Byzantine Fault Tolerance
PCAST	President's Council of Advisors on Science and Technology
PCB	Printed Circuit Board
PHM	Prognostics and Health Management
PID	Proportional–Integral–Derivative
PMSS	Predictive Maintenance Support System
PoA	Proof of Authority
PoS	Proof of Space
PoW	Proof of Work
PUF	Physically Unclonable Functions
QoS	Quality of Service
RNN	Recurrent Neural Networks
RRAM	Resistive Random Access Memory
RTRL	Real Time Recurrent Learning
SCADA	Supervisory Control and Data Acquisition
SCPS	System Control and Process System
SDN	Software Defined Networking
SHM	Structural Health Monitoring
SN-CPS	Stochastic Neuromorphic Cyber-Physical Systems
SNN	Spiking Neural Networks
SOA	Service-Oriented Architecture
STDP	Spike-Timing-Dependent Plasticity
V2G	Vehicle-to-grid
VLSI	Very Large Scale Integration
VFI	Voltage Frequency Islands
VMS	Vehicle Management System
VSM	Value Stream Mapping
WINA	Wireless Industrial Networking Alliance
WoT	Web of Things
WSAN	Wireless Sensor-Actuator Systems

ABSTRACT

In a time marked by rapid technological advancements, the merging of digital and physical realms has given rise to a paradigm that goes beyond traditional limits – known as the Cyber-Physical System (CPS). Characterized by the complex interaction between artificial intelligence and tangible world, CPS has become a crucial element of modern society, influencing various sectors such as manufacturing, healthcare, transportation, and energy. Amidst this evolving scenario, the integration of neuromorphic concepts brings a cutting-edge aspect, highlighting the combination of biological insights with probabilistic computational approaches.

The pursuit of enhanced, flexible, and intelligent systems has spurred the investigation into innovative computational frameworks. Neuromorphic engineering, drawing inspiration from the remarkable efficiency of the human brain, presents a groundbreaking approach to replicating cognitive functions and sensory capabilities in artificial systems. Concurrently, stochastic processes and probabilistic techniques have become essential instruments for capturing and simulating the inherent uncertainties prevalent in real-world settings. The convergence of neuromorphic and stochastic domains gives rise to the concept of "Stochastic Neuromorphic Cyber Physical Design," enabling computational systems not only to perceive, analyze, and interact with the physical environment but also to do so with a foundation in stochastic cognition.

In a period marked by the complex relationship between computing and physical aspects, CPS has become a crucial field, encompassing various uses ranging from self-driving cars to intelligent production. There could be the possible collaboration between random processes, which address natural unpredictability, and neuromorphic technology, which replicates the effectiveness of biological thinking. The integration of neuromorphic computing with cyber-physical systems CPS has garnered significant attention as a promising avenue for realizing efficient, adaptable, and intelligent systems.

The rapid growth and transformation of various industries are being driven by the increasing prevalence of Internet of Things (IoT) devices, blockchain technology, and edge computing. IoT devices are connecting everyday objects to the internet, facilitating extensive data collection and analysis. Blockchain technology is revolutionizing data security and transparency through a decentralized and tamper-proof system for recording transactions. Edge

computing is gaining popularity as a method to process data closer to its source, reducing latency and enhancing efficiency in data processing. These technologies collectively fuel innovation, opening up new opportunities for businesses to enhance operations, elevate customer experiences, and propel digital transformation across diverse sectors.

When integrated with IoT, blockchain technology, and edge computing, CPS form robust interconnected systems that bridge physical and digital realms. By incorporating sensors, actuators, and communication technologies, CPS can gather real-time data from the physical environment to drive informed decisions and streamline processes. IoT devices provide connectivity and data collection capabilities; blockchain technology ensures data security, transparency, and trust within the system; while edge computing supports local data processing for reduced latency and real-time decision-making in CPS applications. The amalgamation of these technologies empowers organizations to establish more efficient, secure, and intelligent cyber-physical systems that foster innovation and enhance performance across a myriad of industries.

The convergence of cyber-physical systems with IoT, blockchain technology, and edge computing yields numerous advantages for organizations. This integration results in enhanced efficiency via real-time data collection and analysis that optimize processes and resource utilization. Enhanced security is achieved through blockchain technology ensuring data integrity and trust within the system while enabling real-time decision-making facilitated by edge computing for faster response times in CPS applications. The transparency provided by blockchain technology boosts accountability and trust in cyber-physical systems leading to cost savings through process optimization improvements. Leveraging these technologies drives innovation, enhances competitiveness, positioning organizations for success in an ever-evolving digital landscape.

CHAPTER 1

INTRODUCTION

1.1 *Introduction*

The development of intelligent systems has been widely recognized as an important topic in modern engineering and science, when rapid progress in computing and communication technologies has made it feasible for even small, specialist computer sciences groups or individuals to solve many problems at work or at home related to the internet. The integration of neuroscience, cyber-physical systems, and stochastic modeling has formulated an emerging paradigm known as Stochastic Neuromorphic Cyber-Physical Systems (SN-CPS) that offers a new power for active perception and control systems in artificial intelligence and autonomous control devices.

By its nature, SN-CPS seamlessly entwines biological neural networks with artificial intelligence, making it a natural competitor in the future. intelligent, adaptive and resilient systems. This research is aimed to provide an exhaustive understanding of this nascent field including the subtleties, opportunities, and consequences.

1.2 Motivation

The first motivation underpinning this research is the ambition to replicate the extraordinary computing prowess of the human brain, and the second is the pressing requirement for more nimble and fault-tolerant cyber-physical systems in the fast-evolving and unpredictable world of the present day. But the dense planetary mass of billions of neurons and synapses, known to us as the human brain, shows us what information processing, learning, and adaptability can look like in nature. Tremendous strides have been made in designing artificial neural networks that approximate its cognitive function, however, scaling these networks, making them energy efficient, and making them robust to real-world uncertainties have proven to be significant challenges.

At the same time, cyber-physical systems (CPS) pervade our society, controlling infrastructural needs, autonomous vehicles, or smart grids. Reliability, adaptability and resilience are demanded to a maximum by these systems which are often exposed to environmental

uncertainties, drug estimation errors, or unexpected events.

This convergence of challenges and opportunities culminates in the intersection of neuromorphic computing, stochastic modeling, and cyber-physical systems referred to as SN-CPS. We aim to address these challenges by pursuing new models, algorithms, and methodologies, which harness the unique abilities of stochastic neuromorphic computing in the context of cyber physical systems. Figure 1.1 shows the basic components of a Cyber Physical System.

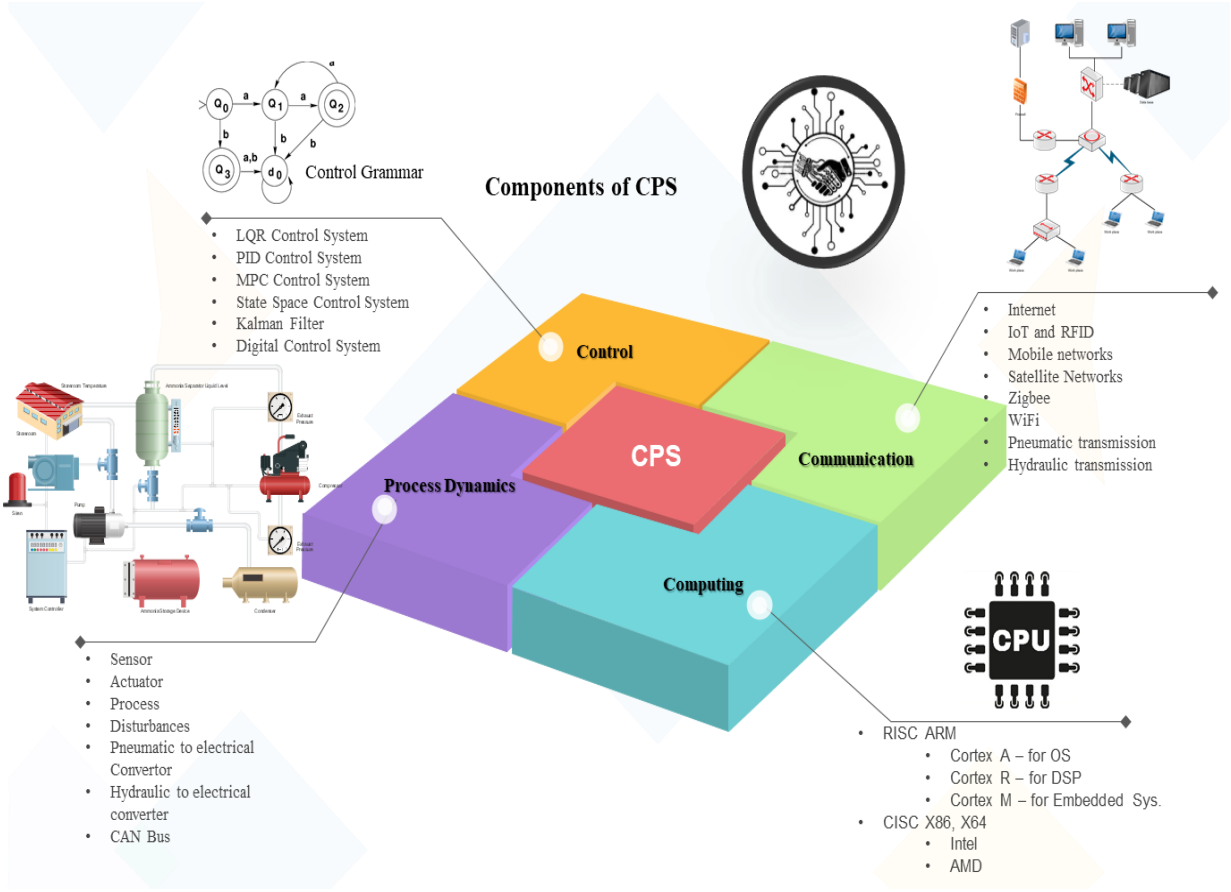


Fig. 1.1 Various components of an CPS

Blockchain is simply a mechanism that secures unalterable records of the transaction based on peer-to-peer network model. Initially associated to cryptocurrencies such as Bitcoin, it is globally identified as a transparent medium, resilient to any alteration and adapted to multiple sectors -from finance to supply chain and even health care. So that it is able to maintain data consistency and deliver operational flexibility

Edge computing is revolutionizing traditional cloud computing by decentralizing data processing and storage nearer to the point of data generation. RocScheduling (Reducing Overhead and Congestion Scheduling) that it make the response time shorter and reduce the

bandwidth resulting that suitable for real-time processing such as autonomous vehicles and smart cities. Edge computing, though, has the advantage when it comes to privacy, security, and speed of the system because edge computing facilitates faster data analysis and quicker decision-making than a similar system without edge computing.

The Internet of Things (IoT) refers to a system of physical devices that are technically savvy, encompassing software, connectivity elements (as sensors and actuators), and storage for its data, which empowers these devices to communicate, collaborate and share information to achieve valuable results on a particular domain, possibly business. For instance, from household gadgets to industrial machinery, all these IoT devices produce large data flows enabling insights, efficiencies, and automation in multiple aspects. IoT is a powerful tool which enhances productivity, convenience and operational effectiveness in a number of sectors like healthcare, agriculture and transportation, by utilizing data analytics and connectivity.

This is where the convergence of blockchain, edge computing, IoT, and Cyber-Physical Systems (CPSs) has the potential to provide a paradigm transformation in terms of security, efficiency, and scalability across industries. The ecosystem of blockchain, edge computing, IoT and CPS integration for secure, efficient, and autonomous operation of interconnected devices and systems. It also has the potential to change industries, from manufacturing and healthcare to transportation and smart cities.

1.3 Contributions

The major contributions of this thesis can be summarized as follows:

- Using modularity algorithm and VFI (Voltage Frequency Island) to efficiently allocate processor cores for different process executions: Efficiently allocates processor cores by grouping tasks with similar communication patterns and allowing cores to operate at different voltage/frequency levels, improving performance and energy efficiency.
- Employing an estimator to assess disturbance signals and adapt control flow within programmed cores, with the goal of minimizing error to negligible levels: Introduces an estimator to monitor and adapt control flow within cores, reducing errors caused by external disturbances and enhancing system reliability in real-time environments.
- Estimating delays at both sensor and actuator ends: Accurately predicts delays at both sensor input and actuator output stages, optimizing decision-making and reducing system latency.

- Employing DVFS (Dynamic Voltage Frequency Scaling) control to enhance process assignment efficiency and decrease energy consumption in computing cores: Utilizes DVFS to dynamically adjust core voltage and frequency based on workload, enhancing process assignment efficiency and reducing overall energy consumption.
- Developing a DVFS controller utilizing a PID algorithm to optimize the supply frequency of computational cores involved in process loops: Implements a PID-controlled DVFS system to regulate core frequency in process loops, optimizing performance while balancing energy use in computational tasks.
- Integrating blockchain, edge computing, and IoT technologies: Combines blockchain for data security, edge computing for low-latency processing, and IoT for real-time monitoring to create a robust, efficient system for Industry 5.0 applications.
- Leveraging Blockchain integration to enhance trust and security within Industry 5.0 CPS: Leverages blockchain to enhance data integrity and trust within cyber-physical systems (CPS), improving security and transparency in industrial environments.

1.4 Thesis Outline

The thesis comprises six chapters. Chapter 1 covers the introduction, while Chapter 2 delves into the literature on neuromorphic systems, their role in Industry 4.0, and the integration of cyber-physical systems within this context, including discussions on Blockchain, IoT, and edge computing. Chapter 3 presents an adaptive framework for various smart industrial cyber-physical systems in the era of Industry 5.0. Chapter 4 outlines a framework for integrating Blockchain, IoT, and edge computing. Chapter 5 explores how blockchain integration enhances trust and security in cyber-physical systems within the Industry 5.0 landscape. Finally, Chapter 6 summarizes the thesis conclusions, drawing from experimental and simulation results, and discusses potential future research directions.

CHAPTER 2

RELATED LITERATURE AND BACKGROUND

2.1 Introduction

In the ever-evolving landscape of modern technology and computing, the convergence of neuroscience, cyber-physical systems, and stochastic modeling has given rise to a captivating and promising field known as "Stochastic Neuromorphic Cyber-Physical Systems" (SNCPS). This interdisciplinary domain investigates the intersection of neuromorphic computing, which seeks to emulate the architecture and capabilities of the brain of a human being, and cyber-physical systems (CPS), which tightly integrate the physical world with computational processes while introducing stochasticity.

SNCP represents a profound departure from traditional computing paradigms, drawing inspiration from the complexity, efficiency, and adaptability of biological neural networks. At its core, it aims to harness the power of stochasticity—randomness or probabilistic behavior—as a fundamental aspect of computation, mirroring the inherent uncertainty found in biological systems.

This literature survey endeavors to provide a comprehensive introduction to the field of SNCP, offering insights into its foundational concepts, research directions, and notable achievements. By thoroughly examining the existing body of knowledge, we aim to elucidate the current state of research and identify the key challenges and opportunities that lie ahead in this compelling field of study.

2.2 Foundations of Neuromorphic Computing

In an era marked by the exponential growth of data and the quest for ever more powerful computational systems, neuromorphic computing emerges as a transformative and captivating approach to computing. At its core, neuromorphic computing seeks to emulate the neural architecture and functioning of the human brain, offering a departure from traditional von Neumann computing models. This paradigm shift stems from the realization that the brain,

with its extraordinary computational capabilities and energy efficiency, serves as a remarkable blueprint for the next generation of intelligent systems.

The term "neuromorphic" itself signifies the fusion of "neuro" (pertaining to neurons, the basic building blocks of the brain) and "morph" (meaning to imitate or emulate). Neuromorphic computing, therefore, endeavors to construct computing systems that mimic the neural processes governing human cognition and perception. Central to this endeavor is the development of spiking neural networks (SNNs), which operate on principles inspired by the firing patterns of biological neurons.

The foundations of neuromorphic computing are deeply rooted in the following key areas:

i. Biological Inspiration: Neuromorphic computing takes inspiration from the intricate and interconnected structure of the human brain. Understanding how neurons communicate, form synapses and process information is fundamental to replicating these processes in artificial neural networks.
ii. Spiking Neural Networks (SNNs): SNNs form the backbone of neuromorphic computing. Unlike traditional artificial neural networks, SNNs use discrete spikes or pulses to transmit information, closely mirroring the behavior of biological neurons. The precise modeling of SNNs is a critical foundation.
iii. Synaptic Plasticity: Synapses in the brain grow and decrease throughout time, adjusting to the patterns of incoming inputs. Synaptic plasticity, which includes concepts like as long-term potentiation (LTP) and long-term depression (LTD), is critical in learning and memory. Replicating these processes in neuromorphic systems is a fundamental challenge.
iv. Learning Mechanisms: Neuromorphic computing explores various learning mechanisms inspired by biology, such as Hebbian learning and spike-timing-dependent plasticity (STDP), to enable systems to adapt and improve their performance through experience.
v. Energy Efficacy: The promise for outstanding energy efficiency is one of the major motivations for neuromorphic computing. By mimicking the brain's energy-efficient processes, researchers aim to create computing systems that can perform complex tasks while consuming significantly less power than conventional computers.

This literature survey aims to dissect and elucidate these foundational aspects of neuromorphic computing. By examining the research and advancements in each of these areas, we seek to

provide a comprehensive understanding of the principles that underlie this exciting field. Furthermore, we will explore the implications of these foundations in shaping the future of computing, from brain-inspired hardware to applications in artificial intelligence, robotics, and beyond. Through this exploration, we aim to contribute to the broader conversation surrounding neuromorphic computing, highlighting its potential to revolutionize the world of technology and artificial intelligence.

The potential for complete co-design of the computing stack in neuromorphic computers exists. As shown in Figure 2.1 one approach is bottom-up, starting with defining materials and devices, which then inform architectures, algorithms, and applications sequentially. However, there's an opportunity for a co-design approach, where all elements of the design stack directly influence each other. For instance, applications could directly impact the choice of materials, or algorithms could directly influence the circuits employed. RRAM, or resistive random-access memory.

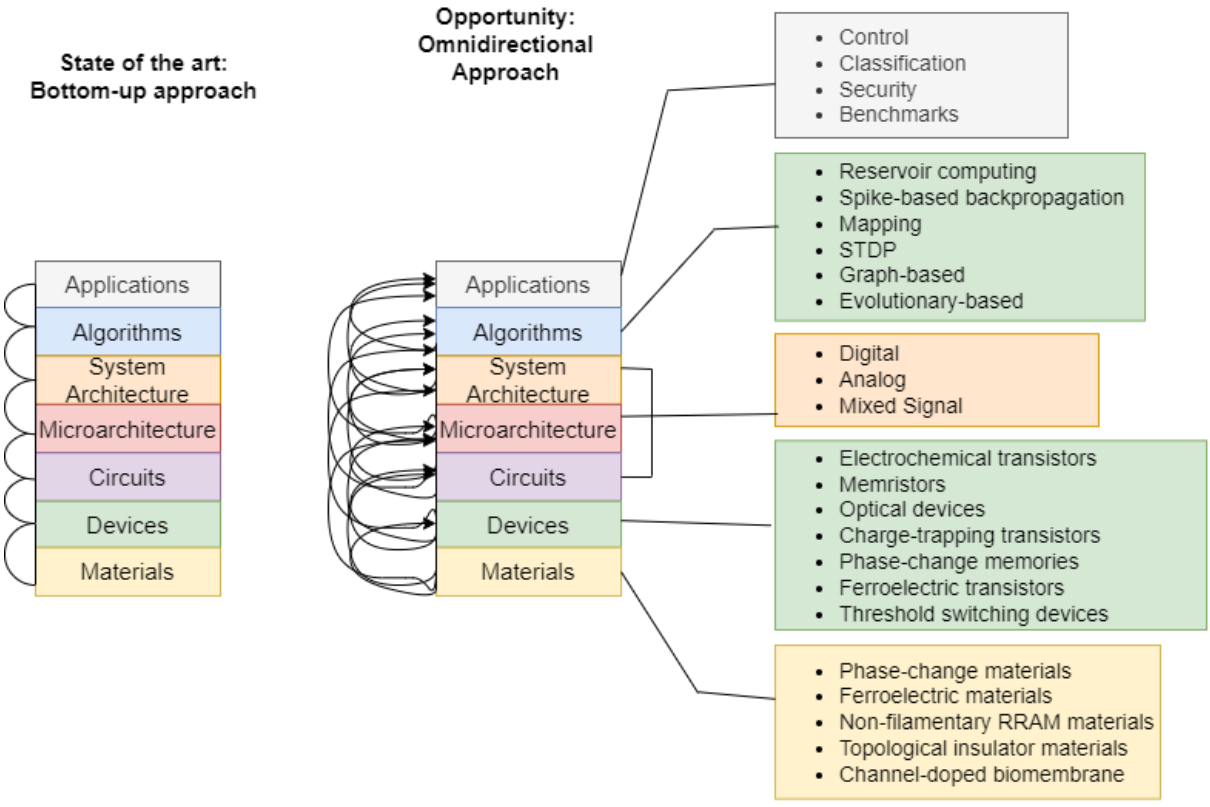


Figure. 2.1. The bottom-up approach and omnidirectional approach

Marković et al.[1] delves into the potential transformative impact of incorporating more profound principles of physics into the algorithms and the utilization of nanoscale materials for data processing within the realm of neuromorphic computing. It explores the remarkable outcomes that have emerged through the integration of physics-driven techniques, such as the

use of resistive switching materials, photonics, and spintronics, among others, to augment the computational capabilities of artificial neural networks. A slew of ambitious, huge-scale neuromorphic initiatives has developed in recent years, pushing the frontiers of this technique to new dimensions and functions. These expansive initiatives have been underpinned by substantial funding endeavors directed toward brain-related research, creating an opportune moment wherein the conditions seem propitious for advancing our comprehension of how the brain processes information. **Furber et al. [2]** embark on a journey through the annals of neuromorphic engineering, tracing its evolution from its inception. Subsequently, they pivot their attention to illuminate the key attributes of some of the foremost large-scale projects currently in play. The authors endeavor to shed light on the varied capabilities that each of these projects brings to the realm of neural modeling and computational neuroscience.

Davies et al [3] embark on a journey to scrutinize the outcomes achieved thus far with Loihi, spanning the prominent realms of algorithmic exploration. These fields include both traditional deep learning paradigms and cutting-edge methodologies aimed at directly harnessing the intrinsic properties of spike-based neuromorphic hardware. Loihi networks, distinguished by their use of repetition, specific spike-timing connections, synaptic plasticity, randomness, and sparsity, demonstrate an extraordinary ability to execute specific computations with a remarkable reduction in both latency and energy consumption, particularly when compared to cutting-edge conventional methodologies. The search for a light yet powerful parallel computing system that is able to smoothly integrating artificial neural networks into hardware remains to be a difficult task. Within this challenging landscape, organic electronic materials emerge as an appealing alternative. These materials hold the potential to furnish neuromorphic devices that are not only biocompatible but also relatively cost-effective, offering the advantage of low-energy switching and remarkable tunability. **van De Burgt et al [4]** delve into the evolution of organic neuromorphic devices. The exploration encompasses various resistance-switching mechanisms, primarily relying on electrochemical doping or charge trapping. The authors scrutinize innovative approaches that augment the longevity of device states and fine-tune their conductance.

Roy et al. [5] offers an in-depth examination of the progress achieved in the field of neuromorphic computing, encompassing advancements in both algorithmic and hardware facets. The authors underscore the essential aspects of learning mechanisms and the underlying hardware frameworks that facilitate the operation of such brain-inspired systems. Furthermore, it delves into the principal challenges confronting neuromorphic computing and casts a

forward-looking gaze on its potential future trajectories, with a particular focus on the symbiotic relationship between algorithmic and hardware co-design. **Burr et al. [6]** provides a viable route for the realisation of extremely efficient and massively parallel neuromorphic computing systems through the use of dense crossbar arrays consisting of non-volatile memory (NVM) devices. The authors explore recent breakthroughs in the use of NVM devices across three separate computing paradigms: spiking neural networks (SNNs), deep neural networks (DNNs), and 'Memcomputing'. They also conducted a thorough examination of the most recent studies in which various types of NVM devices, such as phase-shifting memory, conductive-bridging RAM, filamentary and non-filamentary RRAM, and other NVM variants, have been suggested for incorporation into neuromorphic computing applications, either as synapses or neurons. They also critically evaluate these devices' inherent strengths and limitations, by considering aspects including conductance dynamic range, linearity or non-linearity of conductance responses, symmetry or asymmetry in conductance behaviour, retention of information, perseverance, necessary switching power, and device variability.

The increased interest in photonic computing research can be linked to the extensive use of optoelectronic elements in photonic integration systems. The embedded photonic circuits cleared the path for superfast artificial neural networks, ushering in a new era of data processing gear. In contrast, neuromorphic photonics emerges as an alternative with sub-nanosecond latency, offering a complementary avenue for the expansion of artificial intelligence applications. In **Shastri et al. [7]**, authors delve into recent advancements in integrated photonic neuromorphic systems, analyze the existing challenges, and outline the scientific and technological breakthroughs required to overcome these hurdles. Bridging the gap between deep learning and neuromorphic systems requires overcoming the inherent disparities between backpropagation, which employs continuous-output neurons and synaptic weights, and neuromorphic architectures, characterized by spiking neurons and discrete synapses**. Esser et al. [8]** provides an innovative approach that involves treating spikes and discrete synapses as continuous probabilities, enabling us to employ standard backpropagation for network training. The trained network can seamlessly translate to neuromorphic hardware by leveraging probability sampling to create one or more networks, subsequently merged through ensemble averaging. While numerous approaches to neuromorphic systems have emerged, each utilizing diverse hardware technologies and software programming approaches, a universally accepted solution remains elusive.

Drawing inspiration from recent discoveries in brain science, **Shi et al. [9]** introduced a novel design principle or the fabrication of neurological-inspired computing systems. The authors have successfully created the 'Tianji' neuromorphic chip and showcased its functionality within a multi-chip architecture on a PCB board. **Marković et al.[10]** examines the burgeoning field of quantum neuromorphic computing, which applies brain-inspired quantum hardware to accelerate neural network computations. The authors explore the potential of this emerging paradigm to leverage current and forthcoming intermediate-sized quantum computers effectively. Various strategies are employed, including utilizing parametrized quantum circuits combined with neural network-inspired algorithms for training. Alternatively, some approaches align more closely with classical neuromorphic computing, utilizing the physical attributes of quantum oscillator assemblies to replicate the functions of neurons and synapses in computation. The survey delves into diverse quantum neuromorphic network implementations, encompassing both digital and analog circuits, elucidating their distinct advantages, and appraising recent compelling experimental findings.

Thiem et al. [11] is aimed to advance both hardware and software aspects. It focused on the development of intelligent computer architectures and high-performance algorithms. The in-house investigation primarily centered on designing mathematical models, algorithms, computing structures, and computational efficiencies to enhance neuromorphic computing and neuroprocessors. The software component showcased the integration of computational power with human-level cognitive capabilities, aimed at enhancing the analytical abilities of Department of Defence (DoD) operators and analysts when dealing with textual and character data. On the hardware side, the authors delved into memristor-based and zero instruction set computing technologies, aiming to provide neuromorphic computing solutions suitable for applications with limitations in size, weight, and power. However, due to the offline nature of gradient-based learning algorithms and the requirement for nonlocal computations, training neural networks on neuromorphic substrates offers major hurdles. **Zenke et al. [12]** explains a mathematical paradigm for developing accurate e-learning techniques for neuromorphic materials. Real-time recurrent learning (RTRL), a web-based method utilised for gradient computation in classical recurrent neural networks (RNNs), and physiologically appropriate principles of learning for training spiking neural networks (SNNs) were specially developed by the authors. They also proposed a sparse approximation approach centred around block-diagonal Jacobians, which reduces computing effort, reduces nonlocal information needs, and

has empirically high learning efficiency, therefore being more appropriate for neuromorphic platforms.

There lately has been a surge in curiosity about integrating nanoparticles into these devices and structures. The fusion of artificial synapses with active channels based on nanomaterials creates exciting prospects for advancements in visual recognition, multimodal sensing and processing systems, and hardware-based neural networks. **Li et al. [13]** summarises recent breakthroughs in synaptic devices based on low-dimensional nanomaterials, innovative devices based on hybrid materials or designs, and alternate hardware neural network implementation approaches. The authors go into engineering factors such as management approaches, complexity of design, and manufacturing procedures. They also see potential developments as well as prospective advancements in neuromorphic systems based on artificial synapses. **Neftci et al.[14]** digs into multidisciplinary methodologies based on machine learning theory, with a focus on the way these methods allow the practical implementation of neuromorphic technologies in real-world, human-focused activities. Among the key discoveries are: i) Recent advances in binary deep networks and approximate gradient descent learning match the needs of neuromorphic hardware astonishingly well. ii) Neuromorphic technologies exceed traditional computing systems in terms of real-time adaptability and independence. iii) The field faces challenges related to memory technologies, exacerbated by a historical emphasis on bottom-up approaches. These challenges obstruct significant breakthroughs in the field. Based on these findings, the authors propose creating a neuromorphic learning framework that is specially adapted to the spatial and temporal restrictions of neuromorphic substrates. A framework like this will serve as a guide for the co-design of hardware and algorithms, making it easier to deploy neuromorphic hardware for proactive learning from real-world data.

Hardware implementations of spiking neurons offer significant versatility across diverse applications. The selection of specific circuitry solutions for silicon neuron implementation is contingent upon the unique demands of each application. **Indiveri et al. [15]** encapsulates prevalent building blocks and methodologies employed in constructing these circuits. It provides a comprehensive overview of neuromorphic silicon neurons, encompassing a diverse array of computational models that span from highly detailed Hodgkin-Huxley models to more simplified two-dimensional generalized adaptive integrate-and-fire models. The authors investigate the various design approaches utilized for every silicon neuron type and illustrate their utility using empirical data obtained from a broad collection of manufactured VLSI circuits. Reservoir computing, a pioneering concept within the field of machine learning that

surpasses that of traditional von Neumann computing systems. **Li et al. [16]** presents an exploration of the delayed feedback system, a reservoir computing architecture, and its application in the context of anomaly detection. The authors delve into the intricate design of the three pivotal components within the delayed feedback system and scrutinize their energy efficiency performance. Furthermore, they elucidate how the reservoir computing architecture can be employed for anomaly detection within a smart grid network.

Many current hardware spiking neural networks (SNNs) implementations utilize simplified neuron and synapse models, neglecting the crucial aspects of synapse dynamics required for tasks involving temporal patterns. **Fang et al. [17]** suggests the utilization of an FPGA-based Spiking Neural Network (SNN) that employs biologically inspired neurons and synapses, specifically tailored for temporal data processing. This approach aims to overcome the mentioned limitation and facilitate the integration of more realistic synaptic models into neuromorphic systems. The authors offer a method for converting continuous real-valued data into sparse spike events. Additionally, they offer an event-based realization of the synapse dynamic model and its optimized hardware structure, designed to make the most of sparse characteristics. In reference, **Zenke et al.[18]** , they establish a mathematical basis for creating efficient online learning algorithms tailored for neuromorphic devices. The authors notably establish a direct connection between Real-Time Recurrent Learning (RTRL), which is an online gradient computation method used in traditional Recurrent Neural Networks (RNNs), and biologically plausible learning principles applied in the training of Spiking Neural Networks (SNNs). They additionally provide a sparse approximation method that relies on block-diagonal Jacobians, reducing computational expenses, obviating the requirement for non-local information, and demonstrating enhanced learning performance in practical experiments. Consequently, their framework effectively connects synaptic plasticity and gradient-based techniques in deep learning, paving the way for robust information processing capabilities in future neuromorphic hardware devices

Brown et al. [19] sheds light on recent endeavors aimed at fostering a strong connection between the machine learning and nanoscience communities. It delves into three key facets of their interaction: (1) the utilization of machine learning to analyze and glean fresh insights from extensive nanoscience datasets, (2) the application of machine learning to expedite material discovery, with a specific focus on employing active learning strategies to guide experimental design, and (3) the exploration of nanoscience principles underlying memristive devices, which hold the promise of tailoring hardware solutions customized for machine learning applications.

In conclusion, the authors underscore the challenges and prospects that lie ahead in fostering continued collaboration between nanoscience and machine learning researchers, emphasizing the exciting potential for future breakthroughs in both fields. **Yang et al. [20]** delves deep into the foundational structure and operational concepts of neurons and synapses within the biological nervous system. It then provides a comprehensive survey of the progression of neuromorphic hardware systems, encompassing synthetic synapses and neurons, alongside spike-based neuromorphic computer platforms. The authors' goal is to offer novel insights into the advancement of brain-inspired computing

This review of the literature covers an extensive range of subjects in the realm of neuromorphic computing. It explores the integration of physics principles and nanoscale materials into neuromorphic computing, the emergence of large-scale projects in this field, the use of hardware like Loihi and non-volatile memory for energy-efficient computation, the application of photonics in artificial intelligence, online learning algorithms tailored for neuromorphic substrates, advancements in artificial synapses, interdisciplinary approaches in machine learning and neuromorphic hardware, and the implementation of spiking neurons in silicon circuits. Each of these articles contributes to our understanding of the evolving landscape of neuromorphic computing, highlighting its potential to revolutionize computing paradigms through innovative hardware and algorithms while addressing challenges related to energy efficiency, real-time processing, and biological fidelity. Table 2.1 presents the summary of literature review for neuromorphic computing.

Table-2.1. Summarization of literature review for neuromorphic computing

Author	Technique	Problem Statement	Performance Analysis	Limitations
Marković et al. [1]	Physics for neuromorphic computing	Incorporating physics into neuromorphic computing, use of nanoscale materials	Augmenting computational capabilities, low-power chips	Prospective pathways not detailed
Furber et al. [2]	Large-scale neuromorphic computing systems	Scaling neuromorphic projects, understanding brain processing	Examining large-scale projects, advantages, limitations	Specific project details not provided
Davies et al. [3]	Advancing neuromorphic computing with Loihi	Exploring Loihi results, brain-inspired network architectures	Reduction in latency and energy consumption	Limited focus on conventional deep learning
van De Burgt et al. [4]	Organic electronics for neuromorphic computing	Advancements in organic neuromorphic devices	Low-energy switching, tunability,	Challenges in miniaturization and speed

			integration into arrays	
Roy et al. [5]	Towards spike-based machine intelligence with neuromorphic computing	Progress in neuromorphic computing, learning mechanisms	Challenges and potential future trajectories	Focus only on algorithmic and hardware co-design
Burr et al. [6]	Neuromorphic computing using non-volatile memory	Utilization of non-volatile memory in neuromorphic systems	Advancements in power efficiency, device types	Focuses on NVM devices and does not cover other neuromorphic hardware.
Shastri et al. [7]	Photonics for artificial intelligence and neuromorphic computing	Integration of photonics in neuromorphic systems	Low latency, sub-nanosecond processing	Challenges and breakthroughs in photonics
Esser et al. [8]	Backpropagation for energy-efficient neuromorphic computing	Bridging the gap between backpropagation and neuromorphic hardware	High accuracy at a low energy cost	Disparities between continuous and spiking neurons
Shi et al. [9]	Development of a neuromorphic computing system	Brain-inspired computing system design	Introduction of 'Tianji' neuromorphic chip	Universally accepted solutions elusive
Marković et al. [10]	Quantum neuromorphic computing	Application of quantum hardware for neural network computation	Strategies for quantum neuromorphic networks	Various quantum neuromorphic implementation
Thiem et al. [11]	Foundations of neuromorphic computing	Advancements in hardware and software for neuromorphic computing	Mathematical models, algorithms, and neuroprocessors	Enhancement of cognitive capabilities
Zenke et al. [12]	Brain-inspired learning on neuromorphic substrates	Online learning algorithms for neuromorphic substrates	Real-time adaptability, autonomy, and challenges	Bridging the gap between synaptic plasticity and gradient-based approaches
Li et al. [13]	Artificial synapses enabled neuromorphic computing	Nanomaterial-based synaptic devices	Improved carrier dynamics, photon interaction, hardware neural networks	Engineering challenges in device design
Neftci et al. [14]	Data and power-efficient intelligence with neuromorphic learning machines	Machine learning approaches for neuromorphic hardware	Advantages of neuromorphic technologies, challenges	Memory technology and bottom-up approach challenges
Indiveri et al. [15]	Neuromorphic silicon neuron circuits	Silicon neuron circuitry for spiking neural networks	Computational models, design approaches, silicon neurons	Versatile applications but circuit-specific
Fang, Haowen, et al. [17]	An event-driven neuromorphic system with biologically plausible temporal dynamics	Processing time-based data on resource-constrained embedded devices	10-fold increase in processing speed and 196-fold improvement in energy efficiency	Neglects some aspects of synapse dynamics in current hardware SNN models.
Zenke, Friedemann, et al. [18]	Online learning algorithms for	Training spiking neural networks for practical use in	A bridge between synaptic plasticity and gradient-based	The offline nature of training and non-local computations

	neuromorphic hardware	neuromorphic hardware	approaches in deep learning	in gradient-based learning algorithms pose challenges.
Brown, Keith A., Sarah, et al. [19]	Machine learning in nanoscience	Leveraging machine learning in nanoscience and its role in neuromorphic hardware	Highlights the use of machine learning in analyzing nanoscience datasets and guiding experimental design.	Challenges and prospects in fostering collaboration between nanoscience and machine learning researchers.

2.3 Cyber-Physical Systems Integration

The combination of digital computers, communication technologies, and physical processes in the twenty-first century has resulted in a fundamental shift in how humans interact with the physical world. This confluence gave rise to the subject of Cyber-Physical Systems Integration (CPSI), a dynamic and multidisciplinary sector that is redefining technological and technical limits.

CPSI encompasses the fusion of cyber, representing the digital and computational components, with physical, representing the real-world processes, to create systems that are capable of perceiving, analyzing, and acting upon their environment in real-time. At its core, CPSI seeks to bridge the gap between the virtual and physical realms, leading to a myriad of transformative applications across industries such as healthcare, transportation, manufacturing, and infrastructure. Figure 2.2 shows the 5C architecture of the cyber physical system.

This literature survey is designed to provide an in-depth exploration of the key facets of CPSI, shedding light on the foundational concepts, cutting-edge developments, and emerging trends in this dynamic field.

Sztipanovits et al. [21] presents a unique composition theory optimised for heterogeneous systems, with a particular emphasis on stability. More specifically, it offers a passivity-based technique for disentangling stability from the uncertainty provided by network and computation time. It also covers cross-domain abstractions, which offer beneficial options for entirely automated software synthesis based on models and high-fidelity performance analysis. The design goals of coordinating groups of interconnected unmanned aerial vehicles (UAVs) and developing high-confidence embedded control software for a quadrotor UAV demonstrate the practical applications of these principles. **Jirkovský et al. [22]** delves into various forms of heterogeneity, with a particular emphasis on semantic heterogeneity. The integration challenge of CPSs is dissected into two distinct hurdles. The authors then present a concept and

implementation plan for decreasing semantic heterogeneity, with a particular emphasis on exploiting Semantic Web technologies for successful data integration. Additionally, they explore the utilization of Big Data methodologies to support the implementation process. Lastly, the authors showcase a potential solution by applying these concepts to their proposed semantic Big Data historian.

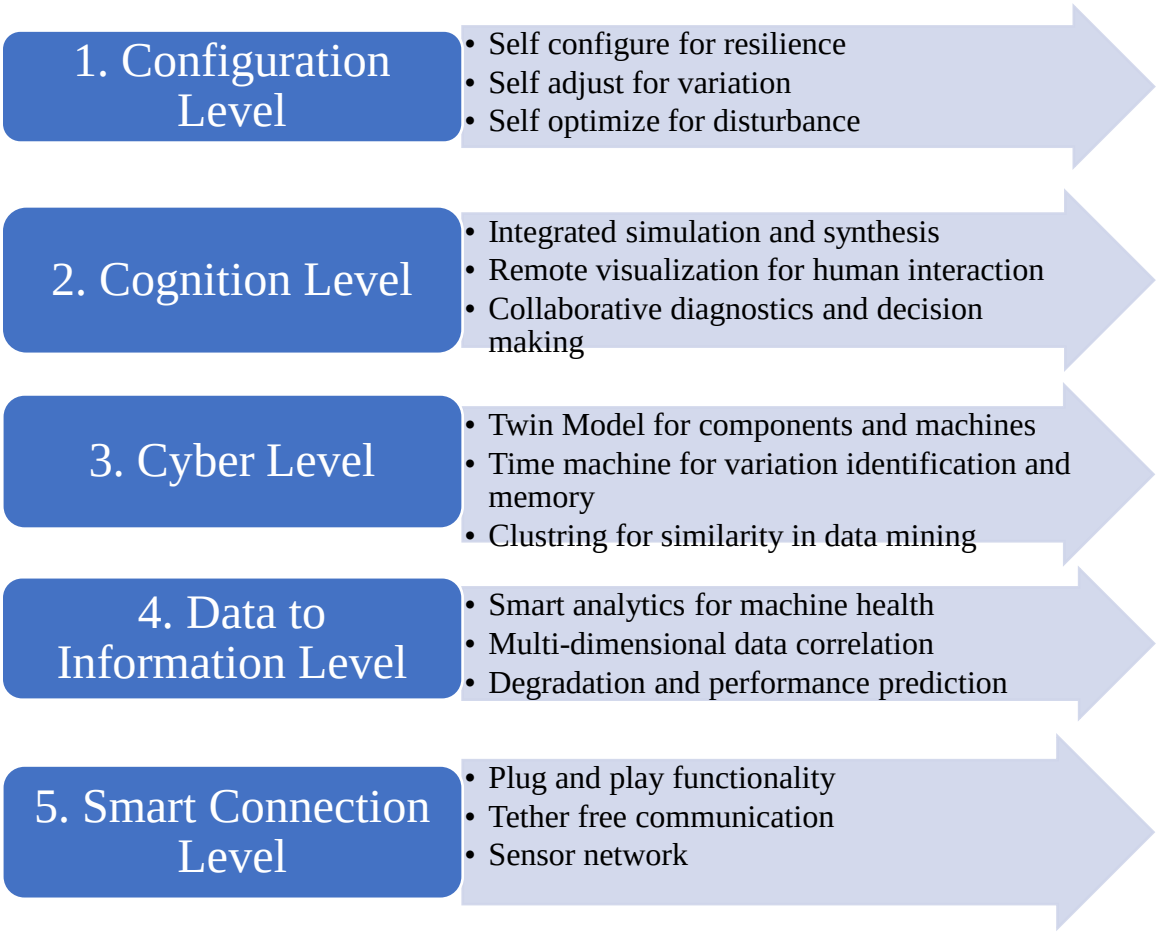


Figure. 2.2. The 5C architecture of Cyber Physical Systems

Khujamatov et al. [23] investigates the combination of IoT, IIoT, and CPS. The authors examine the Industrial Revolution and Industry 4.0 in depth, shedding light on the emergence and usefulness of IoT, IIoT, and cyber-physical systems in the construction of smart environments. Their exploration encompasses the historical origins, developmental trends, definitions, architectural frameworks, constituent elements, applications, and defining characteristics. Furthermore, they undertake a comparative examination of IoT, IIoT, and cyber-physical systems, considering their origins, applications, architectural attributes, distinctive features, and the extent of integration among them. **Hehenberger et al. [24]** aims to offer an overview of various system types and their transition from mechatronics to CPS and cloud-based (IoT) systems. Additionally, the authors emphasize the necessity for CPS design

methodologies to be an integral part of a multidisciplinary development process. They also address challenges associated with CPS design, examining them from the perspectives of physical processes, computation, and integration.

Singh et al.[25] explores the latest advancements in technology and phases like digital twins, big data analysis, artificial intelligence, and the Internet of Things. The authors examine challenges in research, with a particular emphasis on issues related to data reliability, quality, privacy, accessibility, flexibility, manipulation, trustworthiness, monitoring, and governance. They also suggest possible study topics that will need significant effort. They also provide insights into future study areas for academics working in the subject of smart industry, helping to progress the industrial sector and agile management. The integration of digital and physical components within a network framework, achieved through CPSs, is essential for driving advancements in industrial systems in the future. Multi agent systems are similar to CPSs in that they provide a range of features that can improve CPSs' ability to manage complexity, decentralisation, intelligence, versatility, adaptability, resilience, adaptability, and responsiveness. **Leitao et al. [26]** delves into the current landscape of agent technology's industrial applications within CPSs, shedding light on how agents can effectively address emerging challenges in the realm of CPSs.

Liu et al. [27] introduces CPS by outlining its key principles and distinguishing characteristics, as well as providing a review of the present state of CPS research. Furthermore, the authors delve into the CPS development trajectory, examining system modeling, information processing techniques, and software design considerations. Finally, they scrutinize the primary obstacles and pivotal research areas within the realm of CPS advancement. The President's Council of Advisors on Science and Technology (PCAST) has designated CPS as a field of great importance for government research funding. **Sha et al. [28]** explores the inherent difficulties and potential advantages connected with CPS.Furthermore, it highlights specific challenges and prospects within the realm of sensor networks, ubiquitous computing, and trustworthy computing, as relevant to the field.

Mosterman et al. [29] examines critical facilitators of CPS. It delves into the requirements and difficulties associated with designing and managing CPS, while also exploring the technologies designed to tackle these challenges and their potential impact. Their objective is to contribute to the development of a research framework centered on model-based approaches, encompassing design methodologies, implementation technologies, and organizational considerations, all essential for bringing next-generation systems into operation. **Colombo et**

al. [30] delineates the concept of cloud-centric industrial CPS and delves into the initial outcomes of its deployment within the framework of Next Generation Service-Oriented Architecture (SOA)-centered Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) platforms. The writers provide insights into the research, development, and innovation activities of a group of professionals working together on the IMC-AESOP project. These tasks revolve around the creation, construction, execution, and validation of the fundamental features of Intelligent Monitoring and Control Systems, along with the advantages they offer in diverse industrial process control scenarios.

Commencing with an explanation of CPS, **Sanislav et al. [31]** explores the necessity for deploying these systems across diverse application fields, along with the research hurdles involved in establishing a suitable framework that goes beyond merely encompassing networking and information technology. The objective is to seamlessly incorporate information and knowledge into tangible, physical objects. As CPSs are expected to have a substantial impact on the creation and advancement of forthcoming engineering systems, the authors also offer a concise summary of the key research areas within CPS, including generic architecture, design principles, modeling, dependability, and implementation. Due to the significant progress made in CPS technologies in recent years, there is an urgent requirement for the development of enhanced security and trust mechanisms. These mechanisms are essential for mitigating security breaches and addressing privacy vulnerabilities in the various interconnected components of CPS.

Konstantinou et al. [32] concentrates on evaluating security and privacy issues at varying levels of system integration and introduces comprehensive solutions to improve the reliability and dependability of contemporary cyber-physical systems. **Derler et al. [33]** delves into the complexities associated modeling CPSs, which stem from their inherent diversity, simultaneous operation, and susceptibility to timing issues. It employs a section of the airplane's vehicle management system (VMS), specifically focusing on the fuel management subsystem, to illustrate these issues. Furthermore, the authors explore various technologies that offer partial solutions to these difficulties. These technologies include the modeling and simulation of hybrid systems, the use of concurrent and heterogeneous models of computation, incorporating domain-specific ontologies to improve modularity, and comprehensive modeling of both functionality and implementation architectures.

Shi et al. [34] endeavors to enhance comprehension of CPS. At first, the unique characteristics of Cyber-Physical Systems (CPSs) are outlined, and research progress is consolidated across

different aspects, including energy supervision, security, communication, control techniques, resource distribution, and the creation of software through model-driven methods. Subsequently, three paradigmatic applications are presented to underscore the promising prospects within CPSs. Ultimately, the authors succinctly outline the research challenges and offer suggestions for future endeavors.

Monostori et al. [35] underscores the strong foundation, particularly within the CIRP community, that points toward the significance of Cyber-physical production systems (CPPS). The authors also outline the research expectations and practical implementations of CPS and CPPS, offering insights through the introduction of case studies. Additionally, they shed light on the emerging research and development challenges associated with this transformative field. **Törngren et al. [36]** delves into the domain of CPS, where the integration of computation, networking, and physical processes leads to the creation of autonomous, intelligent, interconnected, and cooperative products When integrated into Cyber-Physical Systems of Systems (CPSoS), these systems provide extraordinary capabilities while also bringing about remarkable technological complexities. The authors aim to enhance comprehension, awareness, and strategies for managing this growing complexity. They promote the development of fresh theoretical underpinnings, insights, and approaches to tackle this problem. Additionally, they explore the origins and outcomes of complexity, scrutinizing both overarching aspects and those particular to CPS.

Cyber-physical systems represent a transformative technological advancement with far-reaching ramifications across various sectors, significantly influencing economic dynamics and societal paradigms. **Serpanoset al. [37]** discusses their deployment in diverse fields, spanning from manufacturing and agriculture to critical infrastructure and assisted living, and introduces multifaceted challenges encompassing technological, commercial, legal, and ethical dimensions. **Kure et al. [38]** introduces a comprehensive framework for managing cybersecurity risks in CPS proactively. The author's approach aligns with established risk management practices and standards, encompassing risks from stakeholder perspectives and the interplay between cyber and physical system components, as well as their dependencies. They also provide a cybersecurity assault scenario that takes into consideration the cascading impact of attacks and exposures on these resources. This assault model can help you determine suitable risk levels and devise mitigation techniques. The authors illustrate the practical application of their framework using a power grid system as a case study.

Anumba et al. [39] outlines a particular project with the goal of streamlining the immediate validation process between digital models and actual construction. This paper advocates the efficient integration of diverse computational tools, including wireless sensors, virtual prototyping, real-time tracking, and data fusion, into both the phases of design and construction. It also outlines methods for ensuring that bidirectional consistency between virtual models and the actual facility is maintained, a factor that is sometimes disregarded once physical construction commences. Furthermore, the authors investigate the possibilities of using a CPS approach to instill greater intelligence as well as sustainability into the building process, emphasising the important benefits this method may provide. The forthcoming years are poised to witness significant transformations within the electricity sector, particularly in the grid infrastructure, which has remained relatively unchanged for nearly a century. **Karnouskos et al. [40]** discusses that the emerging SmartGrid represents a paradigm shift driven by the essential role of interactions, underpinned by robust integration of IT technologies across multiple layers for monitoring and control purposes. CPS assumes an integral role within the SmartGrid, necessitating the effective resolution of several outstanding challenges.

Lee et al. [41] analyses the inherent design issues of CPS and poses a crucial question concerning the viability of present computer and networking technologies as a basis for CPS. The authors conclude that enhancing design processes, elevating abstraction levels, or formally verifying designs within the existing abstractions will not suffice. To fully harness the potential of CPS, it is imperative to reconstruct computing and networking abstractions to incorporate both physical dynamics and computation in a unified manner.

Alguliyev et al. [42] aims to offer a complete evaluation and classification of existing research articles on cyber-physical system security. The authors elucidate the fundamental operational principles underlying cyber-physical systems. They further scrutinize the primary types of attacks and threats targeting cyber-physical systems, presenting a structured hierarchy of such attacks. Lastly, they offer insights into potential future avenues for exploration in this critical domain. **Rajkumar et al. [43]** discusses the development, assembly, and validation of CPS entail a range of intricate technical obstacles necessitating collaborative efforts from interdisciplinary researchers and educators. In **Cardenas et al. [44]**, the authors explore three primary challenges associated with enhancing the security of cyber-physical systems. These challenges encompass: i) Gaining insight into the various threats and potential repercussions resulting from attacks on cyber-physical systems. ii) Identifying the unique characteristics of CPS and emphasising how they differ from traditional IT security paradigms. iii) Examining

security mechanisms that are relevant and applicable to safeguarding cyber-physical systems, with a particular focus on prevention, detection, recovery, as well as resilience and deterrence strategies against cyberattacks.

Humayed et al. [45] undertakes a thorough examination and classification of existing CPS security research through the lens of a unified framework. This framework is organized along three distinct dimensions: Firstly, it aligns with established security classifications, encompassing threats, vulnerabilities, attacks, and safeguards. Secondly, it scrutinizes CPS components, categorizing them into the realms of cyber, physical, and cyber-physical components. Finally, it studies CPS systems from both a generic and specialised, representative standpoint, like smart electrical grids, medical CPS, and smart automobiles. The incorporation of security measures into the architecture of CPS necessitates consideration of multiple inherent attributes. These attributes encompass the fusion of the digital and tangible domains, decentralized oversight and control, unpredictability, immediate guidance, and a widespread geographical presence.

Kim et al. [46] offers a comprehensive examination of research in the field of CPS, covering its historical evolution and investigating recent discoveries in domains such as networked control, hybrid systems, real-time computing, real-time networking, wireless sensor networks, security, and model-driven development. The authors also underscore the transformative potential of CPSs within numerous vital societal applications. In **Wan et al. [47]** , the authors undertake a thorough examination of cutting-edge design methodologies from various perspectives. Their primary objective is to enhance comprehension of this evolving multidisciplinary approach. They define CPS characteristics and assess research advances via the prisms of energy management, security of network data transfer and managing, model-based design, control approaches, and system resource allocation. They also demonstrate the promise of CPSs by presenting traditional applications such as the integration of intelligent traffic systems with unmanned vehicles.

Neuman et al. [48] dives into these features and recommends for a design technique that incorporates security into the core system structure. Additionally, it outlines a research roadmap that pinpoints essential components required to facilitate the implementation of this approach. To refine and gain a more precise understanding of CPS, **Gunes et al. [49]** offers an extensive survey of relevant literature. It delves into the origins of CPS, its connections to various research domains, prevailing concepts, and practical implementations. Furthermore, the authors highlight a wide range of technical issues and use specific applications to elaborate

on and give insights into each topic. Computation, communication, control, and physical aspects are all interwoven within CPS. However, there is a noticeable gap in the literature in terms of a comprehensive review of CPS research. As a result, **Chen et al. [50]** intends to fill this vacuum by undertaking an exhaustive literature analysis on CPS applications, concentrating on publications published in the Scopus database between 2012 and 2017. The research categorizes and reviews papers that explore various CPS applications, summarizing their key findings. Additionally, the authors outline the challenges and emerging trends in CPS research. **Yaacoub et al. [51]** conducts a comprehensive survey of key CPS aspects, their associated applications, technologies, and standards. Furthermore, it delves into the vulnerabilities, threats, and attacks pertaining to CPS security, while identifying primary issues and challenges. Additionally, the existing security measures are evaluated, highlighting their principal limitations. The authors put forth several suggestions and recommendations

The literature survey explores the evolving field of cyber-physical systems (CPS) integration, highlighting its significance in various domains, such as manufacturing, industrial automation, smart environments, and critical infrastructure. It emphasizes the need for comprehensive modeling, precision, and predictability in CPS integration, discussing challenges related to system heterogeneity, security, data management, and complexity. The survey also underscores the practical applications of CPS, including coordinated unmanned vehicle networks and intelligent manufacturing, while acknowledging open research challenges in areas like safety and performance guarantees. Overall, it emphasizes the growing importance of CPS integration and its transformative potential across diverse sectors, urging the development of new methodologies and approaches to address emerging complexities and opportunities. Table 2.2 presents summary of literature review for Cyber Physical Systems Integration.

Table-2.2. Summarization of literature review for Cyber Physical Systems Integration

Author	Technique	Problem Statement	Performance Analysis	Limitations
Sztipanovits, Janos, et al. [21]	Theory of composition for heterogeneous systems	The integration of systems in cyber-physical systems (CPS) is overlooked, complex, and lacks scientific recognition.	Passivity-based approach for stability and cross-domain abstractions.	Open challenges in expanding compositional design theory beyond stability.
Jirkovský, Václav, et al. [22]	Reducing semantic heterogeneity	Industry 4.0 adoption introduces heterogeneity in CPS integration.	Leveraging Semantic Web and Big Data methodologies for data integration.	Focused on semantic heterogeneity, other integration challenges are not covered.

Khujamatov, Halim, et al. [23]	Integration of IoT, IIoT, and CPS	IoT, IIoT, and CPS integration in the context of Industry 4.0 and smart environments.	Comparative examination of IoT, IIoT, and CPS with a focus on integration.	Challenges in control, network infrastructure, computation, and security were discussed.
Hehenberger, Peter, et al. [24]	CPS design methodologies	Cost and time reduction in CPS development and seamless integration of components.	Case studies on CPS design challenges and system levels.	Emphasis on design challenges, limited discussion of other aspects of integration.
Singh, Harpreet et al. [25]	Big Data and Industry 4.0 integration	Integration of big data, Industry 4.0, and cyber-physical systems in smart industry.	Challenges in data integrity, privacy, scalability, and governance.	Primarily focuses on big data challenges and smart industry, not comprehensive CPS integration.
Leitao, Paulo, et al. [26]	Multiagent systems in CPS	Enhancement of CPS with multiagent systems for complexity management.	Discusses the application of agents in CPS for complexity management.	Focuses mainly on the role of agents and complexity management, not broader integration challenges.
Liu, Yang, et al. [27]	Introduction to CPS	Introduction to CPS, system modeling, information processing, and software design considerations.	Overview of core CPS concepts, research, and key challenges.	General introduction to CPS without in-depth analysis of integration issues.
Sha, Lui, et al. [28]	Challenges and prospects in CPS	Challenges and opportunities in sensor networks, ubiquitous computing, and trustworthy computing in CPS.	Highlights challenges and prospects in sensor networks and trustworthy computing.	Specific to sensor networks and trustworthy computing, not comprehensive CPS integration.
Mosterman, Pieter J., et al. [29]	Collaborating embedded software systems	Challenges and technologies for system integration, particularly in the operational phase for deployed systems.	Discusses facilitators of system integration and requirements for CPS.	Focuses on the challenges of system integration, particularly in the operational phase, not comprehensive CPS integration.
Colombo, Armando W., et al. [30]	Cloud-based industrial CPS	Introduction of cloud-based industrial CPS and its benefits in industrial process control environments.	Overview of research and development efforts in intelligent monitoring and control systems.	Focused on cloud-based industrial CPS and specific applications, not broader CPS integration challenges.
Sanislav, Teodora et al. [31]	CPS concept and research areas	Definition of CPS, need for implementation, and research areas in CPS.	Overview of CPS research areas, including architecture, modeling, and dependability.	Provides a general overview of CPS and research areas but lacks an in-depth analysis of integration challenges.

Konstantinou, Charalambos, et al. [32]	CPS security	Evaluation of security and privacy issues in CPS at different integration levels.	Introduces solutions to enhance security and trust in cyber-physical systems.	Focuses on security and privacy in CPS, not a comprehensive analysis of broader integration challenges.
Derler, Patricia, et al. [33]	Modeling CPS	Challenges in modeling CPS and technologies to address them.	Explores technologies like hybrid system modeling, concurrent models, and ontologies.	Focuses on modeling challenges in CPS, not a comprehensive analysis of integration issues.
Shi, Jianhua, et al. [34]	Survey of CPS	Overview of CPS, research advancements, and research challenges.	Covers various dimensions of CPS research, including energy management and security.	Provides a broad survey of CPS, but not an in-depth analysis of integration challenges.
Monostori, László, et al. [35]	CPS in manufacturing	Significance of CPS and CPPS in manufacturing, research expectations, and case studies.	Discusses research and development of CPS and CPPS in manufacturing.	Focused on manufacturing and case studies, not a comprehensive analysis of broader CPS integration challenges.
Törngren, Martin, et al. [36]	Managing CPS complexity	Strategies for managing complexity in Cyber-Physical Systems of Systems (CPSoS).	Highlights the need for awareness, research, and organizational strategies.	Focused on complexity management in CPSoS, not comprehensive analysis of broader CPS integration challenges.
Serpanos, Dimitrios et al. [37]	CPS revolution	Discussion of the transformative impact of CPS on various sectors and associated challenges.	Addresses technological, commercial, legal, and ethical dimensions of CPS.	Provides an overview of CPS impact and challenges but lacks a detailed analysis of integration issues.
Kure, Halima Ibrahim, et al. [38]	Cybersecurity risk management in CPS	Framework for managing cybersecurity risks in CPS, with a focus on critical infrastructure.	The framework addresses risk from stakeholder perspectives, attack scenarios, and mitigation strategies.	Emphasis on cybersecurity risk management, not a comprehensive analysis of broader CPS integration challenges.
Anumba, Chimay J., et al. [39]	Cyber-physical systems in construction	Integration of computational tools for real-time validation between virtual models and physical construction.	Strategies to maintain consistency between virtual models and physical construction.	Specific to construction and focuses on real-time validation, not comprehensive CPS integration analysis.
Karnouskos, Stamatis et al. [40]	CPS in the SmartGrid	Discussion of SmartGrid and the role of CPS in real-	Emphasizes the role of CPS in SmartGrid	Specific to SmartGrid and the role of CPS, not

		time data monitoring and control.	and its potential impact.	comprehensive analysis of broader CPS integration challenges.
Lee, Edward A. et al [41]	Design Challenges	Challenges in designing Cyber-Physical Systems (CPS) that incorporate physical processes and computing.	Examines the challenges but does not provide performance analysis.	Calls for a need to reconstruct computing and networking abstractions for CPS.
Alguliyev, Rasim, et al [42]	Security Issues	Addresses security challenges in CPS and explores various facets of human life influenced by CPS.	Provides insights into security challenges and categorizes attacks.	Focuses on security aspects, and does not provide a broader perspective on CPS.
Rajkumar, Ragunathan, Insup Lee, et al [43]	Computing Revolution	Discusses the potential of CPS to revolutionize various sectors and highlights technical obstacles in development.	Discusses challenges in CPS development, but no specific performance analysis.	Emphasizes challenges but does not delve deep into technical details.
Cardenas, Alvaro, Bruno et al [44]	Security Challenges	Explores challenges in securing CPS and examines security mechanisms and strategies against cyberattacks.	Analyzes security challenges and mechanisms.	Primarily focuses on security, and does not provide a comprehensive overview of CPS.
Humayed, Abdulmalik, , F et al [45]	Security Survey	Conducts a comprehensive survey of CPS security research, classifying it based on various dimensions.	Provides a detailed classification of CPS security research.	Specialized in security, may not cover broader CPS topics in depth.
Kim, Kyoung-Dae, et al [46]	Research Overview	Offers an overview of CPS research, historical progression, and contemporary findings in various CPS areas.	Provides insights into different CPS research areas.	Focuses on research overview, may not delve deep into specific technical details.
Wan, Jiafu, , Hui Suo et al [47]	Design Methodologies	Examines design methodologies for CPS, including energy management, network security, and system resource optimization.	Proposes a model for optimizing system performance in CPS.	Primarily focused on design methodologies, may not cover a wide range of CPS topics.
Neuman, Clifford, et al [48]	Security Attributes	Explores security attributes unique to CPS and advocates for integrating security into the fundamental system structure.	Advocates a design methodology for CPS security.	Concentrates on security attributes, may not provide a comprehensive CPS overview.
Gunes, Volkan, et al [49]	Concepts and Challenges	Surveys CPS literature, delving	Identifies technical challenges and	Offers an overview but may

		into its origins, concepts, challenges, and practical implementations.	provides insights into various CPS concepts.	not go into deep technical details of specific CPS areas.
Chen, Hong, et al [50]	Literature Review	Conducts a literature review of CPS applications, categorizes papers, summarizes findings, and outlines emerging trends.	Summarizes key findings and challenges in CPS applications.	Focused on the literature review, may not provide a deep technical insight into CPS.
Yaacoub, Jean-Paul A.,et al [51]	Security Limitations	Addresses security challenges in CPS and explores vulnerabilities, threats, and limitations of existing security measures.	Evaluate existing security measures and highlight their limitations.	Concentrates on security aspects, may not cover a comprehensive view of CPS.

2.4 Cyber-Physical Systems and Industry 4.0

The convergence of CPS with the fourth industrial revolution, informally referred to as "Industry 4.0," has ushered in a revolutionary time of industrial engineering and technological innovation and productivity growth. This interdisciplinary field represents the amalgamation of digital intelligence, physical processes, and advanced connectivity, revolutionizing the way industries operate, automate, and optimize their processes. As we move further into the digital age, understanding the intricate interplay between CPS and Industry 4.0 becomes paramount for driving forward economic growth, sustainability, and technological competitiveness.

This section looks at the link between CPS and Industry 4.0, highlighting how CPS technologies and concepts are employed to help achieve the objective of Industry 4.0. Among the popular topics are smart manufacturing, the Internet of Things (IoT), and data-driven decision-making.

The current era is undergoing the fourth wave of Industrial Revolution, and is marked by the expansion of CPS. These systems, which blend industrial automation with network connectivity and cyber integration, are ushering in a wave of innovative functionalities that are profoundly reshaping our daily existence. It is vital to realise that Industry 4.0 introduces new challenges, particularly in the creation of CPS, as well as their reliability, safety, and data security. Against this context, **Jazdi et al. [52]** provides a quick introduction of Industry 4.0 before demonstrating a prototype application that highlights its key features.

CPS systems offer complete information monitoring and synchronisation across the actual manufacturing floor as well as the cyber computational domain. Moreover, the utilization of advanced information analysis allows interconnected machines to operate with increased efficiency, cooperation, and robustness. This transformational trend ushers in the next generation of production, known colloquially as Industry 4.0. At this nascent phase of development, there is a critical necessity for a precise definition of CPS. **Lee et al. [53]** fulfills this need by introducing a cohesive 5-tier framework that could serve as a viable basis for implementing CPS.

CPS has laid a strong groundwork for advancing industrial systems and applications, enabling the integration of new functionalities via the IoT and Web of Things (WoT). This transformational trend ushers in the next generation of production, known colloquially as Industry 4.0. At this nascent phase of development, there is a critical necessity for a precise description of CPS. Addressing this need, **Lu et al. [54]** fulfills the requirement by introducing a cohesive 5-tier structure as a practical basis for implementing CPS. The fundamental technologies driving Industry 4.0 encompass the IoT, cloud computing, machine-to-machine (M2M) communications, 3D printing, and Big Data. Among these, Big Data analytics holds particular significance within CPS, digital manufacturing, and the broader landscape of Industry 4.0. **Wang et al. [55]** delineates the advancements in CPS, digital manufacturing, and Industry 4.0, alongside the fundamental challenges and potential areas for future research within these fields.

Jiang et al. [56] introduces an innovative framework called the 8C architecture, which builds upon the 5C design by incorporating three additional elements: coalition, consumer, and content. This expanded model offers a comprehensive structure for creating CPS tailored for smart manufacturing. The authors also present a case study in which a smart industrial CPS is built and developed using the 8C architecture to demonstrate its practical usefulness. **Bagheri et al. [57]** introduces a comprehensive framework for integrating cyber-physical systems into manufacturing processes. It also investigates adaptive clustering as a sophisticated analytical methodology for networked systems. It also delves into a case study showcasing the integration of self-aware machines through cyber-physical system implementation.

Zhou et al. [58] outlines five important trends anticipated to influence the future of manufacturing. Additionally, the authors examine the associated technologies linked to Industry 4.0, specifically emphasizing the crucial role of Cyber-Physical Systems (CPS) within Industry 4.0 manufacturing environments. Adopting a Customer-to-Business (C2B) approach,

they propose a comprehensive Industry 4.0 framework that conceptualizes everything as a service. A crucial prerequisite for achieving smart manufacturing is the integration of cyber-physical systems, a concept increasingly embraced by manufacturers. CPS and digital twins (DTs) have emerged as the preferred methods for achieving this integration. Although CPS and DTs both center around key principles like deep cyber-physical interconnections, real-time engagement, integration within organizations, and extensive collaboration, they diverge in several facets encompassing their origins, developmental pathways, engineering methodologies, cyber-physical mapping, and core elements. To clarify these differences and delve into the interrelationship between CPS and DTs, a comprehensive review and analysis of these technologies is carried out from diverse viewpoints by **Tao et al. [59] .**

Pivoto et al. [60] conducts a comprehensive survey of the primary CPS architecture models found in industrial settings, with a focus on their essential characteristics and associated technologies. It also explores the interconnections between these models, highlighting their objectives, advantages, and potential contributions to the introduction of IIoT within I4.0. It identifies the main technologies currently in use and how they align with the key features of I4.0, particularly the vertical and horizontal integration of industrial processes. The authors lay out the criteria for dealing with present and future difficulties, as well as the limits and limitations in current CPS systems.

Colombo et al. [61] explores the successful implementation of digital transformation in an industrial environment using a digitalization procedure that covers the three aspects outlined in the Reference Architecture Model for Industry 4.0. This implementation is achievable through meeting requirements, enhancing processes, and implementing an Asset Administration Shell. The authors suggest that in dealing with the interplay between social and technological elements, it's crucial to integrate human-focused initiatives in Industry 4.0 within the broader scope of sustainability and the circular economy. Reference **Alohali et al. [62]** introduces a novel Intrusion Detection System (AIMMF-IDS) that employs AI and multiple modes of fusion specifically created for Cyber-Physical Production Systems (CCPS) in Industry 4.0. The suggested framework commences with a dual data pre-processing strategy that includes converting and normalizing data. Furthermore, the authors introduce an ensemble model for multimodal fusion, employing a weighted voting system. This fusion technique incorporates Recurrent Neural Network (RNN), Bi-directional Long Short-Term Memory (Bi-LSTM), and Deep Belief Network (DBN), showcasing the novelty of their approach.

Matsunaga et al. [63] investigates how the adoption of technologies and methodologies can substantially enhance overall process efficiency in terms of energy consumption. It comprises three main phases: an initial systematic review to assess the impact of smart manufacturing and cyber-physical systems on manufacturing energy efficiency, followed by real-time monitoring and simulation experiments to optimize industrial energy usage and reduce waste. **Lee et al. [64]** explores the prospective contributions of blockchain technology in the conception and actualization of real-world CPPSs. The authors present a unified three-tier blockchain architecture as a reference point for researchers and industry practitioners to outline blockchain value, simplifying its integration, development, and alignment with manufacturing breakthroughs in the context of Industry 4.0. In the age of Industry 4.0 and CPS, skilled production workers have frequently been demoted to the role of passive data receivers. The rise of Cyber-Human Systems (CHS) represents a change towards rethinking the role of human workers, particularly those engaging in manual value-added jobs in automobile assembly. To move forward, there is a pressing need for a cohesive framework that integrates CHS and CPS, guiding the implementation of smarter manufacturing systems in the future. **Krugh et al. [65]** highlights the significance of this transition and its potential implications for the automobile production sector.

The Industry 4.0 vision, focused on the combination of major technologies and CPSs, is set to revolutionise the industrial industry significantly. There remains an open question regarding whether this evolution will empower employees with greater decision-making responsibilities or lead to increased technological control. **Fantini et al. [66]** addresses this challenge by presenting a methodology designed to facilitate the planning and evaluation of various work configurations. It takes into account both the distinctive aspects of human labor and the features of cyber-physical production within a comprehensive framework. The methodology encompasses routine production tasks as well as exceptional situations such as fault detection or maintenance interventions, which are particularly relevant to human involvement.

Singh et al. [67] attempts to thoroughly investigate cutting-edge technologies and phases such as digital twins, big data analytics, artificial intelligence, and the IoT. The authors dig into the daunting issues offered by the reliability of data, the quality of data, confidentiality of data, data accessibility, data adaptability, transformation of data, credibility, tracking, and management. It also encapsulates potential research areas that warrant significant scholarly attention. The authors emphasise promising improvements in the layout of horizontal, vertical, as well as end-to-end integration mechanisms as Industry 4.0 merges into socio-technical

systems. **Yan et al. [68]** delves into the concept of intralogistics-oriented CPS, focusing on the development of cyber-space models for shop-floor equipment. A remote management platform has been successfully established using wireless sensors and controllers, allowing for equipment interconnection, logistics scheduling, and remote operation via portable terminals over the Internet. This suggested solution's practicability and efficiency have been carefully tested and confirmed in a real manufacturing workshop setup.

The authors of **Navickas et al. [69]** present a compelling explanation for Industry 4.0's importance, describe CPS, and provide insight into its innovative implications. The authors emphasise the crucial need of continuous research into the integration of CPS into supply chain management, an area that has received little attention in the context of CPS thus far. **Nounou et al. [70]** describes a complete framework for integrating Lean concepts with Industry 4.0. Within this framework, authors develop a Lean-based architecture tailored for Industry 4.0 environments. This architecture enhances connectivity among Industry 4.0 components, facilitating more efficient information exchange and, consequently, improved decision-making capabilities. They further innovated by introducing the idea of 'Smart Value Stream Mapping 4.0' (VSM 4.0) aimed at enhancing the movement of both materials and information. VSM 4.0 leverages Industrial Internet of Things (IIoT) advancements to enable immediate decision-making at every stage of production. Integrating Lean-based Industry 4.0 Architecture with VSM 4.0 enhances the overall efficiency, responsiveness, oversight, and adaptability of the system when encountering unexpected challenges and breakdowns.

Sinha et al. [71] offers a comprehensive examination of CPS within the industrial domain, encompassing essential technologies, managerial competencies, architectural considerations, and anticipated features. The authors also showcase select case studies, highlighting their advantages and associated challenges, along with potential solutions. The merging of CPS and big data, which inherently share a symbiotic relationship, has been relatively underexplored. To demonstrate, cyber-physical systems create massive volumes of data on a regular basis, necessitating the use of big data approaches for processing and improving system expansion, safety, and efficiency. As a result, **Xu et al. [72]** is undertaken to shed light on this crucial intersection, bringing it to the forefront of scholarly attention, and to delineate prospective research avenues towards realizing full autonomy within the realm of Industry 4.0.

Cogliati et al. [73] offers Intelligent CPSs, a game-changing iteration of CPSs that can easily integrate intelligent characteristics like defect prediction, autonomous behavior, and self-adaptation straight into the CPS units. These integrated features are poised to increase CPS

autonomy, reduce bandwidth needs, and enhance energy efficiency, allowing them to satisfy the demanding requirements of Industry 4.0 and other relevant technological contexts, such as the smart Internet-of-Things. **Savtschenko et al. [74]** offers a comprehensive examination of the changes accompanying the rise of CPS and Industry 4.0, highlighting the prerequisites for IT governance methodologies that can facilitate the seamless adoption of CPS. The findings are exemplified through the application of the COBIT 5 IT governance framework. The authors contribute to the accumulation of information within the field and play a role in influencing the development of suitable governance approaches within the framework of Industry 4.0 and the convergence of CPS.

Sinha et al. [75] offers a comprehensive examination of CPS within the industrial domain, covering the necessary technologies, managerial expertise, architectural aspects, and anticipated attributes. Additionally, the authors showcase select case studies, discussing their advantages and associated challenges while proposing potential solutions. Furthermore, the socio-economic impact of the CPS-driven industrial revolution is thoroughly explored in this context. **Abikoye et al. [76]** delves into the impact of IoT and CPS technologies on the advancement and realization of real-world smart manufacturing. The authors propose an integrated framework that combines IoT and CPS as a guideline for both researchers and industries, facilitating the full exploitation of IoT's potential in conjunction with CPS for the advancement of Industry 4.0 intelligent production techniques.

Mosterman et al. [77] primarily addresses the dimension of collaborative functionality and offers a collection of tangible illustrations concerning the challenges faced by CPS. These examples are grounded in the context of a pick-and-place machine designed to solve a distributed variation of the Towers of Hanoi puzzle. The authors operate at the level of computational modeling, with the ultimate goal of contributing to the research agenda centered on model-based approaches for designing methods and implementing technologies that are indispensable for realizing the next generation of systems. **Frontoni et al. [78]** explores the conceptualization, representation, and practical implementation of digital twins, using the manufacturing industry as a real-world case study within a cyber-physical context. Furthermore, the authors introduce a novel CPS architecture designed for real-time visualization of intricate industrial processes, emphasizing the Simulation aspect of Industry 4.0. The outcomes, as observed within an authentic industrial environment, showcase impressive performance in terms of real-time responsiveness, virtual reality, WebGL-based CPS visualization capabilities, usability, and comprehensibility.

Ahmadi et al. [79] proposes an enhancement to the conventional 3C CPS architecture for Industry 4.0 to address these restrictions and overcome the disparity between theoretical concepts and real implementation. Connectors, procedures, and sub-components (e.g., human beings, cyber, and physical factors) are among the primary interface elements included in the proposed framework. The improved 3C CPS architecture is intended to be a critical resource and a viable model for future intelligent manufacturing CPS systems and sectors. **Sbaglia et al. [80]** digs into the fundamental principles of Industry 4.0, with a special emphasis on the function and relevance of CPS in this framework. By delineating its key characteristics and juxtaposing it with the business model of the fourth industrial revolution, which revolves around a service-oriented architecture (SOA), the authors aim to elucidate how CPS contributes to achieving a flexible, modular, and personalized approach to production processes.

Sony et al. [81] aims to create a CPS design utilizing an 8 C architecture framework while integrating Lean Six Sigma (LSS) principles to enhance the overall efficiency of a business system. The authors present a thorough examination of the 8 C architecture and investigate its possible integration with the LSS technique using a complete survey of current material. To include LSS concepts into each stage of the design process, a thorough assessment of the connection, transformation, cyber, reasoning, arrangement, collaboration, consumer, and content levels is performed.

This review of the literature gives a thorough overview of the transformational influence of CPS in the context of Industry 4.0. It emphasises CPS's development as a significant driver of the fourth industrial revolution, bringing in new functions and changing different elements of society and industry. In CPS development, the study emphasises the necessity of addressing issues like as dependability, safety, and data confidentiality. It also explores various architectural models, integration with technologies like IoT and AI, and the role of humans in CPS-enabled smart factories. The poll also looks into the possibilities of CPS for energy conservation, the usage of blockchain, and the incorporation of Lean concepts into Industry 4.0. Overall, it underscores the profound impact and interdisciplinary nature of CPS in the evolving landscape of Industry 4.0. Table 2.3 provides the summary of of literature review for Cyber-Physical Systems and Industry 4.0.

Table-2.3. Summarization of literature review for Cyber-Physical Systems and Industry 4.0

Author	Technique	Problem Statement	Performance Analysis	Limitations
Jazdi, Nasser et al. [52]	Industry 4.0	Challenges in developing	Prototype application	Security and data protection

		cyber-physical systems		
Lee, Jay, Behrad Bagheri et al. [53]	CPS Architecture for Industry 4.0-based Manufacturing	Define CPS	Unified 5-level architecture	Limited focus on other Industry 4.0 aspects beyond CPS.
Jiang, Jehn-Ruey et al. [56]	8C Architecture for Smart Factories	Extending 5C architecture, horizontal integration	Guideline for smart factories	Limited discussion on the broader context of Industry 4.0.
Bagheri, Behrad et al. [57]	CPS Architecture for Self-aware Machines	Integration of advanced analytics, case study	Framework for CPS integration	Focuses on manufacturing CPS, not Industry 4.0 as a whole.
Zhou, Keliang, Liu et al. [58]	Industry 4.0 Framework	Industry 4.0 strategies, CPS in factory settings	Proposed Industry 4.0 framework, case study	Varies by country's strategies
Tao, Fei, Qinglin Qi et al. [59]	Digital Twins and CPS Integration	CPS and Digital Twins comparison	Analysis of CPS and DTs	Differences between CPS and DTs
Pivoto, Diego GS, et al. [60]	CPS Architectures for IIoT in Industry 4.0	Survey of CPS architecture models in industrial settings	Characteristics, technologies, interconnections	Addressing challenges in IIoT and CPS integration
Walter Colombo, et al. [61]	Human-focused Industrial Cyber-Physical Systems	Human-centered approach within Industry 4.0	Asset Administration Shell, human-centric considerations	Consideration of sustainability and the circular economy
Alohali, Manal Abdullah, et al. [62]	AI-enabled Intrusion Detection for CCPS in Industry 4.0	AI-enabled IDS for CCPS in Industry 4.0	Novel AI-enabled IDS, multimodal fusion, performance	Security challenges in CCPS in Industry 4.0
Matsunaga, Fernando, et al. [63]	Energy Efficiency in Smart Manufacturing	Optimization of manufacturing energy usage	Systematic review, real-time monitoring, simulations	Improvements in production planning and cost savings
Lee, Jay et al. [64]	Blockchain-enabled CPS for Industry 4.0	Integration of blockchain in practical CPS settings	Unified blockchain framework, reference point	Effective deployment of CPPS in practical settings
Krugh, Matthew et al. [65]	Cyber-Human Systems in Automotive Manufacturing	Integration of CHS and CPS in automotive assembly	Framework for integrating CHS and CPS	Focuses only on automotive manufacturing context.
Fantini, Paola et al. [66]	Human Activities in CPS within Industry 4.0	Modeling and assessment of human activities	Methodology for work configurations, case studies	Human-centric perspectives, KPIs
Harpreet Singh et al. [67]	Big Data, Industry 4.0, CPS Integration	Integration of technologies in smart industry	Challenges in data management, research areas	Data integrity, data privacy, scalability
Yan et al. [68]	Intralogistics-oriented CPS for Workshop in Industry 4.0	Integration of CPS in shop-floor intralogistics	Cyber-space models, wireless sensors, remote management	Shop-floor logistics management complexity
Navickas et al. [69]	CPS in Industry 4.0	Role of CPS in Industry 4.0	Business models, implications of CPS in supply chain	Limited exploration in supply chain management

Nounou et al. [70]	Lean-based Industry 4.0 Architecture	Integration of Lean principles with Industry 4.0	Lean-based architecture, Smart Value Stream Mapping 4.0	Focuses only on the integration of Lean principles with CPS in Industry 4.0.
Sinha, Devarpita et al. [71]	CPS in Smart Factories within Industry 4.0	Role of CPS in smart factories	Technologies, case studies	Broad overview of CPS and Industry 4.0.
Abikoye, Oluwakemi Christiana, et al. [76]	IoT and CPS Integration	Addressing the challenge of smart interconnection in Industry 4.0 smart manufacturing	Proposes an integrated framework for IoT and CPS integration	Current technologies not fully equipped for the challenge
Mosterman, Pieter J., and Justyna Zander, et al. [77]	CPS Modeling and Challenges	Challenges faced by CPS, illustrated using a pick and place machine	Focuses on computational modeling	Moderate complexity of the pick and place machine
Frontoni, Emanuele, et al. [78]	Digital Twins and CPS Visualization	Implementation of digital twins in manufacturing and real-time CPS visualization	Impressive real-time responsiveness and usability	Focuses on visualization aspects, not all-encompassing
Ahmadi, Ahmadzai, et al. [79]	Enhanced 3C CPS Architecture	Enhancing the traditional 3C CPS architecture for Industry 4.0	Addresses interfacing elements	Lacks extensive performance analysis
Sbaglia, Luca, et al. [80]	Role of CPS in Industry 4.0	Examines the role and significance of CPS in Industry 4.0	Focuses on core tenets of Industry 4.0	Does not provide specific implementation details
Sony, Michael, et al. [81]	CPS Architecture with Lean Six Sigma Integration	Designing a CPS architecture using 8 C framework and integrating Lean Six Sigma principles	Analyzes integration of LSS principles	Future research directions and practical implications outlined

2.5 Integrating Cyber-Physical Systems, Blockchain, IoT and Edge Computing

In our rapidly evolving digital landscape, the integration of emerging technologies has become instrumental in shaping the future of various industries. One such convergence of technologies that holds immense potential is the integration of CPS, Blockchain, IoT, and Edge Computing. The goal of this analysis of literature is to look into the numerous dimensions of this integration, shed light on the synergistic opportunities, issues, and consequences for the modern world. Figure 2.3 shows the basic framework of an edge computing network.

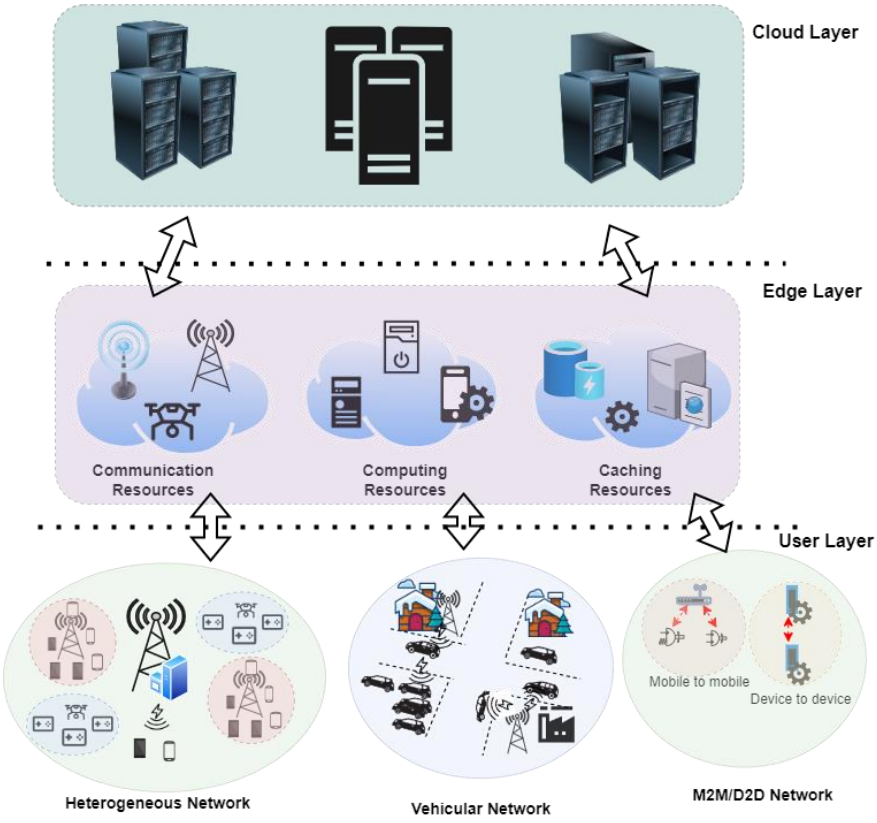


Figure. 2.3. The general framework of an edge computing network

Zhou et al. [82] proposes a secure and efficient framework for vehicle-to-grid (V2G) energy trade that incorporates edge computing, blockchain technology, and contract theory. The authors create a safe energy trading system for V2G, enhancing security by utilising a consortium blockchain. In response to knowledge asymmetry circumstances, the authors offer an effective incentive mechanism based on contract theory. They use edge computing to increase the likelihood of successful block production. The effectiveness of their suggested framework is supported by numerical and theoretical findings, demonstrating its potential and application in the context of V2G energy trading. **Latif et al. [83]** looks into the possible benefits of combining blockchain technology with software-defined networking (SDN) to address energy and security issues in IoT devices. It offers a revolutionary routing protocol with a cluster-based architecture suited for IoT networks, as well as an SDN controller based on blockchain. The proposed architecture eliminates the need for proof-of-work (PoW) and utilises both private and public blockchains to facilitate peer-to-peer (P2P) communication between SDN controllers and IoT devices. The proposed protocol provides a viable option for tackling critical issues, particularly in the fields of energy management and security, within the context of next-generation industrial cyber-physical systems.

There is presently no comprehensive study integrating both views, despite prior research concentrating on either blockchain's implementation in various CPS contexts or its role in increasing CPS safety. In order to fill this research gap, **Khalil et al. [84]** gives a comprehensive summary of current advancements in using blockchain to improve different CPS activities and strengthen CPS security. The authors present a thorough assessment that includes studies concerning blockchain-enabled CPS functions and safety measures. Through consensus methods and smart contract implementations, blockchain provides solutions that improve CPS resilience by providing permanence, resilience to failure, and uniformity. **Yu et al. [85]** provides a full evaluation of the compatibility between blockchain technology and CPS inside the IoT framework in this context. The study is divided into three sections: safety, confidentiality, and trustworthiness. These categories elucidate the utility of blockchain in mitigating security threats, preserving privacy, and managing trust issues, leveraging an array of cutting-edge techniques, including cloud computing, edge computing, machine learning, artificial intelligence, side-chain technology, and more.

Xue et al. [86] seeks to thoroughly investigate the field of Integration of Blockchain and Edge Computing (IBEC). To do this, the authors begin with overviews of blockchain and edge computing. Subsequently, they outline the fundamental architecture of an IBEC system. Their exploration extends to examining diverse applications of IBEC within the IoT context. Furthermore, they delve into optimizations for IBEC systems, considering resource management and performance enhancements. To conclude, the authors assess and synthesize the prevalent challenges posed by IBEC systems, along with prospective solutions for future development. Figure 2.4 shows the structure of a blockchain network.

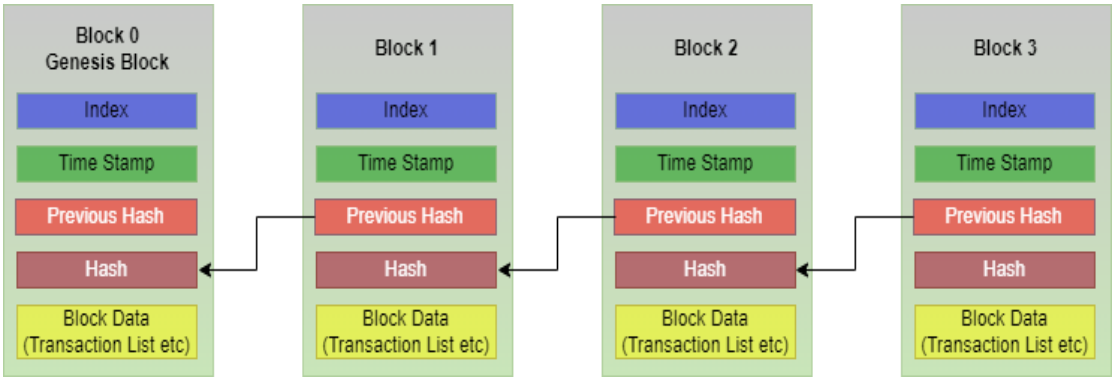


Figure. 2.4. Structure of a blockchain

Al-Ghuraybi et al. [87] focuses on evaluating the efficiency and safety components of CPS, with a particular focus on mitigating external hazards through the use of blockchain technology and machine intelligence. It provides a thorough summary of recent research findings

demonstrating the usage of blockchain to improve CPS efficiency while providing strong safety measures. Furthermore, the authors investigate the synergistic use of blockchain and machine learning approaches to strengthen CPS security. Furthermore, they investigate how combining blockchain with physically unclonable functions (PUF) might significantly improve the efficiency of physical device verification. **Zhao et al. [88]** presents a succinct yet thorough assessment of blockchain-enabled CPS. The authors investigate several blockchain-enabled CPSs that have been described in the literature with regard to of their functioning and the blockchain features that have been deployed. They identify important typical CPS processes that blockchain can allow and classify them based on their time urgency and throughput needs. They additionally explain and categorize blockchain capabilities in terms of CPS advantages, such as safety, confidentiality, indestructibility, resilience to failure, interconnection, background information, simplicity, automation, information/service sharing, and trustworthiness.

Despite the potential benefits of combining edge computing with Blockchain in networked settings, there remain obstacles to overcome, including expansion, management of resources, function integration, self-organization, and rising safety concerns. **Hazra et al. [89]** presents an overview of a safe IoT architecture and explores concepts, facilitators, and safety issues connected with Blockchain and intelligent edge computing integration. Furthermore, it explores future research directions in this area. While conventional blockchains employ Merkle hash trees for data storage, they encounter limitations in supporting batch additions/deletions and non-membership proofs. To address this challenge, **Wang et al. [90]** enhances the accumulator and combines it with the Merkle hash tree, thereby enabling batch addition/removal operations and facilitating non-membership proof generation. In this work, authors establish a Merkle hash tree accumulator and validate the feasibility of our proposed scheme through rigorous assessments of correctness and security.

Ali et al. [91] emphasizes the role of Blockchain as a promising solution for modern CPS applications. The authors underscore how Blockchain implementation in CPS and IoT ensures the secure storage of information across various industrial domains, enhancing adaptability, process integrity, and operational protection. These benefits are particularly relevant in sectors like manufacturing, transportation, healthcare, and energy applications. They aim to furnish a comprehensive technical foundation for understanding Blockchain's role in IoT-based CPS, encompassing discussions on applications, opportunities, and challenges in combining CPS, IoT, and Blockchain technologies. **Rathore et al. [92]** explores diverse applications of CPS

where blockchain integration has been leveraged. It examines how blockchain technology can benefit applications like smart grids, healthcare systems, and industrial production processes.

Al-Ghuraybi et al. [93] provides a thorough review of current research projects focusing on the merging of Blockchain technology with Medical Cyber-Physical Systems (MCPS) including its potential use in the medical arena. The papers reviewed by the authors offered the spotlight on several elements of utilising Blockchain to improve MCPS security and efficiency while protecting medical data. Several unsolved problems, concerns, and recommended solutions in the merging of Blockchain with MCPS have been found as a result of this investigation. **Mei et al. [94]** describes a unique blockchain-based confidentiality-preserving verification method for transportation CPS in a cloud-edge computing context. This solution provides strong security, absolute confidentiality, and data batch integrity authentication, whilst making key management easier. The authors demonstrate the security of their technique by solving an elliptic curve discrete logarithm issue in the random oracle model, which is supplemented by a full security analysis. Finally, they employ a simulated exercise to demonstrate the feasibility and utility of their proposed strategy in contrast to existing approaches.

The inadequacy of existing security mechanisms, such as traditional cloud or trust-based certificate systems, prompted **Rahman et al. [95]** to develop a new blockchain-based architecture to improve the safety and effectiveness of Industry 4.0 systems. This strategy lowers the need for traditional certificate authority by improving the consortium blockchain, reducing data processing delays, and enhancing cost-effective throughput. The suggested framework's implementation of a multi-signature approach enables multi-party authentication, making it appropriate for real-time and collaborative cyber-physical systems. The authors address the pressing security concerns in the contemporary landscape of critical system protection against cyber-attacks.

Lampropoulos et al. [96] provides an overview of the usage of digital twins as a strategy for strengthening and safeguarding cyber-physical systems and, more broadly, Industry 4.0. Digital twins connect the physical and virtual worlds and can supplement other technologies, allowing for real-time monitoring and control, immediate access to dynamic data, continuous visualisation and evaluation, process optimization, advanced decision-making, and predictive systems in a variety of industries. **Yang et al. [97]** focuses on creating digital twin-driven simulations and doing simulation experiments using real-time data. A simulation model is created to mimic the behaviour of a physical system by building a distributed model outfitted

with sensors similar to the original system, allowing simulation experiments to be done. Within the field of simulation-based approaches, the suggested modelling technique shows potential for further use in decision-making assistance systems that rely on real-time data.

Rathore et al. [98] describes DeepBlockIoTNet, a revolutionary deep learning technique that incorporates blockchain technology into an IoT network. In this innovative framework, DL operations are conducted in a decentralized, secure manner among edge nodes at the edge layer. By leveraging blockchain, this approach ensures the security of DL operations and eliminates the need for centralized control. Experimental assessments of this proposed approach reveal its capacity to deliver enhanced accuracy in data analysis.

Xu et al. [99] presents a novel blockchain-based trustworthy edge caching strategy for MCPS mobile users. The authors, in particular, employ blockchain technology to monitor distributed caching transactions between edge nodes and mobile users, assuring the authenticity and irrevocability of caching service information. They also propose a trust management system that allows mobile consumers to identify reputable cache services across various edge nodes. Based on the quality of the cache service offered, this system regularly assesses and improves the reliability of edge nodes. They created a max-min-based resource allocation technique to optimize the utilization of cache resources. This technique allows reliable edge nodes to allocate cache resources fairly based on the optimal demands of mobile users. Simulations show that their suggested strategy improves not just the effectiveness of edge nodes but also the quality of experience for mobile users.

In **Mei et al. [100]** , the authors introduce an innovative blockchain-based privacy-enhancing authentication system tailored for the transportation CPS operating within a cloud-edge computing framework. Their method ensures total confidentiality and validates data batch dependability while mitigating crucial managerial challenges. The suggested privacy-preserving authentication method uses elliptic curves to produce a pairing-free ring signature system, decreasing resource needs in transportation CPS with cloud-edge computing. The authors give a security assessment that demonstrates the scheme's resistance to the elliptic curve discrete logarithm problem in the random oracle model. They ran a simulated test to compare the efficacy of the suggested approach to current techniques. They add to the current literature by providing significant insights into the subject of blockchain-enabled privacy-preserving authentication inside transportation CPS.

Wang et al. [101] is committed to minimizing the total latency of the system of edge-cloud computing in collaboration with CPS, while additionally keeping security and reliability requirements into mind. To accomplish this goal, the authors begin by studying a time-varying channel model known as a Finite-State Markov Channel (FSMC). They present a distributed blockchain-assisted CPIoTS system that enables safe consensus and trustworthy resource management by outsourcing computational workloads to the edge-cloud computing environment. Furthermore, they propose PPO-SRRA, an efficient resource allocation algorithm that optimises the distribution of computational tasks and multi-dimensional resources (including interaction, computing, and consensus resources) using policy-based Deep Reinforcement Learning (DRL) techniques.

A wide range of research articles that study the adoption of blockchain technology into various sections of CPS, IoT, and Industry 4.0 are included in the review of the literature. These studies highlight the potential of blockchain to enhance security, privacy, reliability, and efficiency in these domains. The use of blockchain for safe energy exchange in vehicle-to-grid systems, the use of blockchain to improve security and data management in IoT networks, and the significance of blockchain in protecting critical systems in Industry 4.0 are some of the primary topics and conclusions. Additionally, some studies emphasize the combination of blockchain with technologies such as edge computing, machine learning, and digital twins to address specific challenges in CPS and IoT. These research efforts collectively contribute to advancing the understanding and implementation of blockchain in cyber-physical systems and related domains. Table 2.4 presents the summary of the literature review for integrating CPS, Blockchain, IoT and Edge Computing.

Table-2.4. Summarization of literature review for integrating CPS, Blockchain, IoT and Edge Computing

Author	Technique	Problem Statement	Performance Analysis	Limitations
Zhou, Zhenyu, et al. [82]	Integration of blockchain and edge computing	The imbalance between energy demand and supply in smart grids.	Substantiated through numerical results and theoretical analysis.	Limited discussion on scalability and real-world implementation challenges
Latif, Sohaib A., Celestine Iwendi, et al. [83]	Blockchain and SDN integrated security architecture	Challenges in IoT networks include energy efficiency and security.	Superiority over existing protocols in terms of energy consumption, network throughput, and packet latency.	Lack of in-depth exploration of potential AI vulnerabilities and scalability concerns
Khalil, Alvi Ataur, Imtiaz Parvez, et al. [84]	Literature review on blockchain-enabled security	Addressing various CPS challenges with blockchain technology.	Provides a comprehensive review of research but does not include	Lack of specific case studies and real-world

			specific performance analysis.	implementation examples
Yu, Chunyang, Xuanlin Jiang, et al. [85]	Blockchain-based shared manufacturing	Trustworthiness challenge in SharedMfg within the manufacturing sector.	Introduction of the Blockchain-based SharedMfg (BSM) framework.	Focus primarily on shared manufacturing, may not cover all aspects of CPS
Xue, He, Dajiang Chen, et al. [86]	Integration of blockchain and edge computing	Enhancing resource utilization across network, computation, storage, and security domains.	Examines various aspects of IBEC, including applications, optimizations, and challenges.	Identifies challenges but does not provide a detailed performance analysis.
Al-Ghuraybi, Hind A., AlZain, et al. [87]	Integration of blockchain, physically unclonable function, and machine learning	Performance and security dimensions of CPS with a focus on countering external threats.	No specific performance analysis was mentioned.	Lack of comprehensive exploration on machine learning integration and scalability
Zhao, Wenbing, , et al. [88]	Blockchain-enabled cyber-physical systems	Review of blockchain-enabled CPS in terms of operations and blockchain features.	Does not include specific performance analysis.	Points out open research issues for developing blockchain-enabled CPS.
Hazra, Abhishek, Ahmed Alkhayyat, et al. [89]	Integration of Blockchain and intelligent edge computing	Challenges in scalability, resource management, and security for IoT systems.	Provides an overview of a secure IoT framework and discusses related challenges.	Addresses challenges but does not provide a detailed performance analysis, lacks specific case studies
Wang, Jin, Wencheng Chen, , et al. [90]	Blockchain-based data storage mechanism	Data security concerns in cyber-physical systems.	Enhances data storage scheme and validates its feasibility.	Focuses on data storage but does not discuss broader performance analysis.
Ali, Reham Abdelrazek, Rania , et al. [91]	Applications and Challenges of Blockchain in CPS	Application of blockchain in CPS for enhanced security, reliability, and efficiency.	Provides an overview of applications and challenges in combining CPS, IoT, and Blockchain technologies.	Lacks detailed exploration on specific challenges and real-world examples
Rathore, Heena, Amr Mohamed, et al. [92]	Blockchain-enabled cyber-physical systems	Enhancing the robustness and reliability of CPS with blockchain technology.	Examines diverse applications of CPS where blockchain integration has been leveraged.	Lack of detailed discussion on specific techniques and limitations
Al-Ghuraybi, Hind A., Mohammed, et al. [93]	Blockchain technology integration with machine learning	Security and efficiency of Medical Cyber-Physical Systems (MCPS) with blockchain and machine learning.	Provides a comprehensive overview of research studies on the integration of Blockchain with MCPS.	Lack of comprehensive exploration on machine learning integration and scalability
Mei, Qian, Hu Xiong,, et al. [94]	The privacy-preserving authentication	Privacy-preserving authentication in transportation CPS within a cloud-edge	Offers a novel blockchain-based privacy-preserving	Limited exploration on scalability and real-world

	mechanism for transportation CPS	computing environment.	authentication system.	implementation challenges
Lampropoulos, Georgios, et al. [96]	Utilization of digital twins for securing cyber-physical systems and Industry 4.0.	Security challenges in Industry 4.0 due to digitization and interconnectivity.	Digital twins bridge physical and virtual realms, offering advantages like real-time monitoring and control.	Focus primarily on digital twins, may not cover all aspects of CPS
Yang, W., Y. Tan, K. Yoshida, et al. [97]	Digital twin-driven simulation for a cyber-physical system in Industry 4.0.	Emulation of autonomous entities using digital twins in cyber-physical systems.	Use of a distributed model with sensors for real-time data simulation. Potential use in decision-making support tools.	Limited exploration on specific security aspects and scalability
Rathore, Shailendra, et al [98].	Blockchain-based deep learning for cybersecurity in next-gen industrial CPS.	Demand for precise and responsive big data analysis in IoT-based CPS.	DeepBlockIoTNet incorporates blockchain into IoT for decentralized, secure DL. Enhanced accuracy in data analysis.	Lacks in-depth exploration on specific deep learning algorithms and scalability
Xu, Qichao, Zhou Su, et al. [99]	Blockchain-based trustworthy edge caching for mobile cyber-physical systems.	Challenges in trust management and security for content caching in MCPS.	Blockchain-based scheme for trustworthy caching, trust management mechanism, and resource allocation algorithm. Improved QoE for mobile users.	Focus primarily on secure computation offloading, may not cover all aspects of CPS
Mei, Qian, Hu Xiong,, et al. [100]	Blockchain-enabled privacy-preserving authentication for transportation CPS with cloud-edge computing.	Anonymity, data integrity, and key management challenges in transportation CPS.	Use of elliptic curves for a pairing-free ring signature system, authentication on blockchain. Robustness demonstrated against security challenges.	Limited exploration on scalability and real-world implementation challenges
Wang, Dan, Bin Song, Yingjie Liu, , et al. [101]	Secure and reliable computation offloading in blockchain-assisted cyber-physical IoT systems.	Efficient resource management and latency reduction in CPIoTS with security and reliability considerations.	Finite-State Markov Channel model distributed blockchain-assisted CPIoTS framework and resource allocation algorithm. Reduced system latency and ensured consensus security.	Lack of detailed discussion on specific techniques and limitations

CHAPTER 3

ADAPTIVE FRAMEWORK FOR DIVERSE SMART INDUSTRIAL CYBER-PHYSICAL SYSTEMS IN THE ERA OF INDUSTRY 5.0

3.1 Introduction

Advances in technology like Internet of Things, machine-to-machine communication (M2M), artificial intelligence, cloud computing, cognitive computing, and the utilization of sophisticated ARM processors for embedded tasks are driving a substantial transformation in industrial process automation. The integration of cutting-edge IP-enabled devices such as sensors, actuators, and controllers is transforming the automation industry, propelling it towards Industry 5.0 standards and, eventually, total autonomy without human involvement. Amidst these new technologies, CPS stand out as a crucial element of the fourth industrial revolution. They are composed of linked, separate programmed embedded systems that collaborate on information processing, communication, management, and actuation This chapter provides a diversified CPS architecture that allows for the integration of various hydraulic, inflated, and electrical procedures to control heterogeneous procedure behaviour. The planned architecture design enables for the separation of distinct aspects within a process dynamic, such as computing, management, interaction, and actuation. This division is accomplished by estimating variables like process disruptions, sensor latency, actuator latency, and conversion latency. VFI- Voltage frequency islands with great standard are used to allocate computational embedded cores to diverse physical processes. DVFS- Dynamic Voltage and Frequency Scaling is used to improve all specified process dynamics.

In a varied CPS framework, the importance of standardized wireless sensor-actuator systems (WSANs) is crucial, especially with an advent of trade 5.0 that is shifting towards adopting a decentralized wireless control system [102][103]. In industries spread across different locations, the effectiveness of their feedback control loop greatly depends on the suitability of WSANs like International Society of Automation A100 (created by the ISA), ZigBee, Wireless HART, Wireless Industrial Networking Alliance (WINA), and Highway Ad dressable Remote Transducer Protocol (HART). In order to minimise the requirement for

manual intervention, the SCPS must be extremely steadfast, with tiniest message faults or the swift routing delay[104]. Smart cores integrated across various SCPS types can be interconnected via a smart grid [105]. Structural health monitoring is another area where CPS plays a vital role, enabling remote monitoring of aging constructions like buildings, tunnels, bridges, and roads with an early warning system [106]. Moreover, the implementation of CPS-centered structural health monitoring (SHM) makes it easier to monitor natural calamities such as floods, landslides, and earthquakes [107]. The primary envisioned application of CPS lies in collaborative human-robot interaction for industrial automation (HRC). This involves utilizing robots designed to industrial standards, such as PUMA and SCARA, in various sectors like oil exploration, automotive manufacturing, and intelligent packaging [108]-[112]. These adaptable robots can be precisely programmed and coordinated to match the dynamic requirements of industrial processes [113][114]. The intelligence in these systems is embedded within sensors and actuators, achieved through their integration with signal conditioning, processing units, and communication tools. In a CPS, the control system centered around computers encompasses a series of embedded controllers designed to carry out individual or numerous procedure loops. The effective "synchronization of interconnected embedded controllers in a System Control and Process System (SCPS)" is crucial because of the diverse durations required for each variable's execution. It is crucial to estimate and address disturbances, delays at sensor and actuator nodes, pneumatic and hydraulic conversion times to electrical signals.[115] These factors are pivotal in SCPS to be mitigated through predictive algorithms, enabling the allocation of suitable controllers to the diverse electrical, pneumatic, and hydraulic processes within a manufacturing plant. Figure 3.1 illustrates a layered structure depicting an CPS.

To enable the diverse production units within a manufacturing facility, a diverse Cyber-Physical System (CPS) is necessary, capable of managing both varied batch and continuous processes simultaneously. The rates of these procedures vary: while certain processes, such as the swift movement of oil within pipelines, are quick, others, like the control of temperature in a heat exchanger, function at a more gradual speed. Control algorithms are implemented based on the temporal characteristics of each process. Minimizing human involvement in automated systems poses various unaddressed research hurdles, such as enhancing a DVFS-Dynamic Voltage and Frequency Scaling controller to reduce energy usage across multiple mapped procedures on a computational manager network, both at the controller and actuation levels. Focusing on these areas of study is critical to ensuring that CPS attain high levels of precision, accuracy, speed,

as well as robustness. Modularity algorithms and VFI [116]-[118] are utilized to facilitate the allocation of various computing machines. Synchronizing the processing cores' clocks involves estimating disturbances and delays.

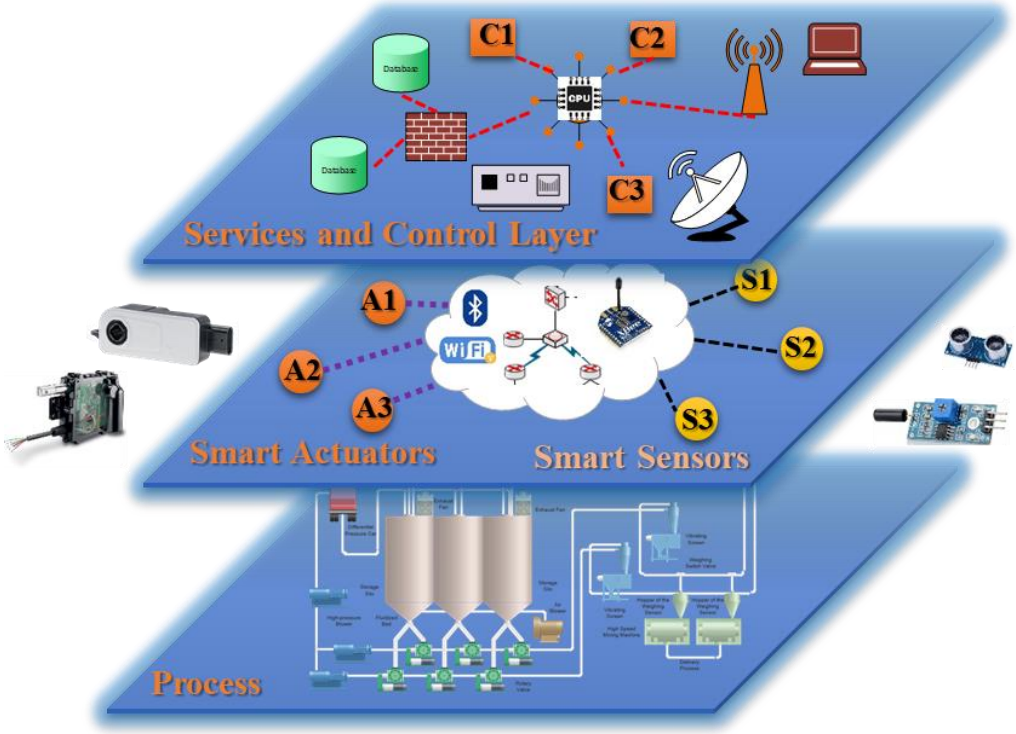


Figure. 3.1. Structured Composition of an CPS in a Stratified Format

Delays in time have a notable impact on the allocation of a computing group for entrenched regulators and the identification of specific occurrence and voltage needs for individual tasks. These anticipated delays play a critical part in shaping the overall recital of the control system, which is fine-tuned through employment of the PID+DVFS controller. In scenarios involving vital real-time dynamic processes where instant information broadcast and security are of utmost importance, a recommendation scheme based on trust holds great relevance [119]. The majority of simulations are conducted using Standard shielding from multiple process process loops, Raspberry Pi Boards, and Arduino Uno were interfaced with using Scicos and MATLAB Simulink. The key elements highlighted in this chapter include:

1. Employing a standard algorithm and VFI to optimize the allocation of processor cores for various process executions.
2. Using an estimator to measure disturbance signals allows for the estimate of control laws inside programmed cores, allowing for error minimization to zero.
3. Estimating delays at both the sensor and actuator ends to enhance system performance.

4. Implementing DVFS controller to streamline the assigned processes and curtail the vigor ingesting of computational cores.
5. Using a DVFS controller in conjunction with a PID switch procedure to optimize the supply occurrence of computational centres engaged in a procedure loop.

3.2 Assigning Computing Clusters to Diverse Processes

To meet the needs of diverse production units within a manufacturing facility, it is necessary to employ a diverse CPS capable of managing both batch and continuous processes simultaneously. While certain processes, such as the flow of oil through pipelines, occur rapidly, others, like regulating the temperature of a heat exchanger, unfold more slowly. Control algorithms are implemented based on the temporal characteristics of each process. Reducing human involvement in automated physics generates various unresolved research challenges, such as accurately estimating disturbances and delays. It is essential to improve the effectiveness of a DVFS controller in saving energy at various stages of control and operation across multiple assigned tasks in a computational controller network. Filling these research voids demands a high level of accuracy, precision, speed, and resilience within the CPS. The modularity algorithm and VFI are utilized to allocate separate computing machines.

The section's proposed work offers a dual contribution:

1. A design approach to divide a provided computing grid into several voltage-occurrence fields.
2. To decrease energy usage, provide each cluster with a distinct threshold voltage according to its clock frequency.

Figure 3.2 depicts the culturing method used to create a multi-controller computational grid.

Owing to their low-slung control consumption and affordability, it is recommended to employ ARM cores in integrating a control algorithm in the Multi-Controller Computational Grid for the CPS Control System. Cortex M cores are utilized for individual processes, while Cortex R cores are employed for hybrid tiles. The collection of controller tiles within the computational grid is represented as $T_{ARM} = \{1, \ldots\ldots, N\}$. Every ARM processor $i \in T_{ARM}$operates with two voltage levels: V_i and V_{Thi}. The stationary vigor linked to each regulating core is articulated in the subsequent manner:

$$E_i(V_i, V_{Thi}) = R_i C_i V_i^2 + T_{ARM-i} K_i V_i e^{\left(-\frac{V_{Th}}{S_{Th}}\right)} \quad (3.1)$$

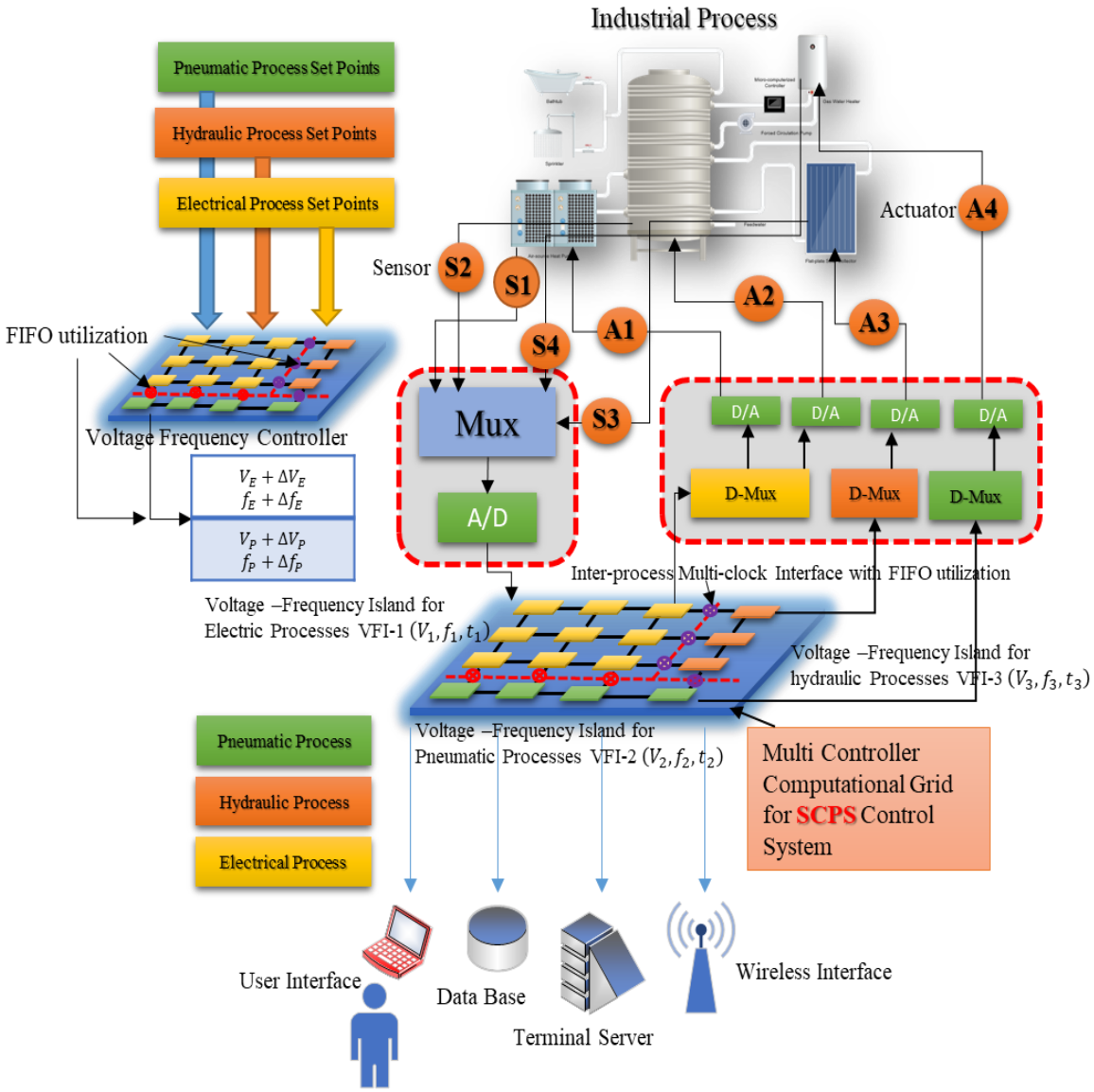


Figure 3.2 Creating a Computational Grid for Managing the CPS Control System with Multiple Controllers

Several factors impact the energy consumption of each controller unit, as shown in Figure 3.3. These include the count of active cycles (R_i) in the process's control loops, the count of capacitance switches per cycle (C_i), the quantity of ideal cycles within a process's control loop (T_{ARM-i}), as well as technology (determined by K_i) and design parameters (S_{Th}) [120].

The timepiece occurrence of individually regulator tile can be established according to the designated clock period, which is described as:

$$\tau_i(V_i, V_{Thi}) = \frac{K_i V_i}{(V_i - V_{Thi})^{\alpha}} \tag{3.2}$$

Where α is the technical restriction. The frequency at which a regulator tile operates within a group based on equation (3.2) is given by:

$$f_i(V_i, V_{Thi}) = \frac{1}{\tau_i(V_i, V_{Thi})} \tag{3.3}$$

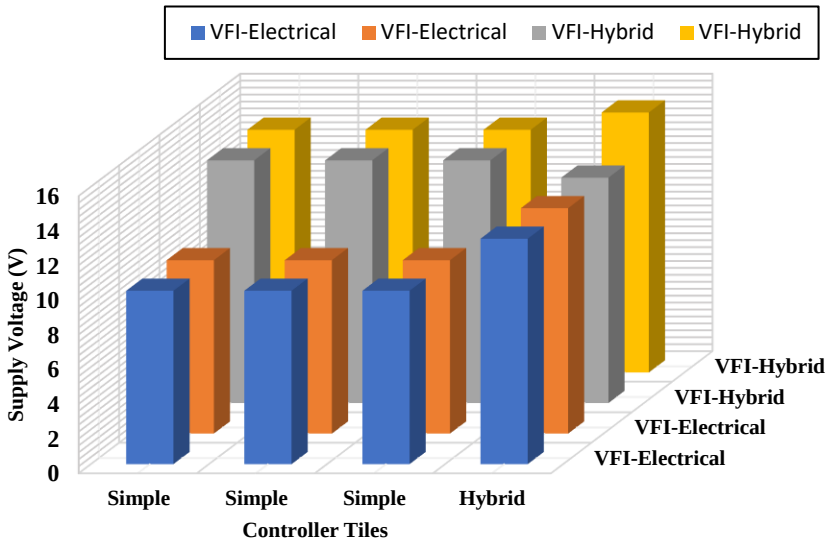


Figure 3.3 The energy needs of individual controller tiles within the Computational Grid for the CPS Control System

The energy associated with a single procedure depicted on a VFI is:

$$E_{VFI-Elect} = E_{ClkGen} + E_{Vconv} + E_{MixClkFIFO} \tag{3.4}$$

Three primary factors contribute to the energy usage in this context. E_{ClkGen} arises from the extra clock signals necessary to support a Big-Little architecture. E_{Vconv} stems from the transfer of processed signals from one VFI to another VFI, and the ultimate energy above, $E_{MixClkFIFO}$, arises from a hybrid process interface that employs a varied voltage and varied frequency FIFO. The magnitudes of energy overheads might differ based on the mapped directed graph that depicts a process's physical dynamics [121] [122]. The simulated supply voltage and verge voltage for each tile in the Multi-Controller Computational Grid described in Figure. 3.2 are shown in Figure 3.4.

One way to confirm the VFI partition is by evaluating its modularity. Greater modularity indicates the utilization of numerous computational tiles to concurrently run diverse control algorithms. To compute modularity, it's essential to have the task graph for process automation mapped onto the Multi-Controller Computational Grid. This grid's modularity is determined by:

$$Q = \frac{1}{2m}\sum_{VFI}\sum_{i,j\in VFI}\left(A_{ij} - \frac{d_i d_j}{2m}\right) \tag{3.5}$$

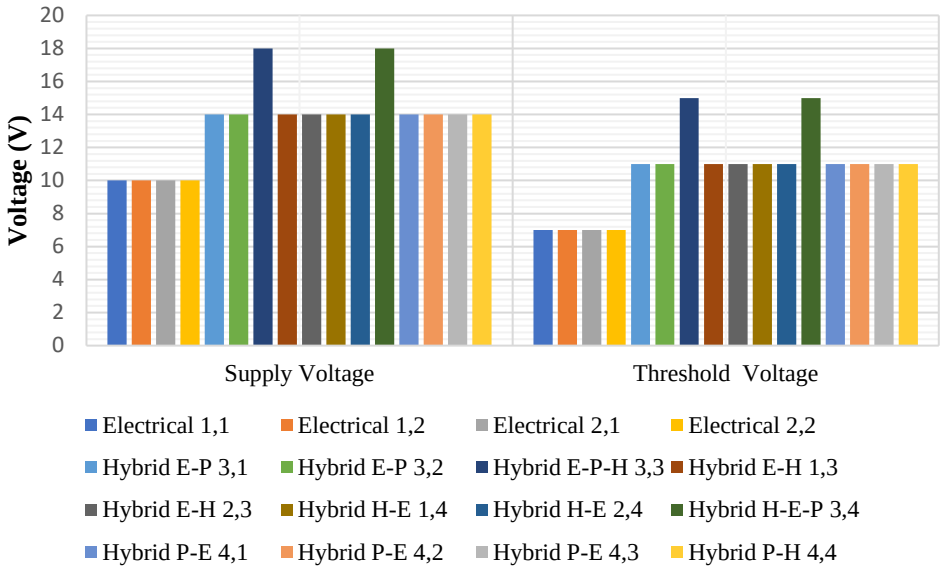


Figure 3.4 The emulated power supply voltage and activation threshold voltage for every unit within the Multi-Controller Computational Grid

A_{ij} represents an entry within the adjacency matrix A, where i and j denote the interconnected nodes on the Multi-Controller Computational Grid. The variable d signifies the node's degree, while m stands for the overall number of links within the procedure mechanization chore diagram that is assigned to the Multi-Controller Computational Grid, as depicted in Figure 3.5.

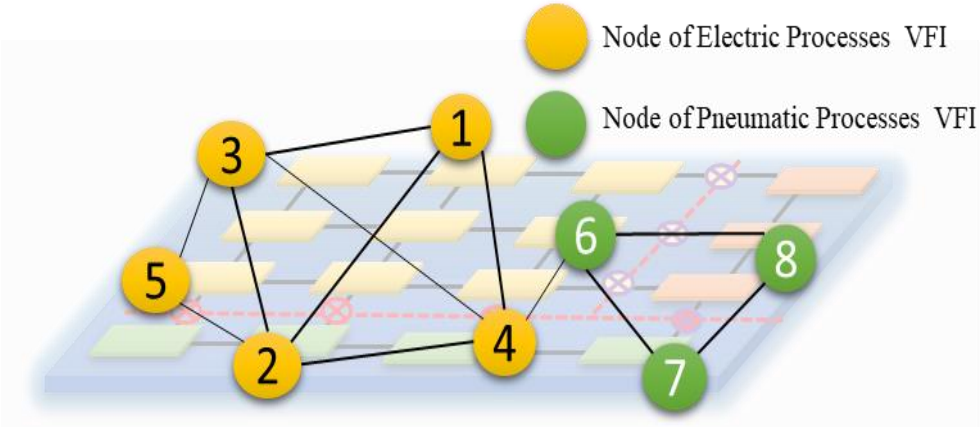


Figure 3.5 Process Automation Task Graph

The task graph's adjacency matrix is

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}, \text{Degree Matrix } d = \begin{bmatrix} 3 \\ 4 \\ 4 \\ 4 \\ 2 \\ 3 \\ 2 \\ 2 \end{bmatrix}, \text{Total degree= } 2m = 24$$

Table-3.1. Modularity matrix $A_{ij} - \frac{d_i d_j}{2m}$ Entries

i, j	1	2	3	4	5	6	7	8
1	-0.375	0.5	0.5	0.5	-0.25	-0.375	-0.25	-0.25
2	0.5	-0.67	0.34	0.34	0.67	-0.5	-0.34	-0.34
3	0.5	0.34	-0.67	0.34	0.67	-0.5	-0.34	-0.34
4	0.5	0.34	0.34	-0.67	-0.34	0.5	-0.34	-0.34
5	-0.25	0.67	0.67	-0.34	-0.17	-0.25	-0.17	-0.17
6	–0.375	-0.5	-0.5	0.5	-0.25	-0.375	0.75	0.75
7	-0.25	-0.34	-0.34	-0.34	-0.17	0.75	-0.17	0.84
8	-0.25	-0.34	-0.34	-0.34	-0.17	0.75	0.84	–0.17

The total of values from the colored tiles within the modularity matrix $\sum VFI$= 8.29

The computational grid's modularity with multiple controllers is $\frac{\sum VFI}{2m}$ = 0.345

Enhancing the division or grouping can be achieved through the utilization of the modularity algorithm.

3.3 Determining the Disturbance Signal Within CPS

A CPS consists of numerous interconnected elements within a compact localized system using wired connections, and in a broader geographical scope, it utilizes wireless connections. Disruptions, also known as disturbances, have a detrimental influence on the operating efficiency of a CPS's control system. Such unwanted signals impede the CPS's accuracy and usefulness. The connection between computers and the physical systems they manage is extremely flexible. Beyond managing inputs and outputs, computer algorithms can also regulate various state space variables within the system.

3.3.1 Designing State Estimators for CPS

The state interplanetary representation of a distinct-time structure's process is:

$$x(k+1) = \Phi x(k) + \Gamma u(k) \tag{3.6}$$

$$y(k) = Hx(k) + Ju(k) \tag{3.7}$$

In equation (3.6), we have the state equation, while equation (3.7) represents the output equation. Here, Φ stands for the system matrix, Γ represents the control matrix, H is the output matrix, and J is the direct transmission matrix. Enhancing the effectiveness of a CPS is possible by directly controlling the state interplanetary subtleties of a real procedure via estimation using a state estimator. The equation provided illustrates the actions of a full State-Space CPS system utilizing a control law and estimator to govern its behavior:

$$\begin{bmatrix}\tilde{x}(k+1)\\ x(k+1)\end{bmatrix} = \begin{bmatrix}\Phi - L_p H & 0\\ \Gamma K & \Phi - \Gamma K\end{bmatrix}\begin{bmatrix}\tilde{x}(k)\\ x(k)\end{bmatrix} \tag{3.8}$$

K represents the controller gain while$L_p$stands for the prediction estimator gain.

The varied combinations of the estimator and controller mechanism depicted in Figure 3.6 are contingent on the specific characteristics of the physical process.

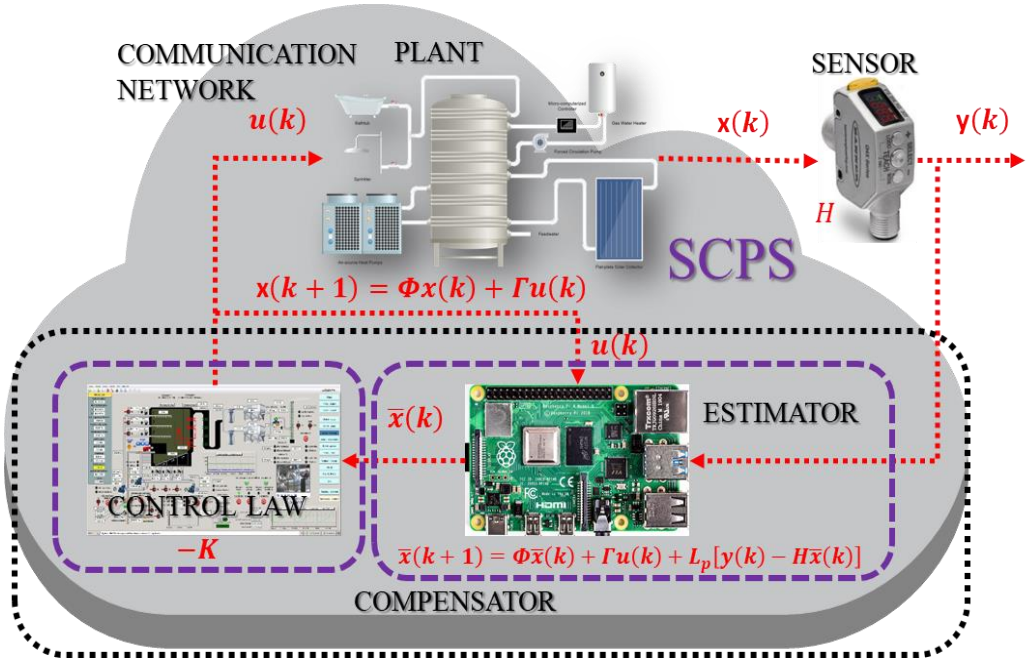


Figure. 3.6. The Mechanism for Estimation and Control in CPS

When computer-installed control algorithms rely on state-space variables, their efficiency improves. The CPS control system is more successful because it estimates and manages the conditions of a corporeal procedure before any aberrations in the process output occur. When dealing with an approximate state interplanetary capricious of CPS, it is easier to visualise the outcome when utilising equation (3.9).

$$\begin{bmatrix}x(k+1)\\ \bar{x}(k+1)\end{bmatrix} = \begin{bmatrix}\Phi & -\Gamma K\\ L_p H & \Phi - \Gamma K - L_p H\end{bmatrix}\begin{bmatrix}x(k)\\ \bar{x}(k)\end{bmatrix} \tag{3.9}$$

Figure 3.7 displays the projected operations of a controlled CPS using a predictive estimator.

As per the formula (3.9), the anticipated vector $\bar{x}$ is derived by receiving the production indicator $y(k-1)$ from sensors associated with CPS. It indicates that the current control value is not dependent on the latest observation, leading to a lower precision of the switch procedure executed on the computer than its inherent capability. Nevertheless, this difference is a subject of the temporary subtleties of a procedure. The following equation illustrates the state-space dynamics for the existing estimator:

$$\begin{bmatrix} x(k+1) \\ \hat{x}(k+1) \end{bmatrix} = \begin{bmatrix} \Phi & -\Gamma K \\ L_c H\Phi & \Phi - \Gamma K - L_c H\Phi \end{bmatrix} \begin{bmatrix} x(k) \\ \hat{x}(k) \end{bmatrix} \quad (3.10)$$

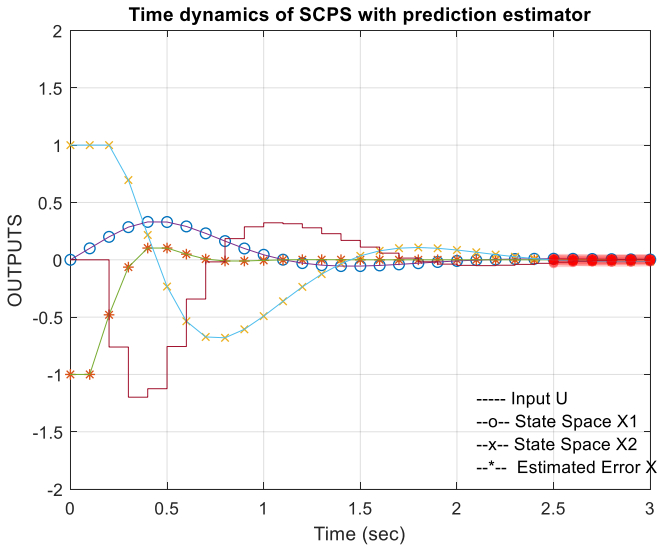


Figure. 3.7. Analyzing the Predictive Estimation in a Controlled Cyber-Physical System's Dynamic Performance.

The illustrated figure, Figure. 3.8, displays the active performance of an administered CPS utilizing a current estimator.

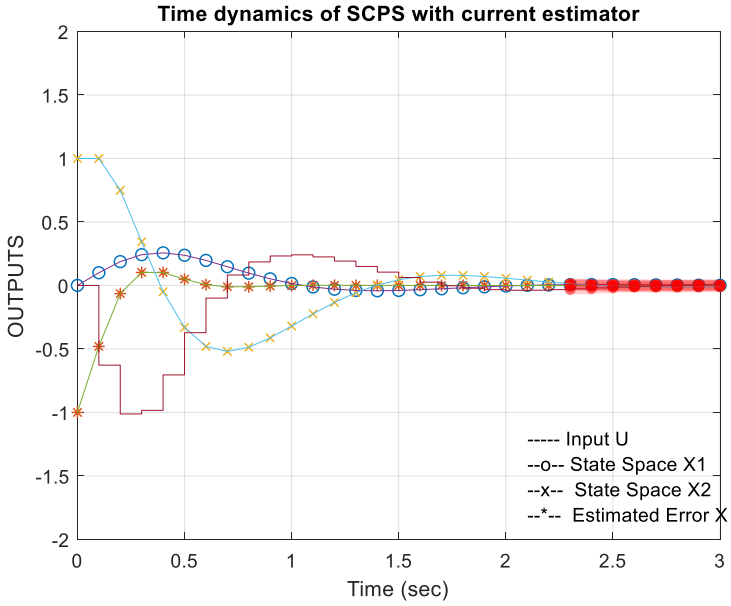


Figure. 3.8. The Evolving Performance of a Regulated CPS Utilizing a Current Estimation System

When directly applying the control rule or deploying the state interplanetary compensator, the use of a state space model for procedure subtleties is quite advantageous. However, there are instances where controlling all state space vectors might not be essential. Therefore, the reduced-order compensator estimates only the state space vectors relevant to the situation. It

directly controls the measured segment of the state vector, x_a, and uses a reduced-order estimator to estimate the remaining part, x_b. The segregated state space model of CPS can be represented by the equations mentioned:

$$\begin{bmatrix} x_a(k+1) \\ x_b(k+1) \end{bmatrix} = \begin{bmatrix} \Phi_{aa} & \Phi_{ab} \\ \Phi_{ba} & \Phi_{bb} \end{bmatrix} \begin{bmatrix} x_a(k) \\ x_b(k) \end{bmatrix} + \begin{bmatrix} \Gamma_a \\ \Gamma_{\boldsymbol{b}} \end{bmatrix} u(k) \tag{3.11}$$

$$y(k) = [I \quad 0] \begin{bmatrix} x_a(k) \\ x_b(k) \end{bmatrix} \tag{3.12}$$

Therefore, it is necessary to segment the control gain K.

$$u(k) = [K_a \quad \boldsymbol{K_b}] \begin{bmatrix} x_a \\ \boldsymbol{x_b} \end{bmatrix}, \text{ where } K = [K_a \quad \boldsymbol{K_b}] \tag{3.13}$$

The following equation gives the outcome for the reduced order estimator.

$$\begin{bmatrix} x(k+1) \\ \hat{x}_b(k+1) \end{bmatrix} = \begin{bmatrix} \Phi - \Gamma[K_a \quad 0] & -\Gamma K_b \\ L_r H\Phi + \Phi_{ba}H - \Gamma_{\boldsymbol{b}} K_a H - L_r \Phi_{aa} H & \Phi_{bb} - \Gamma_b K_b - L_r \Phi_{ab} \end{bmatrix} \begin{bmatrix} x(k) \\ \hat{x}(k) \end{bmatrix} \tag{3.14}$$

where $[K_a \quad \boldsymbol{K_b}]$ and $\begin{bmatrix} x_a \\ \boldsymbol{x_b} \end{bmatrix}$ are divided into identical dimensions, and $L_r$represents the gain of the reduced order estimator. The illustration in Figure 3.9 represents the behavior of a regulated CPS employing a lower-order estimator.

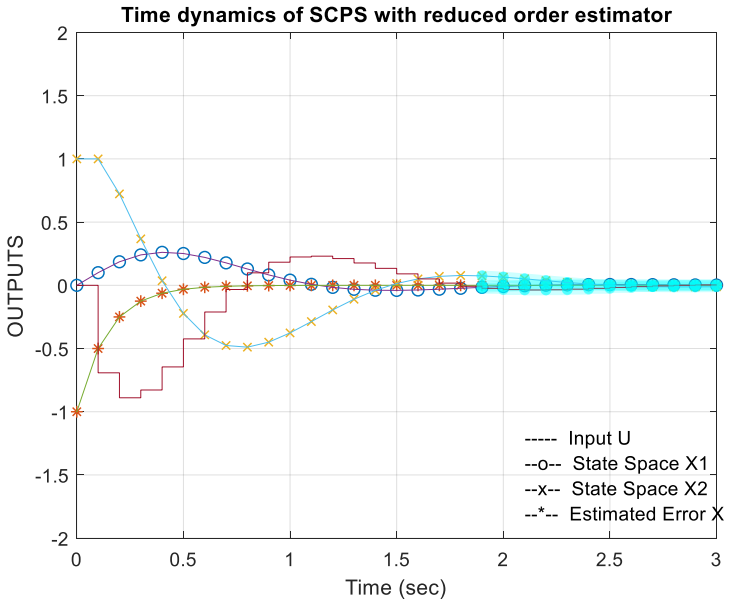


Figure. 3.9. Dynamic Performance of a Precise CPS using a Abridged Instruction Estimator

The three algorithmic variations designed for diverse estimators have been utilized across prototypes representing various procedure subtleties. The essential gears of CPS connect through strengthened, wireless, and internet networks. Given that all activities are under

computer control, the signal triggering actions needs to be adapted to align with the particular process. Figure 3.10 illustrates the simulated settling duration of individual processes using various estimators. The simulation depicts the behavior of process dynamics under ideal conditions, where activities occur without external disruptions in the communication network and with minimal conversion time delays.

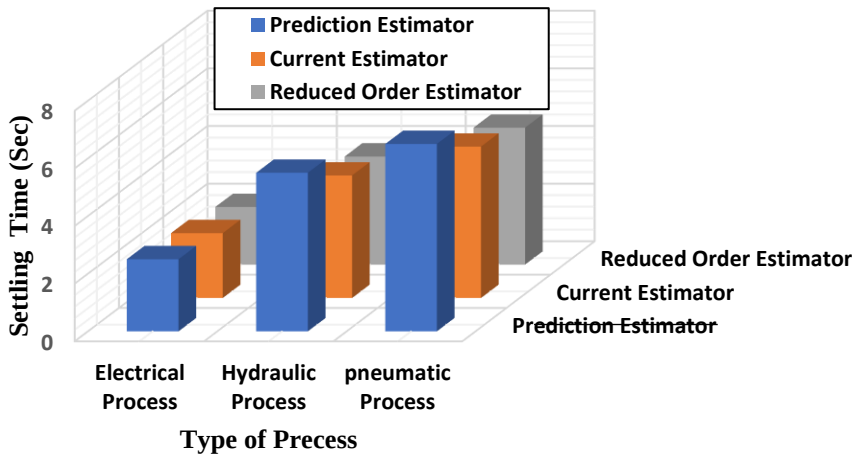


Figure. 3.10. Duration required for various processes to stabilize with distinct estimators

3.3.2 Disturbance Estimation in CPS

Within contemporary CPS, the integration of rapid computing units with mechanical, hydraulic, and electric components using diverse communication networks creates potential disruptions across computation, communication, control, and actuation stages. Anticipating and compensating for these disturbances before they happen is critical to minimize steady-state errors. It's crucial to acknowledge that disturbances could arise at any juncture within the plant or process dynamics. [123] A control signal can be introduced exclusively at the control input for managing considerable distances. This virtual signal replicates the effects of a genuine disturbance in the plant equations, maintaining an equivalent steady-state error [124]. Introducing this simulated signal, characterized by a 180° phase shift, aims to counteract the influence of the actual disturbance on the plant, leading to the mitigation of the error to zero Estimating this virtual disturbance is achievable through an estimator using the virtual disturbance equation. Figure 3.11 illustrates a setup for rejecting input disturbances.

The CPS's representation of the disturbance input in a distinct manner is provided as

$$x_d(k+1) = \Phi_d x_d(k) \tag{3.15}$$

$$w(k) = H_d x_d(k) \tag{3.16}$$

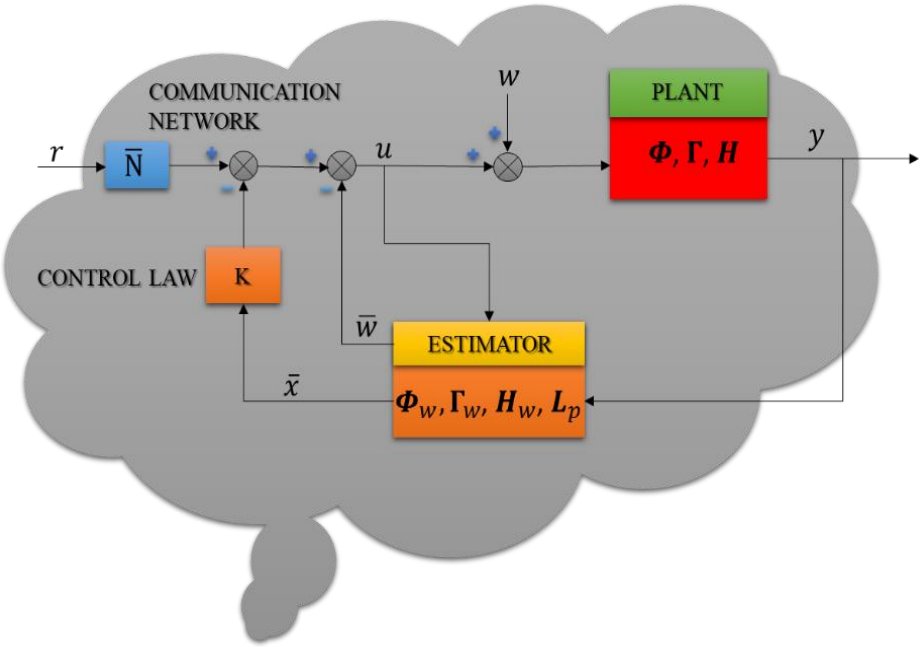


Figure. 3.11. Estimator designed to enhance the rejection of input disturbances

To estimate disturbances effectively, the system model and disturbance model are enhanced in the following manner

$$\begin{bmatrix} x(k+1) \\ x_d(k+1) \end{bmatrix} = \begin{bmatrix} \Phi & \Gamma_1 H_d \\ 0 & \Phi_d \end{bmatrix} \begin{bmatrix} x(k) \\ x_d(k) \end{bmatrix} + \begin{bmatrix} \Gamma \\ 0 \end{bmatrix} u(k) \tag{3.17}$$

$$y = [H \quad 0] \begin{bmatrix} x \\ x_d \end{bmatrix} \tag{3.18}$$

Which can also be written as

$$\begin{bmatrix} x(k+1) \\ x_d(k+1) \end{bmatrix} = \Phi_w \begin{bmatrix} x(k) \\ x_d(k) \end{bmatrix} + \Gamma_u u(k)$$

$$y = H_w \begin{bmatrix} x(k) \\ x_d(k) \end{bmatrix}$$

If there is continuous interference, equations (3.17) and (3.18) will be simplified to

$$\begin{bmatrix} x(k+1) \\ w(k+1) \end{bmatrix} = \begin{bmatrix} \Phi & \Gamma_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x(k) \\ w(k) \end{bmatrix} + \begin{bmatrix} \Gamma \\ 0 \end{bmatrix} u(k) \tag{3.19}$$

$$y = [H \quad 0] \begin{bmatrix} x(k) \\ w(k) \end{bmatrix} \tag{3.20}$$

Figure 3.12 demonstrates the neutralization of a sudden change in a process by an approximated virtual disruption.

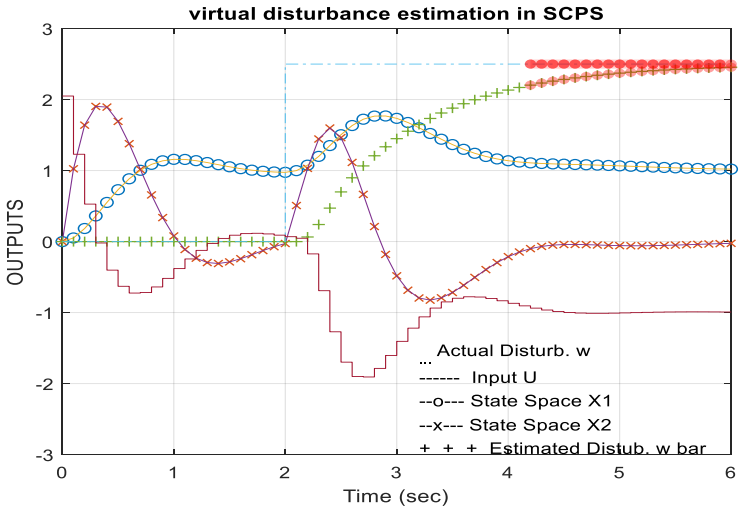
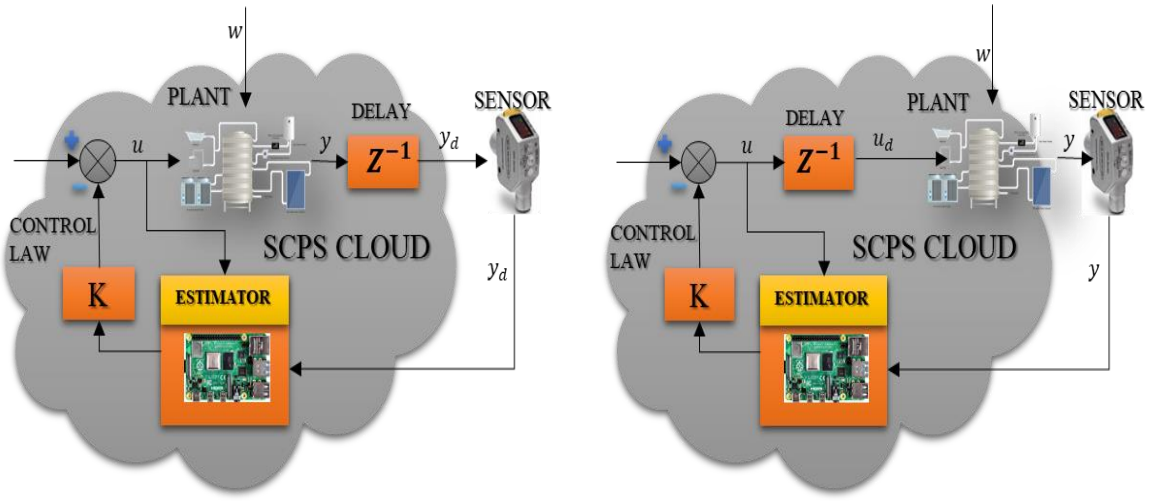


Figure. 3.12. An approximated disruption aimed at rejecting input step disturbances

3.4 Impact of Delays in Cps

In a CPS, numerous elements link via a communication network. Delays can occur at various stages within a specified process loop [125][126]. Syncing time is critical in today's computing interface, aligning computer clock speed with the dynamic of the physical process. The harmony between clock speed and process behavior is pivotal. Multiple delay sources exist in modern CPS, such as network congestion, livelocks, deadlocks, delays in converting pneumatic and hydraulic signals to electrical ones, and lag in process execution.

Delays are quite evident in contemporary CPS when many hybrid elements link via a smart network. Introducing even a single sequence delay Z^{-1} at the point within the CPS switch loop reduces structure stability if there are no adjustments made to the compensation setup. Figure 3.13 illustrates systems affected by delays.



(a) (b)

Figure. 3.13. Systems experiencing delay, including (a) delays in sensors and (b) delays in actuators.

When there is a one-cycle delay during the process, the phase margin decreases by $\lambda\omega$, resulting in decreased frequency response stability. To recompense for every sequence of suspension, the command of the state interplanetary model must be increased by an equal amount. For example, a delay in the range of $0 < \lambda \leq T$ will augment the state interplanetary prototypical by one, but a delay in the range of $T < \lambda \leq 2T$ will result in a 2-unit increase in the command of the state interplanetary prototypical. To maintain steadiness, additional poles need to be positioned in accordance with the amplified system order. The system model with a sensor delay of two cycles is given by:

$$\begin{bmatrix} x(k+1) \\ y_{1d}(k+1) \\ y_{2d}(k+1) \end{bmatrix} = \begin{bmatrix} \Phi & 0 & 0 \\ H & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x(k) \\ y_{1d}(k) \\ y_{2d}(k) \end{bmatrix} + \begin{bmatrix} \Gamma \\ 0 \\ 0 \end{bmatrix} u(k) \tag{3.21}$$

$$y_d(k) = [0 \quad 0 \quad 1] \begin{bmatrix} x(k) \\ y_{1d}(k) \\ y_{2d}(k) \end{bmatrix} \tag{3.22}$$

where y_d is the two-cycle delayed output.

The system model will be as follows for the actuator delay:

$$\begin{bmatrix} x(k+1) \\ u_d(k+1) \end{bmatrix} = \begin{bmatrix} \Phi & \Gamma \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x(k) \\ u_d(k) \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u(k) + \begin{bmatrix} \Gamma \\ 0 \end{bmatrix} w(k) \tag{3.23}$$

$$y(k) = [1 \quad 0] \begin{bmatrix} x(k) \\ u_d(k) \end{bmatrix} \tag{3.24}$$

Figure 3.14 illustrates the influence of actuator delay within CPS.

Figure. 3.15 illustrates how the delay in different processes caused by various interfaces within CPS affects its impact. The instruction of the state interplanetary prototypical increases based on the magnitude of the delay.

3.5 Control of Voltage and Frequency in CPS for DVFS Management

The execution of regulator procedures and estimation algorithms in a CPS takes place in either a mainframe tile or a federal computing cloud system. The integration of intelligence in contemporary cyber-physical structures is achieved through compact dispensation centers. Some centers are designated for the implementation of specific loops in embedded systems, while others manage real-time execution with a focus on time as the crucial limitation. The tiles allocated for the mixture procedures outlined in Section 3.2 have the flexibility to function

at diverse frequencies and voltage levels, as depicted in Fig. 3.1. The adjustment of these frequencies and voltages is dependent on the assigned tasks to the computing principal. The optimization of tasks for processing cores engaged in mixture procedures is illustrated in Fig. 3.16.

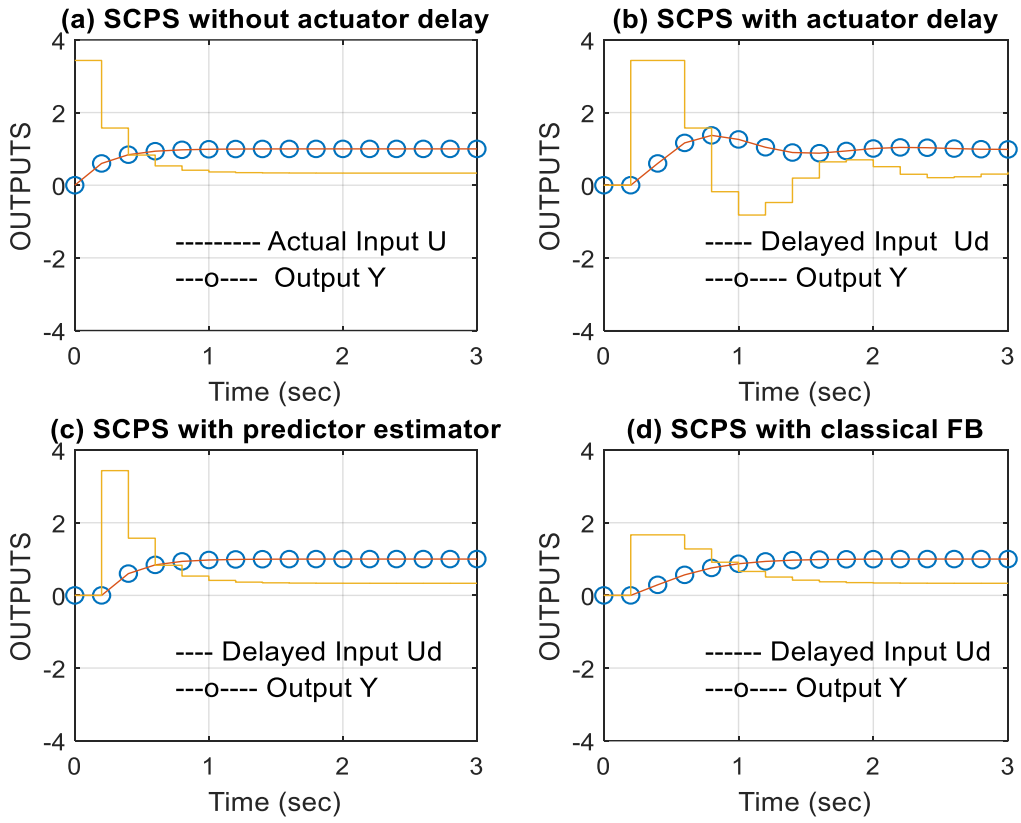


Figure. 3.14. CPS (a) without Actuator Delay, (b) with Actuator Delay, (c) with Actuator Delay in connection with Predictor Estimator, and (d) with Actuator Delay in conjunction with Classical Feedback.

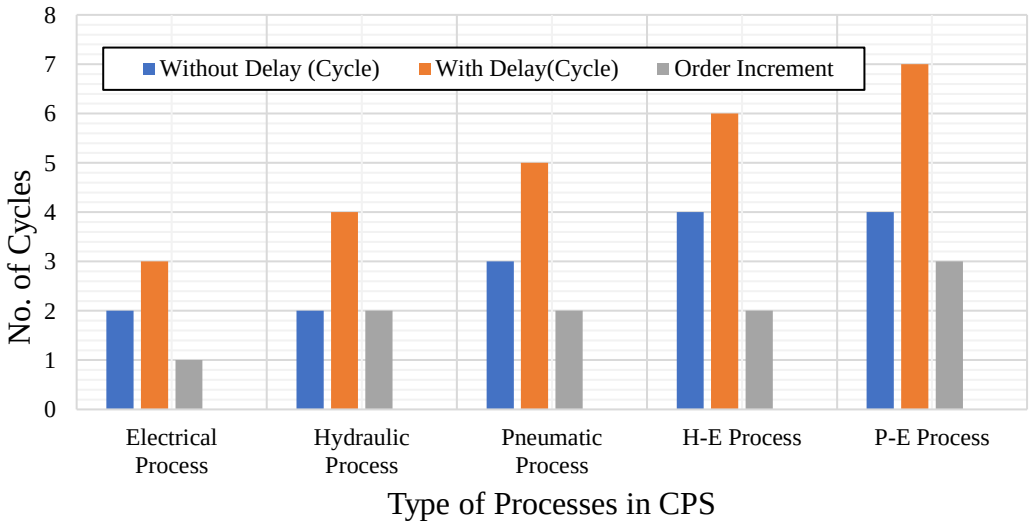


Figure. 3.15. Variation in Time Required for Various Processes in Cyber-Physical Systems

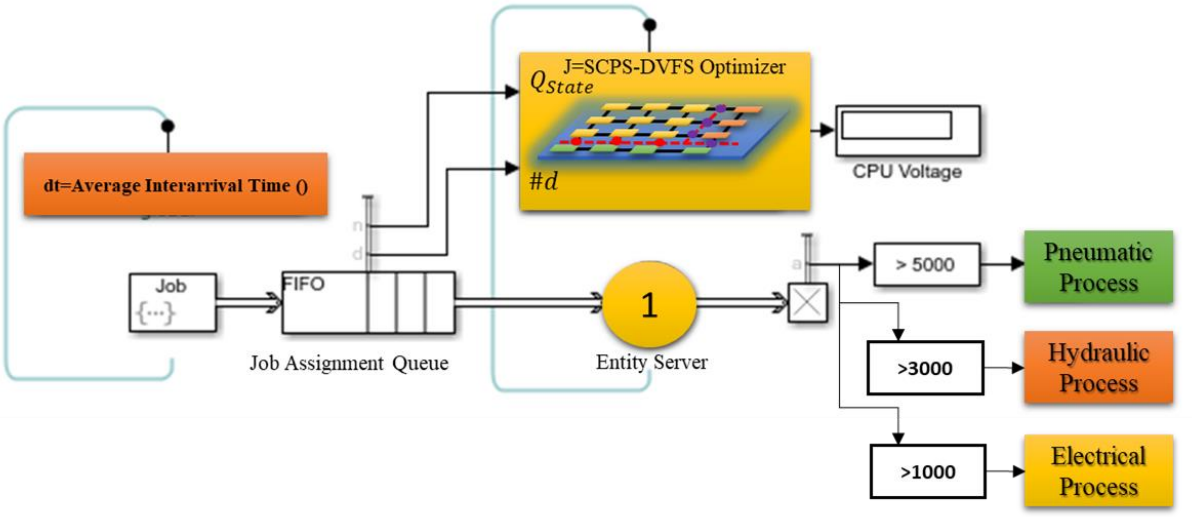


Figure. 3.16. Control of Frequency and Voltage for DVFS Management in CPS

The primary processors utilized in Cyber-Physical Systems (CPS) mainly consist of cores based on ARM Cortex-M and ARM Cortex-R. There's a growing realization that energy consumption poses a significant challenge for the computational elements. Therefore, there is a strong emphasis on developing CPS with highly efficient energy usage. Additionally, considering environmental concerns and constraints on energy resources, it's strongly advised to prudently manage and utilize energy resources within these systems. Hence, investigations within Cyber-Physical Systems (CPS) contribute to environmentally-friendly computing. In order to preserve energy when workloads are low, the timepiece occurrence and voltage supplied to these centers are abridged while maintaining quality of services (QoS). This action aims to diminish the cost function and fulfill specific performance criteria [127]

$$J = \frac{1}{2}\sum_{k=0}^{\infty}\left\{\begin{bmatrix}x(k)\\ \xi(k)\end{bmatrix}^{T} Q \begin{bmatrix}x(k)\\ \xi(k)\end{bmatrix} + u(k)^{T} R u(k)\right\} \tag{3.25}$$

Matrices Q and R are employed to allocate positive-weighted values to switch and state courses. The alterations in participation voltage for different procedures under DVFS control are illustrated in Figure 3.17.

The suggested plan enables the regulation of voltage and frequency mechanisms within a dynamic voltage and frequency system. Following the guidelines of industry 5.0, various microcontrollers and microprocessor cores will regulate all processing circuits through computational algorithms. These components will be interconnected within a CPS computational grid, as shown in Figure 3.16. The dependability of the IP-enabled computational tiles within the CPS grid is predominantly contingent upon:

i. Ensuring accurate timing or handling delays

ii. Effectively overseeing power management

iii. Implementing efficient thermal control

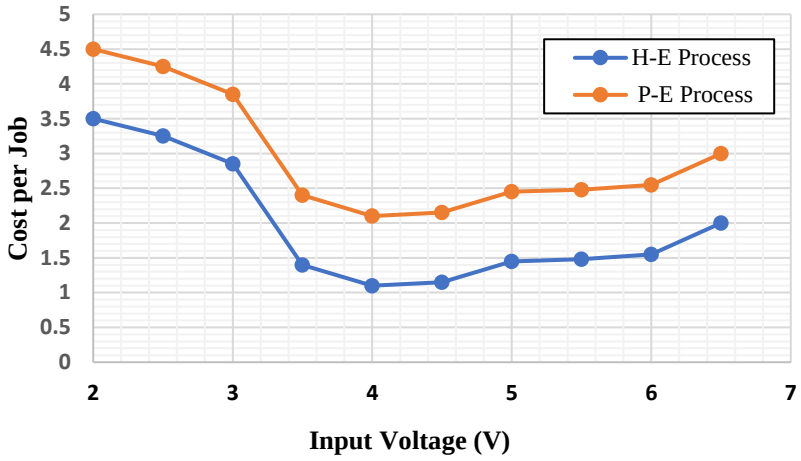


Figure. 3.17. Improving Task Efficiency through DVFS Control in CPS

An intricate automation sector must streamline three crucial factors. The variability in task demands within processing circuits, whether concentrated on a solitary core or distributed across several cores, is contingent upon the stationary and active supremacy characteristics of dispensation centers. The PID+DVFS controller, illustrated in Figure 3.18, is instrumental in regulating these aspects. Specifically, the DVFS regulator modulates the supply frequency, increasing it for intensively lively procedures and decreasing it for less active procedure loops. This approach facilitates liveliness conservation in both the control and operational facets of the procedure loop.

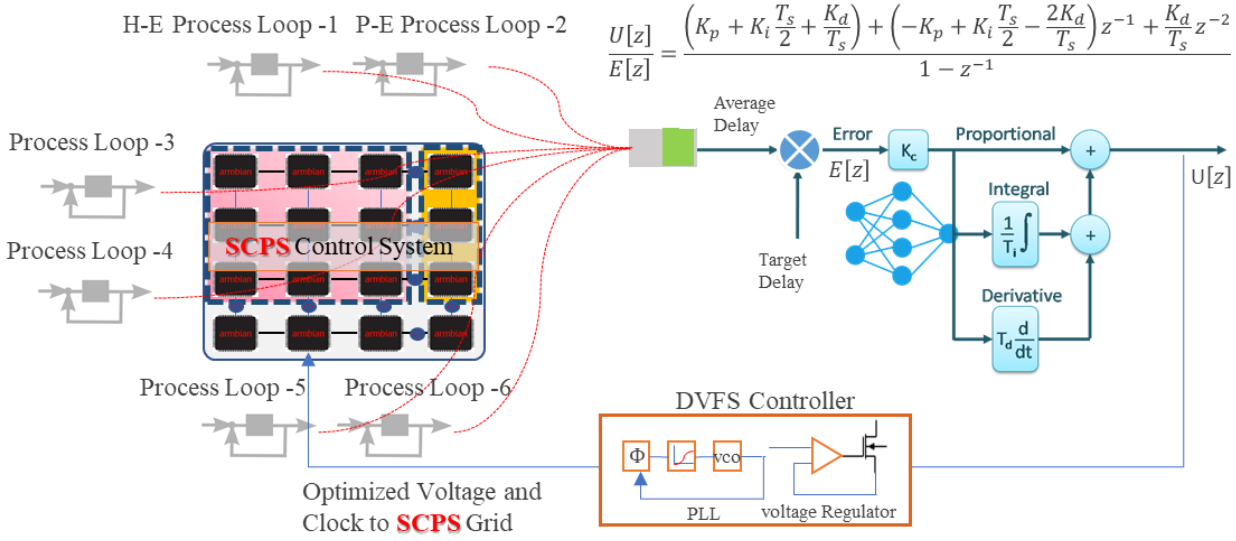


Figure. 3.18. Optimizing clock and voltage through a DVFS controller while employing CPS grid execution for diverse process loops.

Genetic procedures are utilized to modify and tailor the limitations of an interconnected PID controller. A collection comprising different system setups featuring varied parameter values competes to diminish the cost function. The parameters that successfully minimize the cost are inherited by subsequent generations based on a set of genetic principles [128]. The genetic representation of a PID controller's parameters is presented as a numerical sequence, wherein the optimized parameters for specific objective functions are recognized as focal points. Through the utilization of a genetic algorithm, these parameters are symbolically expressed as a genetic sequence incorporating various values. The associated cost for each parameter value is visually represented using color, as depicted in Figure 3.19.

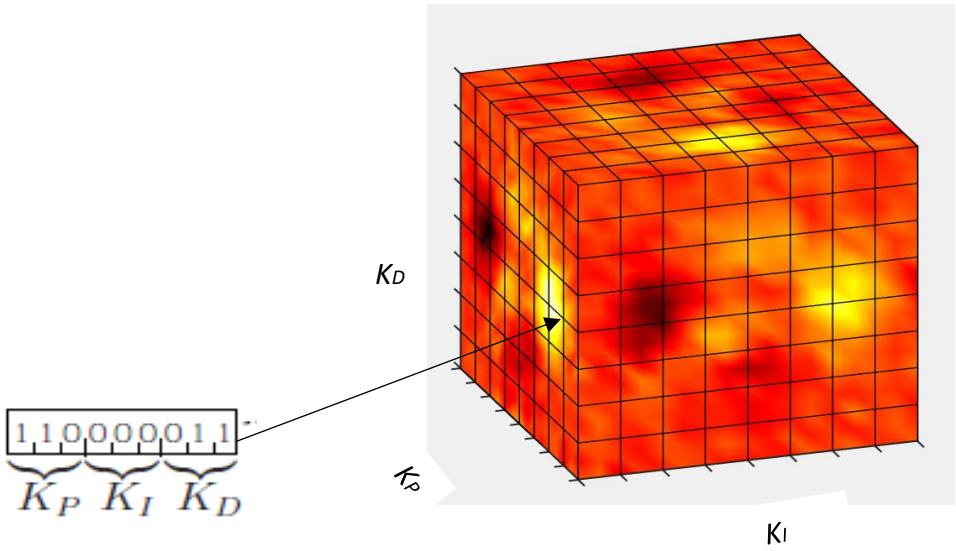


Figure 3.19. Representation of the parameter cube used in PID control

We perform a sequence of 10 iterations, wherein each iteration comprises 25 individuals within a generation. The characterization of the structure's transfer function (G) is articulated as follows:

$$G = \frac{5}{(s-1)(3s^2+5s+1)} \tag{3.26}$$

For the goal function (J), we use a mixture technique that combines the Linear Quadratic Regulator (LQR) cost function with the PID control rule to minimise the related LQR cost. The cost function employed by LQR is depicted by the following equation:

$$J = \int_0^T Q(w_r - y)^2 + Ru^2 d\tau \tag{3.27}$$

When Q equals 1 and R equals 0.001, and considering a step response with w_r=1, Figure 3.20 illustrates the alterations in the cost function throughout different generations. As generations advance, there is a consistent decline in the cost function.

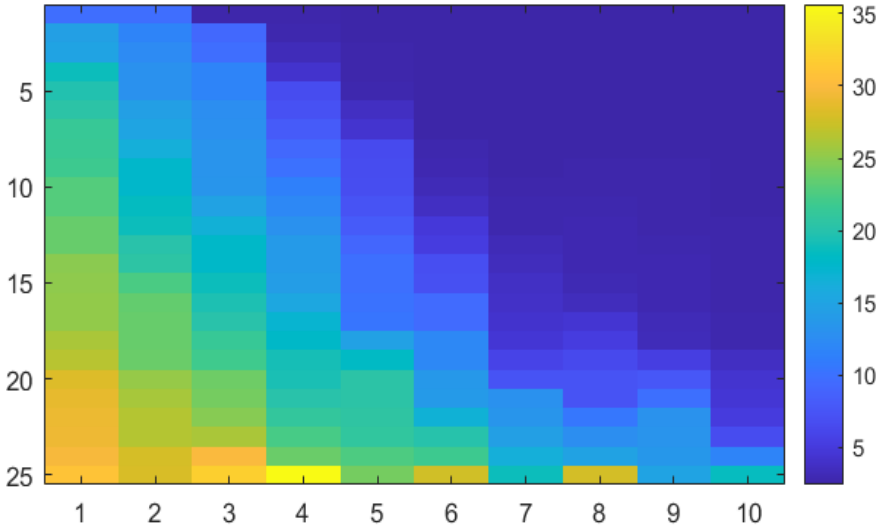


Figure 3.20. The cost function changes over successive generations due to the genetic algorithm's optimization of PID gains.

The DVFS control algorithm has the capability to be used on a solitary mainframe principal or on a group of several dispensation centers. The results depicted in Figure 3.21 shows the impression of the optimized DVFS regulator on the SCPS grid timepiece occurrence and package dormancy within the system.

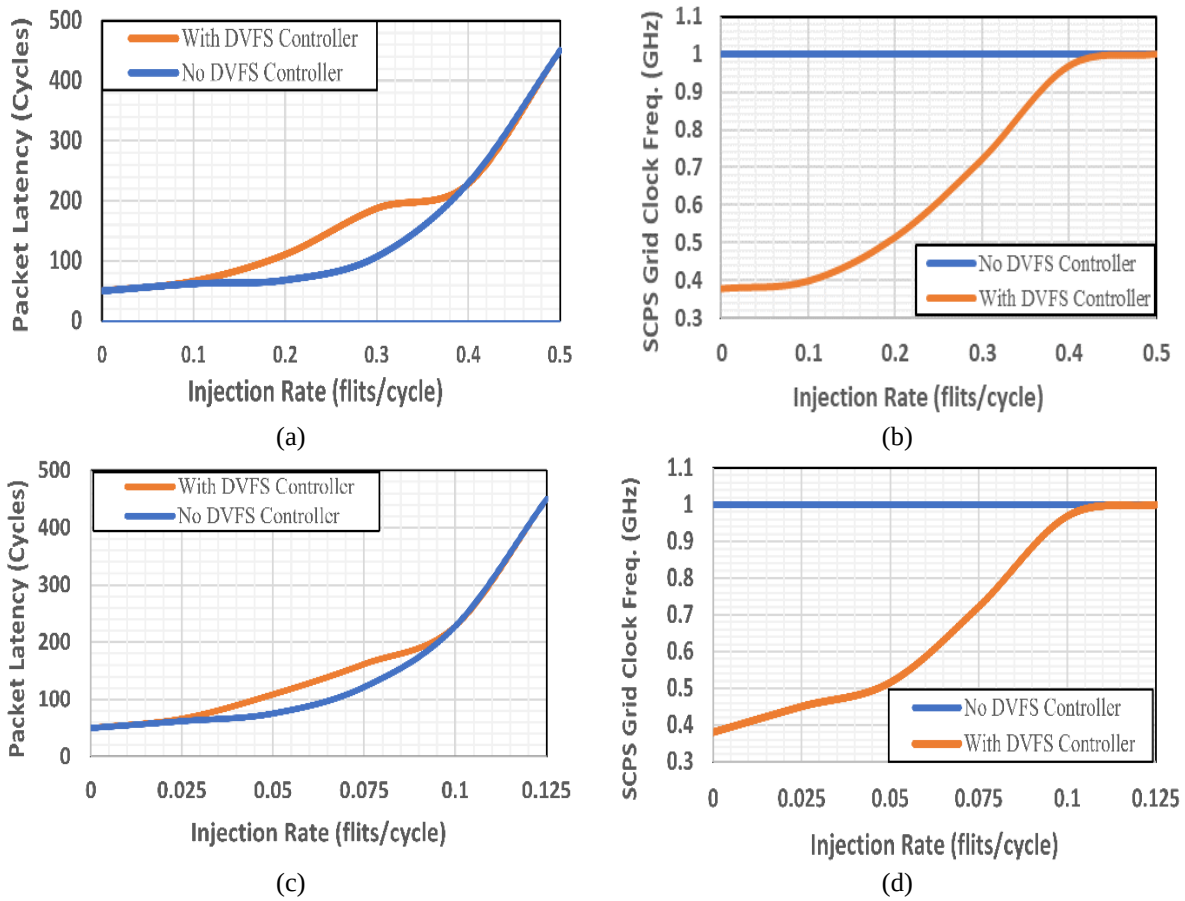


Figure 3.21 The influence of the DVFS Controller on: (a) Optimization of SCPS Grid Clock Frequency for Process Loop -1, leading to enhanced performance in packet latency, (b) Enhancement of packet latency for Process Loop -1, (c) Fine-tuning of SCPS Grid Clock Frequency for Process Loop -2, and (d) Improvement in packet latency for Process Loop -2.

3.6 Summary

The majority of CPS submissions are crucial in real-time scenarios, the dependability and steadiness of the actuator's reaction hold utmost importance. Ensuring the performance assurance of this response within mission-critical CPS directly relies on the duration it takes for a message to transfer from a sensor protuberance to the actuator protuberances through cyberspace. In this chapter, significant concerns regarding the creation of an intelligent CPS are addressed. These concerns pertain to the segmentation of processing elements in the VFI concerning tasks such as control algorithm implementation, compensator design, estimating and compensating for disturbances, sensor and actuator delays, as well as optimizing energy consumption through DVFS control.

CHAPTER 4

SYNERGIZING EDGE COMPUTING WITH BLOCKCHAIN FOR CYBER-PHYSICAL SYSTEM INTEGRATION

4.1 Introduction

Blockchain, as a fundamental technology used in managing decentralized systems such as smart grids and healthcare, has garnered significant interest. However, due to its high resource demands and limited scalability, especially with frequent, resource-intensive transactions, its application on resource-constrained mobile devices is restricted. One potential solution lies in leveraging edge computing, allowing these devices to delegate processing tasks to cloud resources. Integrating blockchain with edge computing ensures scalability, secure transactions, consistent access, distributed computing, and uncompromised storage. Overcoming challenges related to reliability, adaptability, and resource management is crucial for successful integration. Despite these efforts, there remains a need for further research to tackle issues concerning confidentiality, flexibility, and reliability, essential for establishing a functional, secure decentralized data storage system. This chapter emphasizes utilizing edge computing to create an Internet of Things (IoT) framework that fulfills the safety and scalability standards needed for integration. It integrates peer-to-peer and blockchain technologies for this purpose. Additionally, existing blockchain and associated technologies have been explored to propose solutions addressing concerns such as secrecy, reliability, and scalability, aiming to effectively integrate blockchain into IoT systems.

The swift growth of the IoT and the massive number of interconnected devices, totaling in the hundreds of billions, have resulted in the creation of a vast amount of data. As these devices interact within networks, the data traffic experiences an enormous surge. However, due to limited bandwidth, it is impractical to transfer and analyze all this data in the cloud. Moreover, these individual devices are highly susceptible to breaches; their limited computing power,

storage, and network infrastructure make them more vulnerable to security threats compared to other edge nodes such as smartphones, PCs, and tablets. These challenges serve as strong motivators for both academic and business sectors to innovate and develop advanced cloud computing technologies.

Placing an edge server in proximity to data-generating devices like smartphones, sensors, and smart devices enables data processing via edge computing. This approach enhances the performance of real-world applications that require low-latency processing and alleviates the strain on cloud servers. A prime illustration of real-time edge computing is evident in self-driving cars. These vehicles necessitate instantaneous decision-making without the option of relying on cloud instructions due to minimal latency tolerances. Furthermore, industries like interconnected factories or hospitals are cautious about privacy concerns and, therefore, opt to evaluate or modify sensitive data locally before uploading it to the cloud, rather than transferring the entire information.

Combining edge computing with blockchain tech enables safe management of network access, memory, and decentralized computing resources at the edge. This combination allows secure proximity to computational, storage, and network control capabilities. However, merging blockchain and edge computing networks necessitates addressing challenges related to scalability, self-organization, asset integration, strategic resource planning, and specific security concerns [129] before they can be effectively applied to edge computing scenarios.

Successfully integrating systems requires addressing essential security concerns, resource management issues, feature integration, and scalability improvements, among other critical factors. Several research projects have been initiated to resolve these challenges. These investigations have indicated that addressing privacy, authenticity, and flexibility problems is crucial before effectively employing blockchain for decentralized data storage in the Internet of Things. Further exploration into resolving these issues is necessary since blockchain solely guarantees pseudonymity, while integrity relies on the number of ethical miners and the intricacy of Proof of Work (PoW), and adaptability is limited by its complexity [130].

Alongside their significant potential, edge computing, IoT, and blockchain each present their own set of limitations and difficulties, which can complement each other when integrated. Despite the promising technological advantages of blockchain, meeting strict computational, storage, and bandwidth demands for nodes is essential to achieve higher transaction speeds while upholding top-tier security standards. Although the decentralized nature of edge

computing is advantageous, its widespread application across networked devices exposes it to potential threats. Security issues include the distribution of computing tasks, external storage usage, and managing decentralized network governance. While IoT devices have the potential to enhance global connectivity, intelligence, and efficiency, they are constrained by limited computing power, low energy resources, and storage capabilities.

The primary contributions of the chapter include:

i. Evaluating contemporary blockchain technology to formulate a robust architectural approach capable of providing adequate security and scalability.
ii. Analyzing current blockchain technology to tackle issues related to data integrity.
iii. Exploring supplementary protocols and methods that enhance anonymity beyond pseudonymity.
iv. Thoroughly investigating various protocols and techniques aimed at enhancing confidentiality in IoT applications.

4.2 Proposed Framework

Edge computing is an open framework designed to facilitate IoT, 5G, AI, and other technological progressions. It is perceived as a strategy to mitigate various security concerns. The distributed architecture of Edge incorporates computation, monitoring, storage, connectivity, and communication in close proximity to services and data sources [131]. This configuration enhances security by introducing an additional layer of protection, safeguarding interconnected systems from the edge server to the device. In this model, security functions locally at the edge, as opposed to being managed remotely [132].

Even the tiniest and least resource-intensive networked devices are overseen by edge nodes employing various security measures. This involves establishing a reliable distributed foundation and execution site for numerous services, monitoring login details, conducting virus scans, and promptly distributing software updates [133]. The Edge ensures a secure connection by detecting, verifying, and reporting attacks. It has the capability to recognize and isolate attacks through the continuous monitoring of the security status of nearby devices [134].

If any security issues are identified, the edge responds promptly by deploying trusted architectural components, enabling immediate real-time event response. The detection and response to attacks occur within the local environment, minimizing service disruption. The challenges of implementing blockchain in low-cost endpoints stem from scalability, flexibility, capacity, and resource distribution issues within edge computing networks. Nonetheless,

blockchain holds the potential to address various security concerns and challenges in edge computing. Consequently, the convergence of blockchain is proposed as a reliable and secure connectivity solution to bolster edge computing [135]. It is also considered a potential remedy for several technological issues in edge computing and the IoT.

One of the latest strategies for integrating blockchain technology into the IoT edge involves a hybrid architecture combining cloud and blockchain elements. [136] This approach addresses the transmission of a significant portion of IoT data within the conventional IoT cloud-edge framework. Where public oversight is necessary, the blockchain is used at the application level [137]. The goal is to combine existing cloud and edge architecture with blockchain technology's permanent data storage capabilities and low-latency data transport capabilities. As shown in Figure 4.1, the authors offered a composite cloud-blockchain architecture as a remedy, which would lessen the necessity of storing all produced events on the blockchain. Even though the structure depicted in the picture uses the accountability aspects of the blockchain, that does not include distributed SLA enforcement for safety at the IoT edge[138].

Figure 4.1 visually demonstrates how blockchain technology is effective and practical in both wireless and fixed edge computing setups. In this network architecture, each element performs tasks such as data collection, storage, service delivery, and sharing through applications that leverage blockchain technology. The validation of every operation is ensured through the mining process employed in the blockchain.

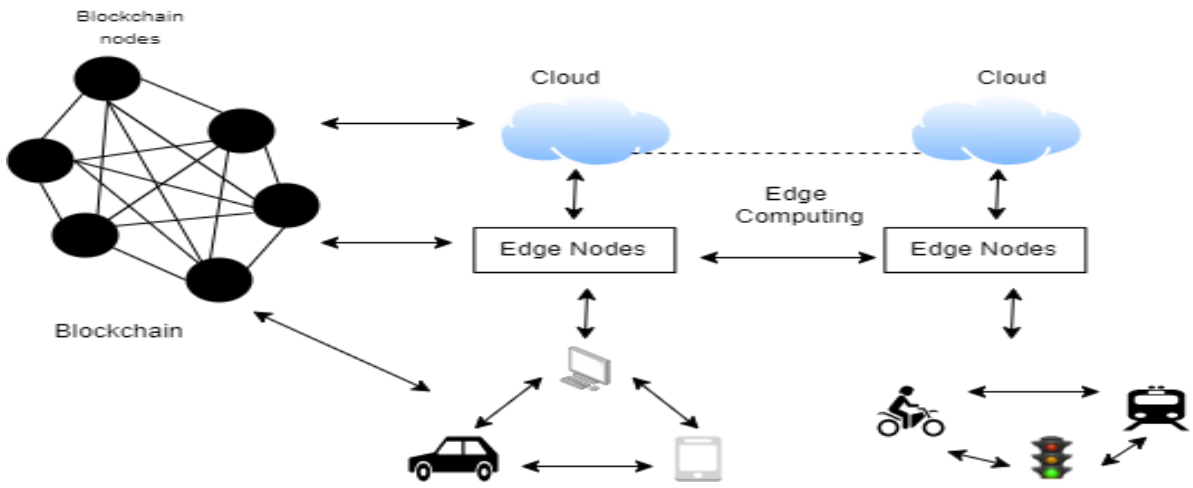


Figure 4.1. Combining Edge Computing and Blockchain: A Hybrid Architectural Approach

To tackle the problem of growing record sizes exceeding storage limits caused by a rising block creation rate, the solution involves utilizing edge computing for ledger storage. Verified transactions, performance metrics, node details, and communication among nodes will be

stored at the edge computing nodes across the network. Meanwhile, transaction verification and block creation will adhere to standard blockchain techniques. In this approach, IoT devices function as blockchain nodes but transfer and store records on edge computing nodes during each transaction stage. The design incorporates smart contracts for implementing network transaction data validation, storage systems, service administration, and edge device activation. The ledger is accessible to edge devices, enabling them to update it with the addition of new blocks, resulting in quicker and lower-latency access to storage. The integration of blockchain and edge computing not only enhances the efficiency and reliability of IoT devices but also improves the overall performance of the entire edge network.

Edge devices will employ the data encapsulation method in alignment with the service requirements of the application. This implies the potential utilization of device data, encompassing aspects like power demands, availability, and physical states, to ensure consistent provision of the appropriate Quality of Service. Additionally, the amalgamated data derived from edge devices holds the potential to enhance operations and resource utilization in various sectors, including power, healthcare, autonomous vehicles, manufacturing, and others.

Figure 4.2 illustrates the composition of our architecture, consisting of three tiers: the cloud layer, the edge layer, and the IoT layer. P2P device networking has been incorporated into every layer of the framework, mirroring the structure of edge computing. This integration enhances processing and storage capabilities.

Figure 4.3 depicts how blockchain proves its efficiency and feasibility in various edge computing setups, whether mobile or static. In this network design, every unit employs blockchain-powered applications for data gathering, storage, service provision, and data exchange. The authentication of all activities occurs via the blockchain mining process.

i. **IoT Device Layer:** The proposed framework aims to integrate edge computing and blockchain to effectively store and manage IoT data, as depicted in Figure 4.2. The system is structured into layers, segregating the application layer, housing low-resource IoT devices, from the resource-intensive blockchain activities. We have detailed the procedures required for each level of the framework. Subsequently, we delve into the implementation of three fundamental IoT needs: network traffic management and control, external storage systems, and compute offloading. A diagram accompanies the description of service deployment, illustrating the integration of the framework's

solutions for confidentiality, reliability, and flexibility. Peer devices can communicate only if the server furnishes a common secret key in this mode.

On the flip side, devices and servers have the capability to participate in public blockchain activities via peer-to-peer communication. The limited capabilities of end devices in this scenario prompt the involvement of more potent servers situated in the upper tiers, at the edge, and in the cloud within the blockchain. Servers handle intricate processes, while end devices manage simpler tasks such as exchanging transaction summary files with peer nodes or receiving firmware upgrades. Figure 4.3 illustrates how edge servers can securely offer substantial external storage and high computing capacity to IoT devices on demand. This characteristic is shared by both centralized and decentralized forms of communication. Additionally, the close positioning of edge servers to end users enables them to swiftly address requests from IoT applications.

Because of the decentralized structure of peer-to-peer connections, devices can efficiently shift resource-intensive tasks such as processing or storage to an edge server or a nearby peer with greater capabilities. This results in much faster response times. By offloading these tasks, nodes are freed from the burden of heavy processing, as they only need to store a specific portion of the chain necessary for their transactions rather than the entire chain. Additionally, blockchain enables seamless communication among smart devices from different suppliers, overcoming the limitations imposed by the absence of standards.

ii. **Edge Layer:** Expanding the cloud to enhance service delivery speed and reduce latency is facilitated by the edge layer. Edge servers possess the capability to internally distribute information, allowing for synchronized data processing and duplicate data storage. This empowers smart IoT devices with the necessary resources. Figure 4.3 illustrates the utilization of blockchain through servers positioned at the edge layer of the network, ensuring a distributed platform with secure data transfer. The implementation involves edge nodes dynamically eliminating themselves, achieving self-organization. These edge nodes perform basic analysis on their own and neighboring nodes, transmitting messages within the network. Moreover, they oversee data, transmitting real-time data analysis to either back-end devices or a distributed cloud for extended storage, contingent on the situation. The P2P structure within this tier sets up a reservoir of mobile resources to facilitate rapid processing, temporary storage, and analytical functions.

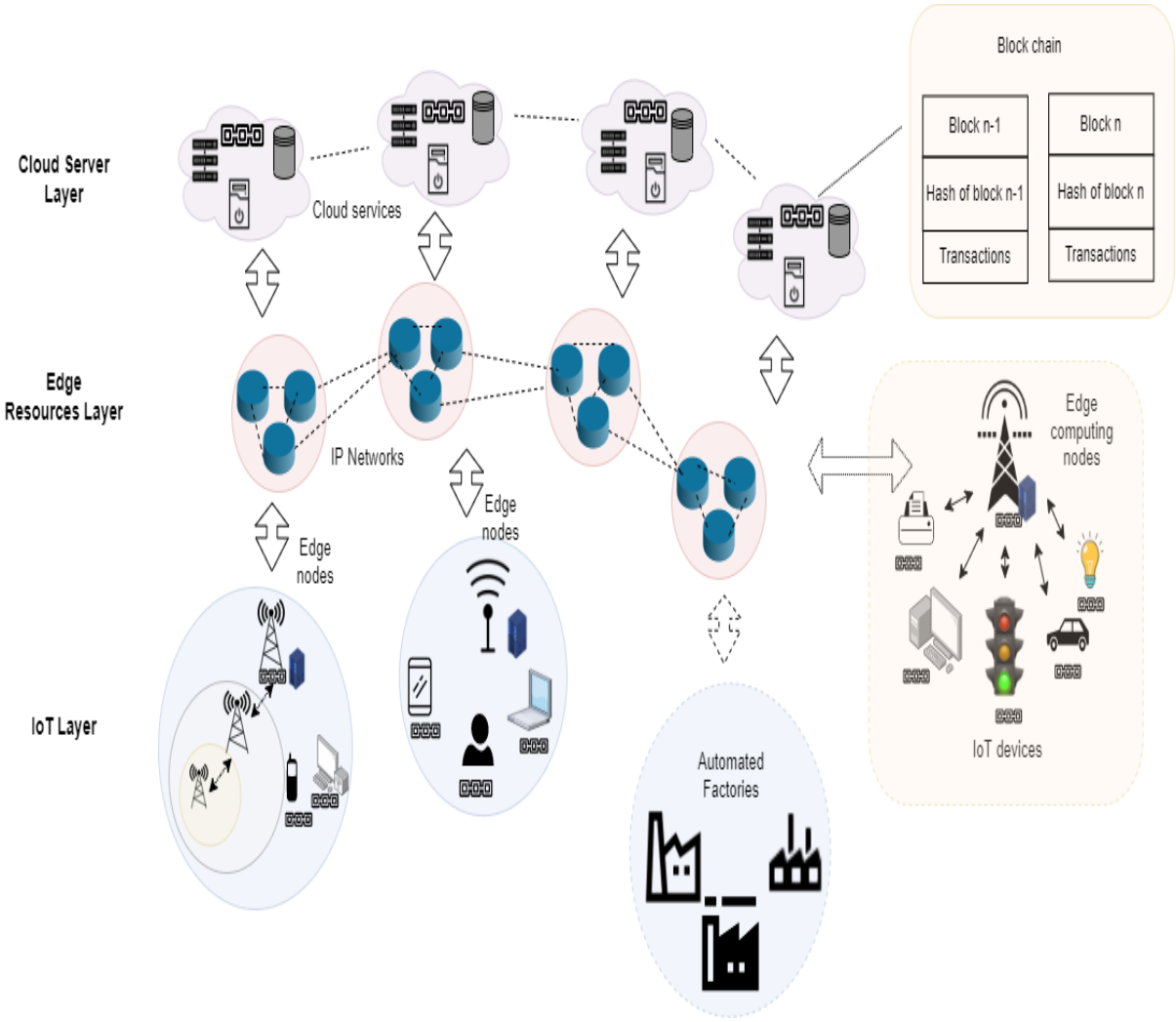


Figure 4.2. A suggested framework for the incorporation of edge computing and blockchain.

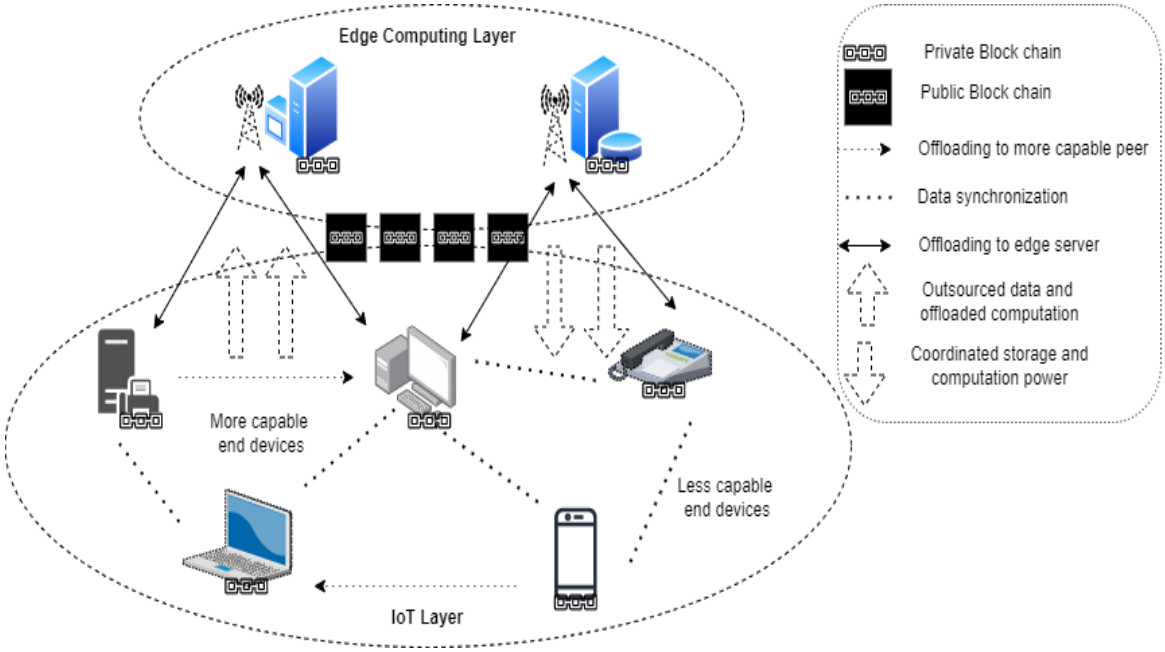


Figure.4.3 The functions of the IoT device layer

If the computing requirements exceed the capacity of the edge servers, they have the option to delegate certain tasks and leverage cloud services. The validation of device claims related to computing and storage requirements is carried out through the consensus processes of the blockchain. Employing smart contracts on a public blockchain, such as Ethereum, that utilizes straightforward consensus mechanisms provides a straightforward method to ensure reduced latency and increased throughput for a diverse set of peer-to-peer networked edge servers and distributed cloud resources.

The speed at which the CPU functions is determined by the CPU cycles, denoted as f_m. Contemporary mobile CPU architecture incorporates an adaptive and intelligent dynamic frequency and voltage scaling technology. This technology allows for the adjustment of CPU cycles, facilitating both an increase or decrease in processing speed and energy consumption. Notably, the computing power of a mobile device is limited by a peak value, f_{max}. This constraint impacts the value of f_m.

A calculation task is defined by the formula $D \triangleq (d, c, T)$, where d represents the data size of the task, c is the quantity of CPU cycles needed for computing one bit, and T is the maximum delay allowable for the task. The local execution time of a computing task D can be expressed as follows:

$$T^L = dc/f_m \tag{4.1}$$

This indicates that a higher number of CPU cycles are necessary to decrease the latency of execution.

The effectiveness of computing greatly depends on how much power is consumed during local execution, which is a crucial factor for performance, particularly given the energy limitations of devices. The energy required for each CPU cycle is determined by, ζf_m^2, where ζ represents the effective switching capacitance, depending on the chip architecture. The energy expended to accomplish task D utilizing f_m CPU cycles can be computed as follows:

$$E^L = \zeta dc f_m^2 \tag{4.2}$$

If the latency surpasses the specified threshold T^L or the device's battery capacity falls below E^L, it is advisable to transfer the task to edge servers for processing, as per (4.1) and (4.2). Alternatively, if neither of these conditions is met, the computational task can be effectively handled through local execution.

The individual user's edge setup consists of a single device paired with one edge server. F_e, denotes the computing resource utilization capability of the edge server. The device offloads the entire computational task to the edge server for processing. As a result, the computation time for the task is expressed as such:

$$t^{F,computing} = dc/F_e \tag{4.3}$$

Due to the necessity of a wireless connection for offloading, the overall duration for task execution encompasses both the total time spent on task calculation and the total time devoted to task transmission. This can be expressed as follows:

$$T^{F,s} = \frac{dc}{F_e} + \frac{dc}{r_s} \tag{4.4}$$

The symbol r_s denotes the data rate of the wireless link connecting the device to the edge server.

Furthermore, besides the computation being offloaded, energy consumption involves two additional elements: the energy used for computation and the energy expended on wireless transmission. The overall energy consumption can be expressed as:

$$E^{F,s} = \zeta dcF_e^2 + p\frac{dc}{r_s} \tag{4.5}$$

In the scenario where multiple devices are connected to a single edge server in a multi-user edge system, they can concurrently transfer tasks to the edge server. In such cases, only a fraction of the edge server's processing capabilities is assigned to each device. The computational workload for a given device, denoted as D_i, is defined as $D_i \triangleq (d_i, c_i, T_i)$, where d_i represents the task's data size, $c_i$denotes the number of CPU cycles needed to compute one bit of the operation, and T_i indicates the maximum acceptable latency. The computing resources allocated to device i's by the edge server are labeled as f_e^i. Considering wireless transmission during the offloading procedure, the total execution time for device i's tasks can be expressed as:

$$T_i^{F,m} = \frac{d_i c_i}{f_e^i} + \frac{d_i}{r_i^m} \tag{4.6}$$

The data rate of the wireless connection, denoted as r_i^m, between device i and the edge server determines the energy consumed by device i to execute the offloaded calculation task. This energy can be expressed using the equation:

$$E_i^{F,m} = \zeta d_i c_i (f_e^i)^2 + p_i \frac{d_i}{r_i^m} \tag{4.7}$$

Here, p_i represents the transmission power of device i.

Our method employs Kasireddy's off-chain state channels to delegate computation tasks. This allows the blockchain to handle increased amounts of data and intricate tasks. Implementing this method into our system improves the scalability of the blockchain by tackling adaptability challenges, enabling specific operations to take place away from the main blockchain network. The process involves three stages, utilizing secure cryptographic procedures, as depicted in Figure 4.4, resulting in notable improvements in speed and cost reduction.

Initially, smart contracts are used to lock specific blockchain data in Step 1, enabling participants to modify transactions without immediate blockchain commitment in Step 2. Subsequently, in Step 3, the parties communicate the status to the blockchain to finalize agreements, ensuring secure communication and unlocking the state. Notably, only Steps 1 and 3 are publicly recorded on the blockchain; Step 2, where most tasks occur, remains independent of blockchain involvement.

Less powerful IoT devices leverage off-chain state channels to lock blockchain segments necessary for their transactions in Step 1. Rather than engaging with the entire blockchain, these devices can update firmware or exchange data with others based on transaction summaries from Step 2. Upon instant transmission of state modifications to the main chain, the state channel is closed, and the locked state is unlocked.

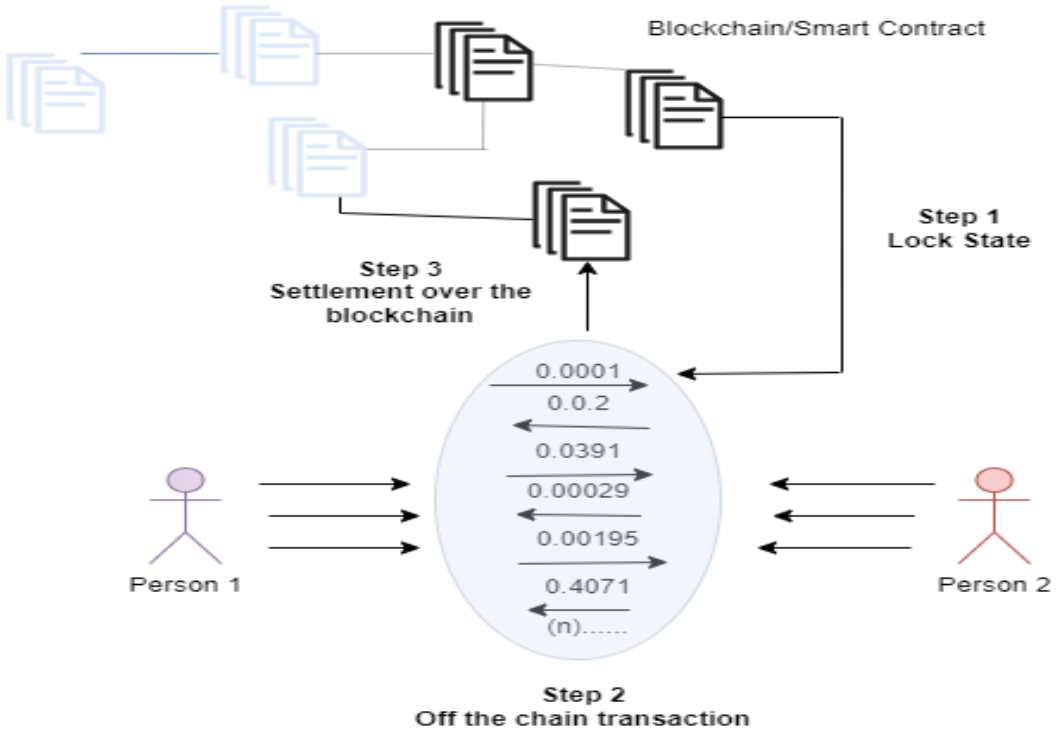


Figure.4.4 Method for off-chain state channel

iii. **Cloud Layer** : The cloud layer serves as the backbone for data analysis and storage services, akin to a blockchain node capable of mining. Its distributed blockchain relies on consensus to ensure top-tier computing services with extensive storage and processing capabilities. The integrity service ensures that blockchain nodes are rewarded for good behavior and penalized for misconduct. Cloud layer nodes operate independently from edge layer nodes, and their use of blockchain ensures seamless replication of exchanged data.

Blockchain-enabled data integrity: Figure 4.5 illustrates a hypothetical Data Integrity Service (DIS) that utilizes blockchain technology to ensure data integrity. Within DIS, there are two user categories: data owners and consumers, each utilizing their respective applications. The cloud storage service (CSS) functions as both an independent cloud service and a node within the blockchain network. Through matching public keys, owners and consumers are uniquely identified within the system. When they become part of the blockchain network, applications belonging to data owners (DOAs) and data consumers (DCAs) create interconnected sets of private and public keys. Authentication of each node occurs through the public key, with access granted via the private key. Transactions within the system are only permitted if the node's account holds sufficient funds. While both DOAs and DCAs have the option to join the network as miners, the limited processing capacity of DOAs often makes it challenging and unnecessary for them to earn deposits. Conversely, DCAs may choose to engage in mining activities based on their hardware capabilities and available funds.

In our proposed integrated architecture for secure data storage leasing, we utilized Ethereum and smart contracts to offer a practical solution for data security. This approach entails encrypting all data from end devices before transmission to ensure privacy. Within a peer-to-peer network, peers utilize Proof-of-Space to distribute their storage and validate deposits' authenticity. By allocating a substantial portion of memory or disk space to complete assigned tasks, a prover demonstrates their commitment to the service. This concept of 'PoSpace' signifies this commitment. Alongside committing the required space, substantial information exchange between the prover and verifier is essential to surpass the PoSpace barrier.

Peers must initially undergo proof of space verification to authenticate their transactions before participating in a blockchain transaction. IoT users employed smart contracts to store transactions within the system. Transactions are generated when data is encrypted locally to prevent unauthorized access and then released to the P2P network through owner clients who have specified their requirements and inquired about associated costs. Miners evaluate the

requirements of users and the services at their disposal to offer customers essential storage space for lease during transactions. Internet of Things (IoT) gadgets have the option to delegate data storage responsibilities to uphold a decentralized peer-to-peer storage system. This system operates under the governance of smart contracts, which establish suitable incentives and consequences.

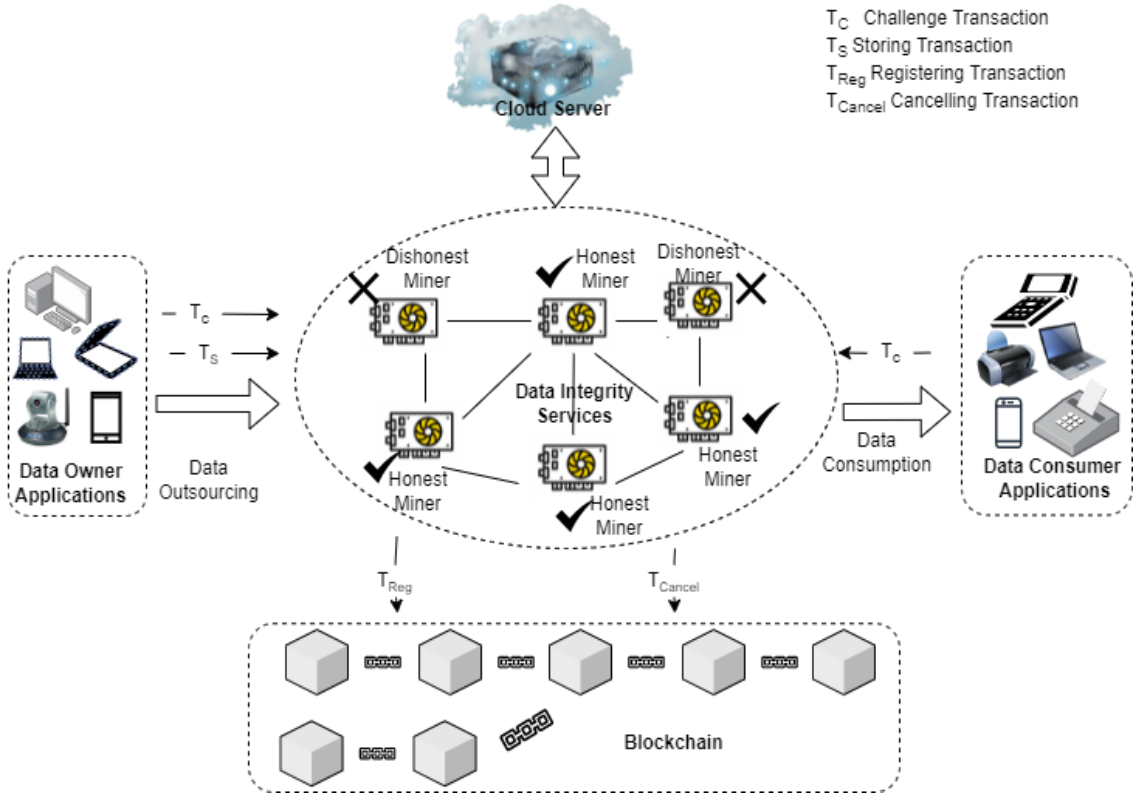


Figure.4.5. Data Integrity using Blockchain

IoT users can initiate challenge transactions to compel miners storing outsourced data to provide proof and record it on the blockchain for data verification. If the computed proof fails verification, miners, acting as data servers, face consequences, including a refund of the initial deposit made during IoT user registration. Miners retain the option to withdraw pledged space by submitting a canceling transaction and reclaiming the deposit received upon registration at any time.

4.3 Results and Discussion

We employ an eleven-block generation cycle within a relay network, consisting of intervals ranging from 25 minutes down to 0.5 seconds. For every cycle, we conducted simulations for 10,000 blocks. We have used Blockchain Simulator available online publically*.

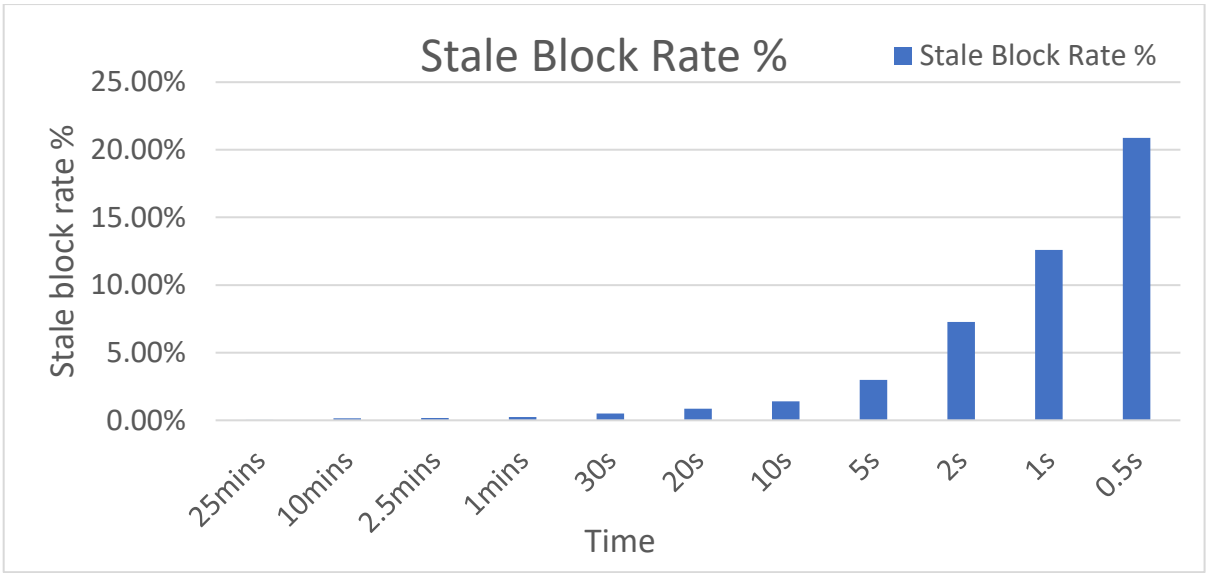
(* https://arthurgervais.github.io/Bitcoin-Simulator/index.html)

The results of these simulations are presented in Table 4.1 and Figure 4.6.

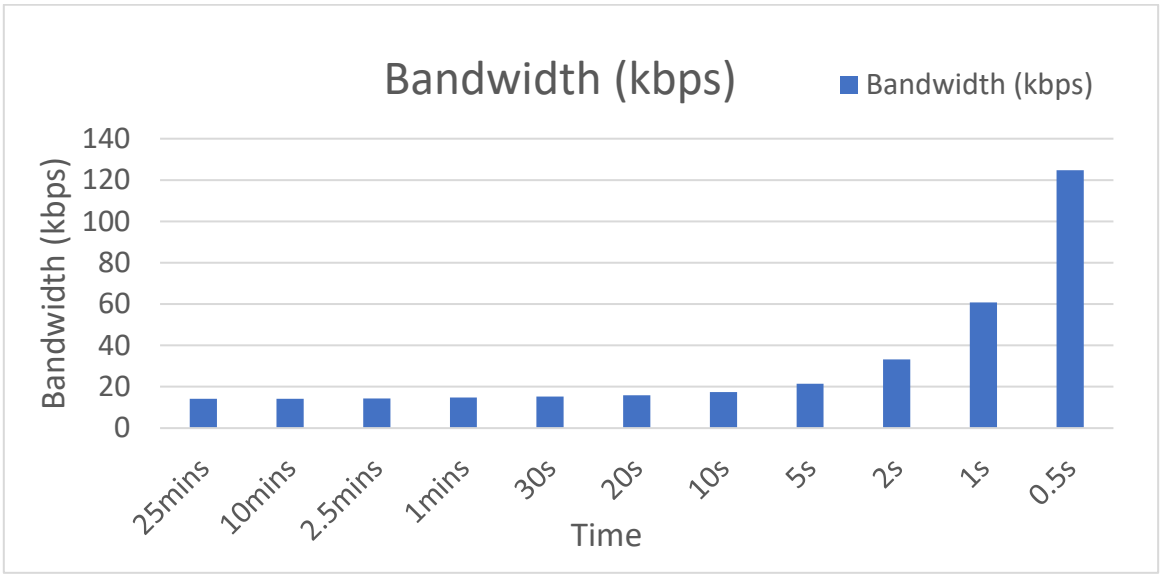
Shorter intervals for creating blocks lead to increased network traffic, as evidenced by the need for block propagation to occur faster than block creation in 90% of cases, as dictated by decentralization standards. However, IoT devices, constrained by limited bandwidth, struggle to meet this requirement, resulting in prolonged block propagation times beyond the specified threshold. Consequently, the heightened demand for bandwidth on IoT devices due to block propagation contributes to higher rates of stale blocks when block creation intervals are shorter.

Table 4.1. Effect of block generation interval on the throughput and stale block rate in a relay network

Interval	**Block Propagation Delay**						**Stale Block Rate %**	**Bandwidth (kbps)**
	Mean	Median	10%	25%	75%	90%		
25mins	30.11	22.5	8.22	13.94	39.56	42.99	0.02%	14.1
10mins	12.12	9.41	3.52	6.09	15.52	17.8	0.13%	14.16
2.5mins	3.26	2.6	1.16	1.75	3.94	4.71	0.15%	14.38
1mins	1.48	1.3	0.67	0.95	1.75	2.22	0.29%	14.64
30s	0.92	0.84	0.49	0.64	1.08	1.38	0.52%	15.3
20s	0.73	0.69	0.42	0.53	0.85	1.14	0.82%	15.79
10s	0.55	0.53	0.36	0.41	0.63	0.89	1.59%	17.85
5s	0.46	0.45	0.32	0.36	0.53	0.8	3.05%	21.6
2s	0.42	0.39	0.28	0.34	0.47	0.74	7.10%	33
1s	0.4	0.38	0.27	0.33	0.43	0.73	12.52%	52.97
0.5s	0.42	0.38	0.26	0.33	0.42	0.84	21.10%	94.53



(a)



(b)

Figure. 4.6. Effect of block generation interval on: (a) Stale Block Rate (b) Bandwidth (kbps)

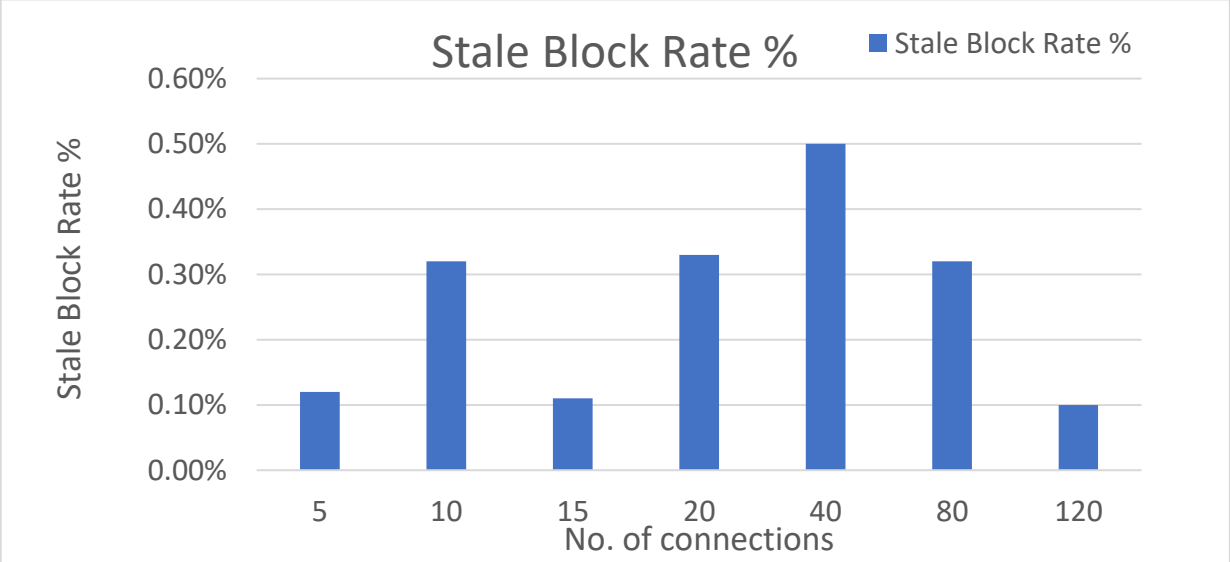
We additionally utilize a seven-phase generation process involving varying numbers of IoT devices: 5, 10, 15, 20, 40, 80, and 120. In each phase, we simulated the production of 10,000 blocks. The outcomes of these simulations are presented in Table 4.2 and Figure 4.7. As the number of IoT devices increases, along with the frequency of block creation, both throughput and average network traffic per device experience an uptick. However, this also leads to longer block propagation delays due to elevated stale block rates and increased network usage.

Considering various block sizes and production intervals, we investigated how the number of miners impacts throughput and stale block rates. We analyzed five different miner counts: 16,

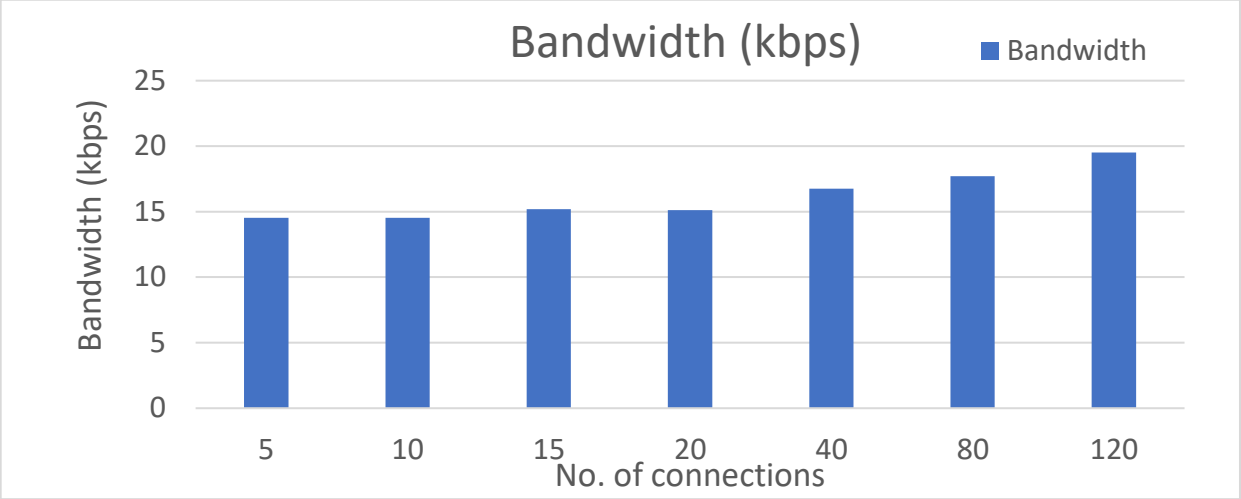
32, 64, 128, and 256. Due to bandwidth constraints on IoT devices during block propagation, combining short block creation times with large blocks leads to higher stale block rates. To mitigate this, using short blocks with short creation intervals can help reduce stale block rates. Alternatively, longer creation intervals enable the utilization of larger blocks, like those with a 1 MB size, which can also contribute to reducing stale block rates.

Table 4.2. Effect of no. of connections on the throughput and stale block rate in a relay network

No. of Connections	**Block Propagation Delay**						**Stale Block Rate %**	**Bandwidth (kbps)**
	Mean	Median	10%	25%	75%	90%		
5	3.001	2.714	1.275	1.879	3.631	4.852	0.12%	14.603
10	2.912	2.599	1.234	1.799	3.563	4.734	0.32%	14.57
15	2.898	2.572	1.196	1.75	3.559	4.755	0.11%	14.577
20	2.809	2.516	1.156	1.693	3.421	4.586	0.33%	14.38
40	2.794	2.501	1.122	1.687	3.415	4.6	0.50%	14.777
80	2.824	2.52	1.153	1.721	3.44	4.607	0.32%	15.261
120	3.016	2.698	1.23	1.852	3.713	4.954	0.10%	16.505



(a)



b)

Figure. 4.7. Effect of number of connections on: (a) Stale Block Rate (b) Bandwidth (kbps)

To reach the minimum limit for generating less stagnant blocks, longer block generation times can be employed for larger blocks. Moreover, it's evident that block sizes exceeding 1 MB are impractical for IoT due to notable rates of stagnant blocks, even with an extended block generation interval. Achieving a low rate of stagnant blocks has a positive influence on transaction throughput. The impact of the number of miners on both the stagnant block rate and throughput is depicted in Table 4.3 and Figure 4.8.

Table 4.3. Effect of the number of miners on the throughput and stale block rate

Block size	**Block interval**	**No. of miners**									
		16		**32**		**64**		**128**		**256**	
		Stale Block Rate	**Through put**	**Stale Block Rate**	**Through put**	**Stale Block Rate**	**Through put**	**Stale Block Rate**	**Through put**	**Stale Block Rate**	**Through put**
0.25	30s	0.76	33.4	0.75	33.4	0.97	33.4	1.07	33.4	0.94	33.4
0.1	10s	1.76	40	1.86	40	1.74	40	1.9	40	1.9	40
0.25	20s	1.11	50	1.2	50	1.16	50	1.36	50	1.31	50
0.25	15s	1.45	66.7	1.65	66.7	1.62	66.7	1.8	66.7	1.88	66.7
0.5	30s	0.98	66.7	1.11	66.7	1.13	66.7	1.18	66.7	1.16	66.7
1	1mins	0.74	66.7	0.86	66.7	0.88	66.7	0.87	66.7	0.88	66.7

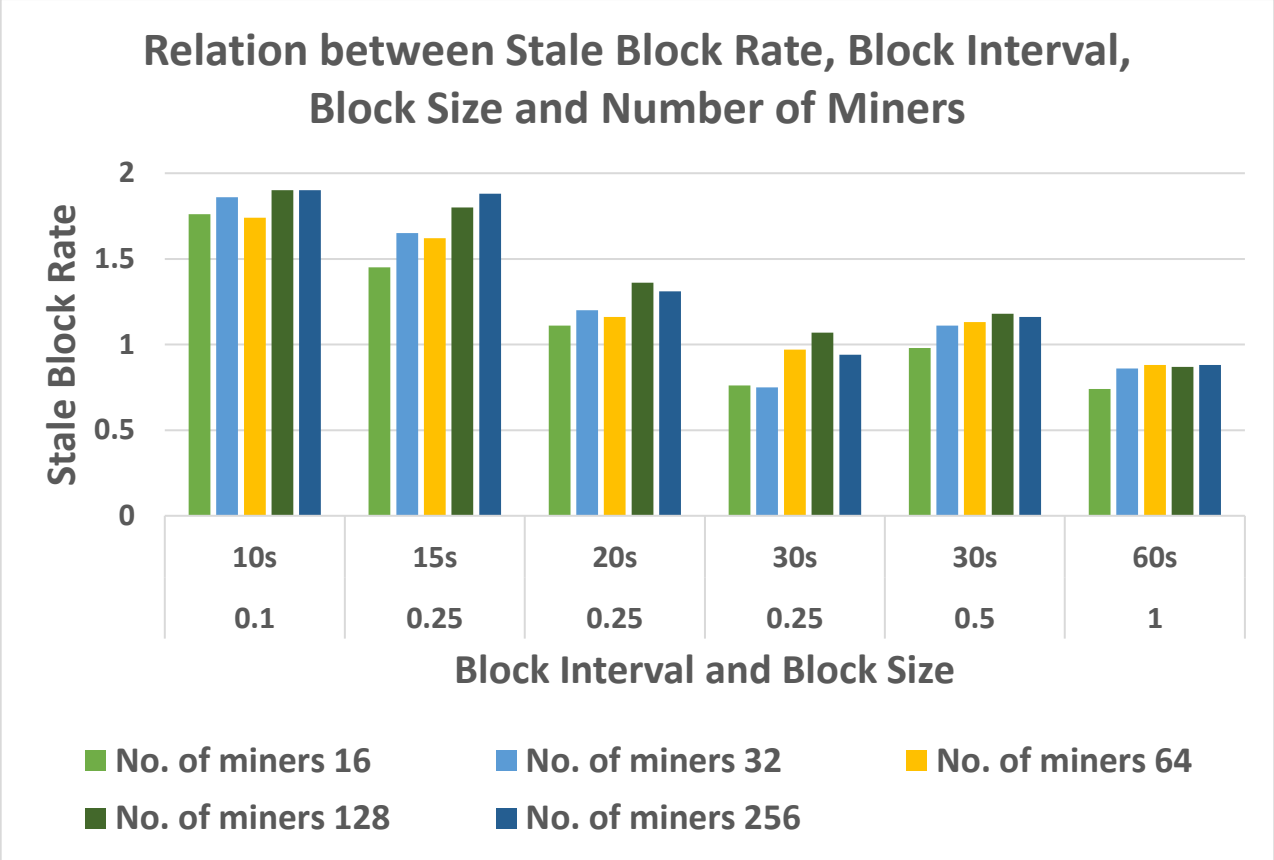


Figure. 4.8. Effect of the number of miners on the stale block rate

It is determined that to maintain low rates of outdated blocks and promote decentralization, careful selection of block sizes and generation intervals is necessary. Block creation intervals should be as fast as feasible, and blocks smaller than 1 MB should be utilized.

4.3 Summary

We've developed a comprehensive framework for the Internet of Things using peer-to-peer networks, leveraging edge computing and blockchain for their substantial storage capabilities and top-notch security features. Our approach integrates smart contracts for tasks like device identification, data management, and scheduling services and resources. This hybrid architecture combines blockchain and edge computing, ensuring security and reliability by incorporating cutting-edge technologies that address issues such as consistency, flexibility, and confidentiality. By segregating the blockchain layer from the application layer, facilitated by the Raiden network and enhancing Ethereum's transaction scalability and efficiency, our layered design enhances scalability. This separation allows devices with limited processing capabilities to retain only the necessary blockchain components, optimizing their functionality.

The conceptual model for a prototype system has primarily been assessed based on the strengths of its individual solutions. Our forthcoming efforts will focus on enhancing various elements, including CPU and memory utilization, as well as energy consumption on the edge server. This will allow us to evaluate system performance and test the feasibility of our proposed decentralized application scheme.

CHAPTER 5

ENHANCING TRUST AND SECURITY IN INDUSTRY 4.0 CYBER-PHYSICAL SYSTEMS THROUGH BLOCKCHAIN INTEGRATION

5.1 Introduction

The integration of physical and virtual technologies in the Industry 4.0 era has brought about a significant transformation in production and industrial operations. Cyber-Physical Systems (CPS) play a vital role in this shift by combining physical devices with computational capabilities to create interconnected and intelligent systems [139]. This integration, along with the seamless incorporation of IoT and big data analytics, has enabled enhanced levels of automation, efficiency, and real-time decision-making. However, this rapid digitalization and connectivity also present new challenges, particularly in terms of trust and security within CPS environments.

As CPS applications become more widespread across various industries, so do the risks associated with cyber threats, data breaches, and system vulnerabilities [140]. The interconnected nature of CPS networks exposes them to potential attacks, manipulation of critical data, and unauthorized access, all of which can have serious consequences on operations, safety, and overall reliability. Traditional centralized security approaches have proven ineffective, as they leave CPS systems vulnerable to single points of failure and lack transparency, making it difficult to identify the sources of security breaches and tampering incidents [141].

In response to the emerging challenges, blockchain technology has gained considerable attention as a potential solution for boosting trust and security in CPS ecosystems. Originally developed to support cryptocurrencies like Bitcoin, blockchain is a decentralized ledger that revolutionizes data management by offering immutability, transparency, and trust among

participants. Its design ensures a secure trail of transactions, making data tampering virtually impossible [142].

Integrating blockchain into CPS environments presents an exciting opportunity to establish a resilient and secure infrastructure. By doing so, we can create a tamper-resistant framework that guarantees data integrity and strengthens trust among interconnected devices, sensors, and systems [143]. The decentralized nature of blockchain adds an extra layer of protection against unauthorized access, data manipulation, and cyber-attacks.

Additionally, the use of smart contracts, which are self-executing programs with predefined rules, enables the automation of trust-based activities, thereby enhancing the reliability and accountability of CPS operations. However, despite the benefits, implementing blockchain in CPS comes with challenges such as scalability issues, resource consumption, limited transaction throughput, privacy concerns, and trust issues [144].

To address these challenges, it's essential to understand various blockchain architectures and select the most suitable one for a specific application. Since CPS have diverse application fields and specific requirements, there's no one-size-fits-all approach to building blockchain-based solutions for CPS [145][146]. Figure 5.1 illustrates some design alternatives for blockchain-based CPS systems.

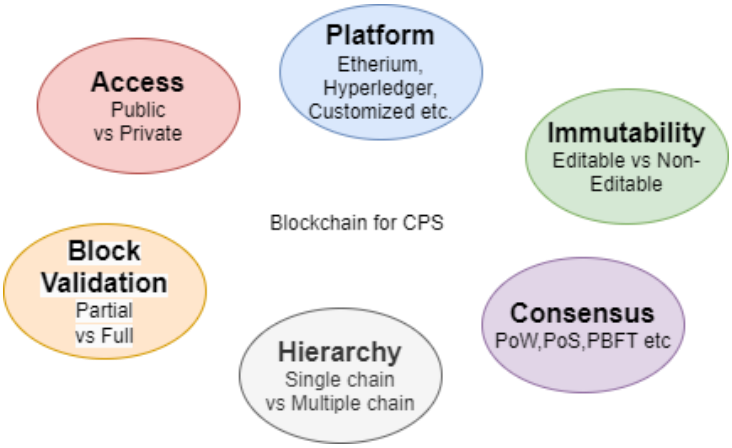


Figure 5.1. Decisions on blockchain design for CPS

The combination of physical and digital technology has completely transformed manufacturing and industrial processes in the age of Industry 4.0. Our goal is to explore the fundamental principles and capabilities of blockchain technology, assess its compatibility with Cyber-Physical Systems (CPS), and analyze its practical implications using real-world examples from various industries [147]. We'll also pinpoint the main challenges and limitations of this

integration and propose potential strategies for optimizing and scaling the use of blockchain in CPS environments.

We anticipate that our research will provide valuable insights for industry players, policymakers, and academics interested in leveraging blockchain technology to enhance trust, security, and resilience in Cyber-Physical Systems [148]. By gaining a thorough understanding of both the benefits and obstacles of this integration, we can pave the way for secure and reliable CPS implementations that support the smooth advancement of Industry 4.0 and beyond [149].

5.2 Designing Blockchain For CPS

Designing a blockchain for Cyber-Physical Systems (CPS) requires careful attention to the specific needs and challenges of this field. CPS combines physical and computational elements, creating a complex and widely distributed environment. Here are some key considerations for designing a blockchain tailored to CPS:

i. **Scalability:** Given the large volume of data generated by sensors and devices in CPS, scalability is crucial. Consider employing scalable blockchain protocols like sharding or those with high throughput capacity. Sharding involves breaking the blockchain into smaller segments to process transactions in parallel [150], significantly enhancing scalability. Off-chain solutions like sidechains or state channels can also alleviate the main blockchain's processing load.

ii. **Low Latency:** Real-time data processing is essential in CPS applications. Opt for fast and efficient consensus mechanisms to achieve low latency. Prioritize time-sensitive transactions and explore lightweight consensus methods like PBFT or DPoS to reduce confirmation times.

iii. **Security:** CPS systems often involve critical infrastructure and sensitive data, demanding robust security measures. Employ strong cryptographic algorithms for data encryption, access controls, and regular security protocol updates to mitigate emerging threats.

iv. **Interoperability:** CPS ecosystems encompass diverse devices and communication standards, necessitating blockchain support for interoperability. Standardized data formats and communication protocols facilitate seamless interaction between CPS components. Middleware or adapters can bridge the gap between the blockchain and existing CPS systems [151].

v. **Consensus Mechanism:** Choose a consensus mechanism suitable for CPS requirements, considering factors like energy consumption and efficiency. Explore alternatives to PoW, such as PoS, DPoS, or PBFT, and investigate hybrid consensus methods for a balance between security and efficiency.

vi. **Privacy:** Protect sensitive CPS data with privacy features like confidential transactions or zero-knowledge proofs. Utilize permissioned blockchains or hybrid models to control data access based on defined roles and permissions.

vii. **Data Validation:** Ensure data integrity in CPS by implementing validation techniques like cryptographic hashing and digital signatures. Reputation systems or oracle mechanisms can validate data from external sources or IoT devices.

viii. **Smart Contracts:** Design smart contracts to automate CPS processes and interactions, considering specific logic requirements. Write smart contracts securely to avoid vulnerabilities and bugs [152].

ix. **Energy Efficiency:** Optimize blockchain energy consumption to minimize impact on resource-constrained CPS devices. Energy-efficient consensus mechanisms and lightweight data structures can reduce computational burden on CPS nodes.

x. **Governance:** Establish a governance model aligned with CPS ecosystem requirements and goals. Define transparent rules for protocol upgrades, consensus changes, and dispute resolution.

xi. **Fault Tolerance:** Ensure CPS blockchain resilience to failures and attacks by employing fault-tolerant consensus mechanisms capable of handling Byzantine faults.

xii. **Regulatory Compliance:** Address legal and regulatory considerations relevant to CPS blockchain applications. Implement auditing and traceability mechanisms to demonstrate compliance and accountability [153].

xiii. **Testbed and Simulation:** Before deployment, conduct thorough testing using testbeds and simulations to assess performance, security, and scalability under various conditions. Identify and address potential bottlenecks and vulnerabilities [154].

5.3 Blockchain Enabled CPS (BCPS) Structure

Blockchain-Enabled Cyber-Physical Systems (BCPS) represent a novel approach that merges blockchain technology with Cyber-Physical Systems (CPS), offering decentralization, transparency, and security to CPS environments and opening up new possibilities across industries. BCPS architecture consists of several key components:

i. **Blockchain Layer:** This core component includes the blockchain network, with options for either public or private blockchain, and encompasses elements like consensus mechanisms, smart contracts, data storage, and peer nodes.
ii. **CPS Layer:** Comprising physical and computational components of CPS, this layer consists of sensors, actuators, and embedded systems that interact with the blockchain layer to exchange data and trigger actions.
iii. **Data Collection and Oracles:** Responsible for gathering data from CPS devices, while oracles facilitate the transfer of real-world data to the blockchain network.
iv. **Smart Contracts:** These automate processes and execute actions based on predefined conditions, facilitating transactions and interactions within BCPS.
v. **Consensus Mechanism:** Ensures agreement among network nodes on transaction validity and ordering, employing methods like Proof-of-Work or Proof-of-Stake.
vi. **Identity and Access Management:** Governs access rights to the blockchain network using cryptographic methods for secure authentication.
vii. **Privacy and Encryption:** Utilizes encryption and zero-knowledge proofs to protect sensitive data privacy.
viii. **Interoperability and Middleware:** Enables seamless integration between blockchain and existing CPS systems through middleware that translates data formats and protocols.
ix. **Monitoring and Analytics:** Provides insights into network performance and behavior, aiding in anomaly detection and process optimization.
x. **Governance and Upgrades:** Defines decision-making processes for BCPS, ensuring adaptability and participation in protocol upgrades and dispute resolution.

BCPS aims to address challenges in real-world deployment by focusing on four key areas: Interchangeability, Data integrity, Safety and confidentiality, and Resilience. Figure 5.2 provides an overview of the detailed BCPS architecture, while Table 5.1 outlines the primary requirements for each layer of BCPS.

5.3.1 Connection Layer

The Connection Layer focuses on advanced connectivity, data management, authenticity, and privacy. It emphasizes interoperability as a crucial element for global connectivity and integration. Achieving technical interoperability involves addressing issues related to open standards, open-source software, multilingualism, subsidiarity, security, privacy, and accessibility. Blockchain technology plays a significant role in enhancing security and privacy

through cutting-edge cryptographic algorithms and a universal consensus mechanism, thanks to its decentralized structure. This structure also reinforces subsidiarity.

In this layer, larger nodes, known as Master Nodes, can serve as local servers for nodes with fewer resources. This arrangement allows the resource-constrained nodes to store data, perform computations, and communicate with other nodes. To facilitate communication, resource-restricted nodes obtain private IP addresses through their respective Master Nodes, while each Master Node may have a public IP address for direct connections with other nodes. Consequently, all nodes can interact, exchange data, and share computing and networking resources. Shared storage and networking sharing enhance system redundancy, leading to greater network resilience.

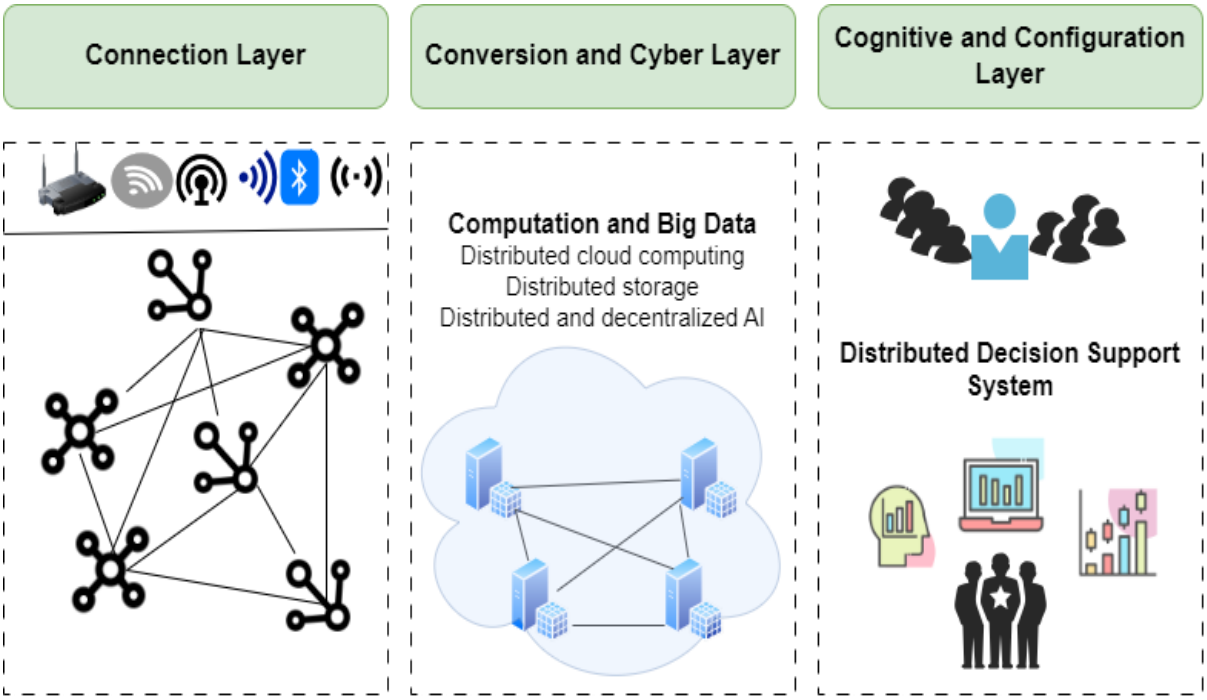


Figure.5.2 The proposed three-tiered BCPS design

Table 5.1 The BCPS structure's key characteristics and needs

BCPS Architecture	Features	Requisites
Configuration	• Supervisory Control (ERP, MES, SCM, CMM, and PLM) • Autonomous Decision Making • Smart Business Organisation	• Self-configuration • Self-adjustment • Self-optimization • Sustainable Organization Strategies
Cognition	• Decision-Making Aids • Fabrication and simulation merged	• Access to data in real time • Dependable source of information • Access to structured information
Cyber	• Digital Twins • Big Data • Cloud Computing	• Storage, bandwidth, and computing redundancy

	• Simplicity Modelling • Data Warehousing (DW) • Cyber-Cyber Interactions	• Connectivity that is efficient in terms of bandwidth, latency, accessibility, and reliability • Integrating and connectivity across domains • Managing Design Complicatedness • Safety and confidentiality
Conversion	• AI Analysis Software • Models of AI/Machine Learning / PHM Tools • Intelligence that is distributed and decentralised • Fog / Edge Computing • Deep Learning	• Resilience • Rapid Computing • Adaptive, Trustworthy, and Reliable
Connection	• Physical-Physical Interactions and Physical-Human Interactions • Sensors, Actuators, Processes, Machines, and other Smart Nodes	• Connectivity that is efficient in terms of bandwidth, latency, accessibility, and reliability • Safety and confidentiality • Interchangeability

5.3.2 Conversion and Cyber Layer

The Conversion and Cyber Layer manages the transformation of data into usable information and facilitates interactions between cyber-physical and cyber-cyber systems to ensure integrity, fault tolerance, and resilience. Key concerns at this level include cybersecurity, big data management (Volume, Variety, and Velocity), cloud computing, network connectivity, privacy, and transparency. Grid and cloud computing technologies are commonly used to enhance system resilience, expand networks, and efficiently utilize available resources by distributing computation and storage tasks across networked computers. The evolution of distributed computing requires the adoption of a blockchain architecture, which offers advantages such as data security, shared information storage, and enhanced data access through a peer-to-peer (P2P) network.

Incorporating AI methods into this layer is essential for converting unstructured data into actionable insights and providing individual Nodes with access to valuable information. Modern manufacturing processes heavily rely on network systems with AI capabilities. Moreover, distributed and decentralized AI (DDAI) systems outperform centralized cloud computing systems. Blockchain facilitates distributed operations, knowledge sharing, and coordination for AI technologies. Training DDAI modules with diverse and reliable global data improves their robustness and dependability. Direct input from operations enhances DDAI reliability, while peer-to-peer resource sharing and automatic machine learning (AutoML) significantly reduce deployment costs.

5.3.3 Cognitive and Configuration Layer

The Cognitive and Configuration Layer involves leveraging extensive data from the cyber level to support decision-making in a data-driven decision support system (DSS). The goal is to enable quick and informed decisions, enhance productivity and resilience, and ultimately promote sustainable production. In traditional industrial systems with dispersed components and users, a robust and distributed platform is essential to ensure the integrity of company information and improve competency, efficiency, and competitiveness. Using blockchain as the foundation for such a DSS creates a decentralized and distributed system, where decisions are made based on global consensus and considering all limitations within the network. This allows any node to actively participate in decision-making. Leveraging blockchain technology offers several advantages, including location independence, fault tolerance, security, autonomy, and scalability. Stakeholders' needs and demands, as well as how the suggested blockchain-based decision support system architecture can meet them, are outlined in Table 5.2.

Table 5.2. The influence of blockchain on the demands and expectations of stakeholders

BCPS Layers	Stakeholders' Wants and Demands	Blockchain Contribution
Management Net	Decision-assisting systems' dependability, adaptability, safety, and effectiveness	Distributed and decentralised cryptography
	Lowering overhead costs	Peer to peer interactions, smart contracts
	Decreased bureaucracy	Peer to peer interactions, smart contracts
	Confidentiality and safety of data	High-tech cryptography
	Supervision and management of resources	Transparency in peer-to-peer interactions
	Ownership as a Service (OaaS)	Tokenization of assets, smart contracts
Cyber Net	The translation of data into information that can be utilised	AI model training using additional data from open datasets, distributed and decentralised AI.
	Single point of breakdown eradication	Work and share of resources (computation, storage, and communication) between nodes
	Confidentiality and safety of data	High-tech cryptography
	Data storage that is efficient	Micro clouds, storage of information in each Node
	Data as a Service (DaaS)	Peer to peer interactions, smart contracts
Connection Net	Supply chain transparency	Component tracking from beginning to end - Transparency
	Device interconnectivity	Master Nodes, peer-to-peer interactions
	Automation	Peer to peer interactions, smart contracts
	Connectivity that is efficient (in terms of bandwidth, latency, and resilience, for example)	Common resources, Master Nodes, and peer-to-peer interactions
	Confidentiality and safety of data	High-tech cryptography

In the realm of blockchains, there's no single central node tasked with validating ledgers across various nodes. In simpler terms, consensus refers to the dynamic process of reaching agreement

within a network. Unlike voting, which often favors the majority and disregards minority interests, consensus aims to find solutions that benefit the entire community. Consequently, consensus is seen as a resilient method for establishing irreversible agreements among multiple nodes or devices in a peer-to-peer network, thus thwarting potential network exploitation. Table 5.3 presents well-known blockchain consensus techniques along with their advantages.

Table 5.3. Blockchain networks' well-known consensus processes

Name	Description	Notion
Proof of Work (PoW)	Proof of work refers to a method that necessitates a considerable but manageable amount of effort in order to prohibit frivolous or malicious usage of computer resources.	Hal Finney used the notion for money in 2004 with the concept of "reusable proof of work."
Proof of Stake	PoS was created as a replacement for PoW in order to remedy the latter's basic shortcomings. The PoS system compels miners to approve transaction blocks depending on the number of coins they own, or their stake.	PoS was discussed in Bitcoin circles as early as 2011. Proof of stake is simply a type of proof of money ownership.
Delegated Proof of Stake (DPoS)	DPoS uses the influence of stakeholder approval voting to settle consensus issues in a fair and democratic manner. Delegated network characteristics include charge schedules, block intervals, and transaction sizes.	Eric Wustrow and Benjamin Vander Sloot of the University of Michigan introduced DPoS.
Proof of Authority (PoA)	PoA is assumed to be similar to PoS and DPoS in that only a small number of pre-selected authority (known as validators) safeguard the distributed ledger and may create fresh blocks. Only when the validators achieve a supermajority are new blocks added to the network.	Gavin Wood, co-founder of Ethereum and Parity Technologies, created the phrase.

Historically, existing consensus algorithms in large-scale blockchain networks have struggled with inconsistency issues, many of which were initially devised for the bitcoin industry. To address these challenges, Abraham and colleagues proposed a unique consensus mechanism that leverages practical Byzantine fault tolerance (pBFT). In this pBFT-based approach, each cycle determines a new block, with a primary node selected based on specific criteria to organize transactions. The process involves three stages: pre-preparation, preparation, and commitment.

pBFT algorithms surpass proof-of-work (PoW) and proof-of-stake (PoS) algorithms in terms of resource efficiency and security. Consequently, pBFT was chosen to enhance blockchain

networks for small and medium-sized enterprises (SMEs) based on previous research findings. The pBFT implementation employed for this purpose was built upon the work of Mao et al. for the BCPS system, with the suggested algorithm outlined in algorithm 5.1.

Algorithm 5.1. Proposed algorithm for the BCPS platform

```
1   Initialization
2   set K_eu and K_sp.// K_eu as a end user key. K_sp as a service provider key.
3   Input n                    // Number of transactions
5   if (K_eu = K_eu &K_sp)
        then      // The miner node signs and timestamps the transaction information.
        n=n+1
    else
        Because the request information was not authorised, transaction information
    was sent to the next miner node.
    if (K_eu ≠ K_sp)
        The request information is also not authorised, and the transaction information
    and n are sent to the next miner node.
        then
        n≥51%   // more than the number of scheduled nodes
        The block stores transaction data.
    else
    Transaction failed
5   end
```

In the initial step of the recommended approach, both the end user and service provider choose specific keys. If the provided key aligns with the required information, the transaction data gets signed, and a new block containing the transaction details is generated by the mining node. If the requested information isn't authorized, it's forwarded to additional mining nodes until at least 51% of them validate the transaction. If the acceptance threshold isn't met, the transaction fails, and all pertinent data remains in the block.

The consensus process is managed by an approved edge node (service provider) and mining nodes, as shown in Figure 5.3. In the BCPS system, the pBFT consensus method involves five main phases. Initially, the end user sends the transaction to all nodes. Once the leader node receives it, it forwards it to relevant consensus nodes. From there, transactions are distributed to all subsequent consensus nodes, ensuring that all nodes' transaction pools remain synchronized.

Following that, the preliminary preparation phase involves organizing transactions according to predetermined criteria, such as batch size. When consensus nodes are linked, they receive a pre-prepared message from a specific node and use current view and block number data to verify its authenticity. If the check confirms the message's validity, it is broadcasted to all consensus nodes. These nodes then cross-validate the batch by comparing their results with the primary validation outcome provided in the pre-preparation message. Upon successful

verification, the nodes issue a commit message, indicating their agreement with the primary validation outcome. Failure to validate suggests an abnormality in the primary process. Once all consensus nodes reach agreement on validation, the execution outcome is recorded in their local ledger.

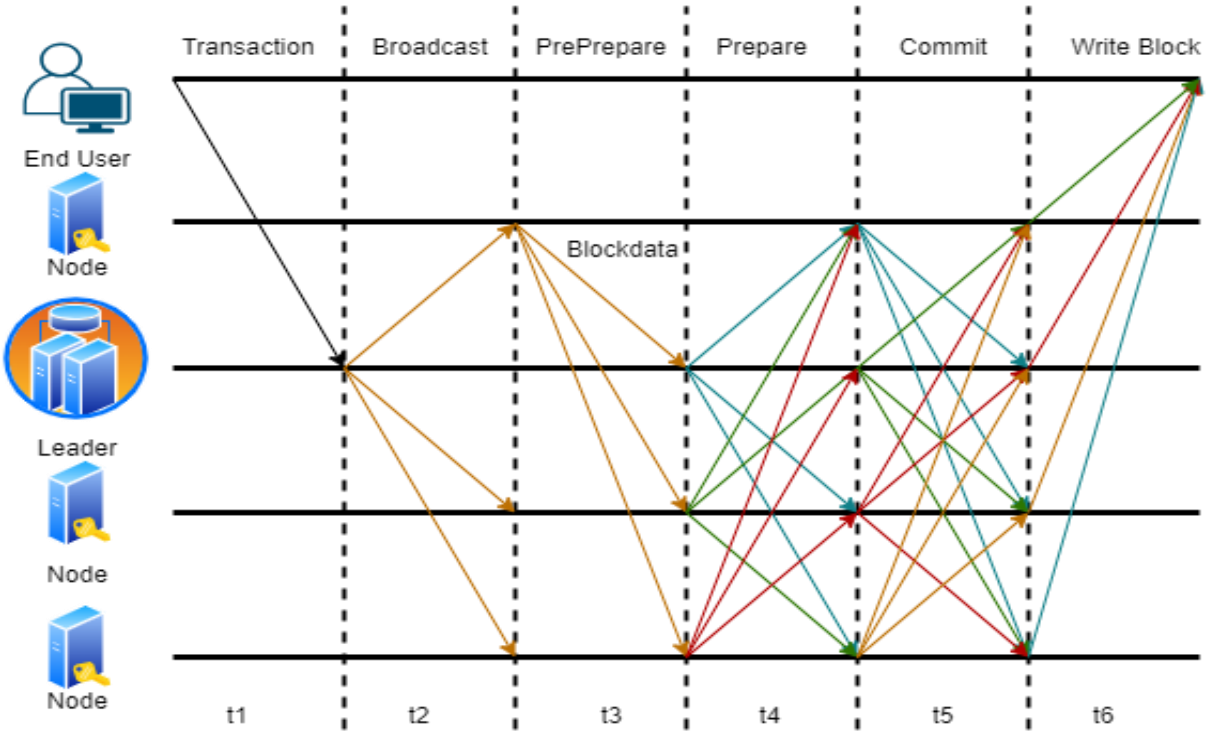


Figure 5.3. The BCPS consensus procedure.

5.4 Blockchain-Enabled Cyber-Physical Systems (BCPS) for Prognostics and Health Management (PHM) Structure

Figure 5.4 illustrates a case study in the Prognostics and Health Management (PHM) field, showcasing the practical application of various Blockchain in Cyber-Physical Systems (BCPS) functionalities for monitoring the health of manufacturing machines. The research involves deploying four distinct devices at two different locations referred to as 'Location A' and 'Location B'. These devices collect data, which is then transmitted to fog computing devices. Subsequently, relevant and actionable data at the fog layer is forwarded to the cloud for further advanced PHM analysis.

The adoption of blockchain technology offers potential solutions to current challenges in the BCCPS framework. It specifically tackles three key issues: 1) Ensuring data availability, 2) Implementing Smart PHM, and 3) Enhancing the Predictive Maintenance Support System (PMSS), which will be discussed in the upcoming sections.

5.4.1 Data Availability

Within the BCPS framework, the movement of data from one level to another poses significant concerns regarding security, privacy, and capacity. To tackle this challenge, a solution has been proposed at the initial layer of BCPS, involving the use of 'Master Nodes' as intermediaries. These Master Nodes possess the capability to share resources with other Nodes within their local network. By implementing this method, potential cyber-physical threats targeting actuators, sensors, communication networks, and physical interfaces—each critical in cyber-physical interactions—can potentially be mitigated effectively within the proposed BCPS architecture.

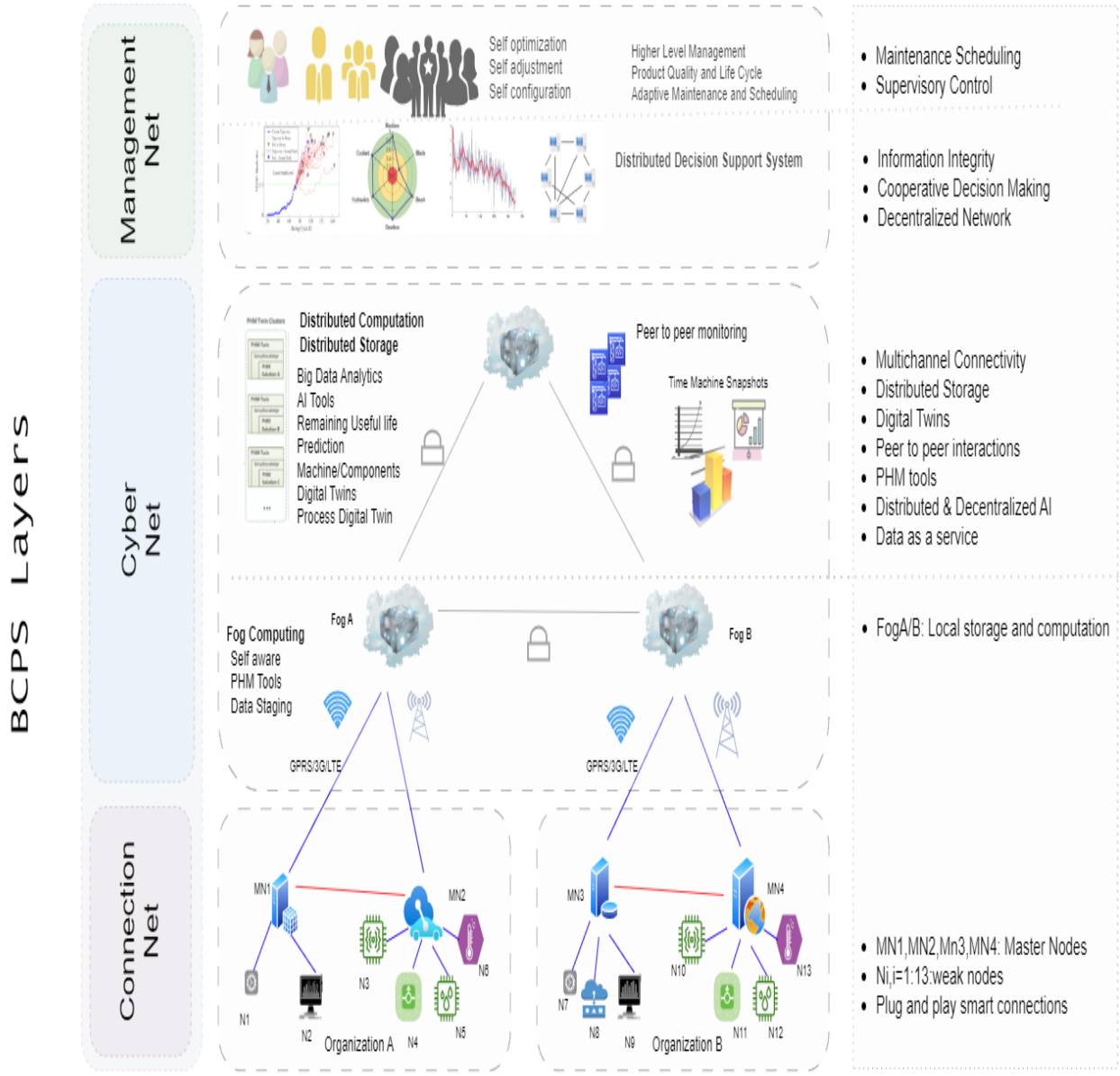


Figure 5.4 An analysis of the BCPS Structure based on PHM

5.4.2 Intelligent PHM

AI technologies relying on PHM face challenges in adapting to the dynamic industrial landscape. Privacy and security concerns often restrict access to critical data necessary for their effectiveness. One potential solution is the development of a blockchain-enabled Distributed Data AI (DDAI) platform. This platform would enable AI learning agents to access additional training data securely, enhancing system reliability and performance. For instance, in PHM applications, CNC machines in different factories could gather data snapshots, which local AI agents within the machines could analyze. The encrypted results could then be shared with relevant parties, such as maintenance workers and CNC manufacturers, leveraging the high degree of connectivity provided by the "Cyber Net."

5.4.3 Predictive Maintenance Support System (PMSS)

By gathering additional data from various sources, such as the cost of production equipment, its lifespan, order delivery times, downtime for substitutions, and the distribution of workloads from different network levels like 'Connection Net' and 'Cyber Net', we can create a unified support system for intelligent predictive maintenance. Integrating this information into a Decision Support System (DSS) at the 'Management Net' level enables the development of a comprehensive decision-making system for Prognostics and Health Management (PHM) applications.

5.5 Results and Discussion

To assess and validate our proposed platform, our initial focus was on evaluating the performance of the underlying network topology. Following this, a security audit survey was conducted, demonstrating how our suggested architecture enables reliable service transfer without involving a third party. Initially, we examined the practical Byzantine Fault Tolerance (pBFT) in our core network architecture study to assess the proposed consensus method using real machine data. An autonomous agent connects with physical equipment whenever a smart contract between the end user and the service provider is active. To streamline consensus procedures and reduce complexity, we include cost, size, time limits, and quality levels as smart contract components due to computational constraints. Consequently, the algorithm's difficulty level was adjusted to ensure timely completion of the mining process in the network. The simulation results align with the Proof of Work (PoW) consensus, which is better suited for a permissioned chain where participants are already trusted and identified. When comparing the two consensus algorithms using existing machine data, we considered the time for mining

transactions and the time to complete 255 validated requests. In our scenario, we analyzed 1000 platform transactions. Figure 5.5 illustrates the throughput performance of pBFT compared to PoW, while Table 5.4 presents comprehensive findings, including mean, standard deviation, standard error, and more.

Thorough analysis reveals that the proposed consensus mechanism outperforms Proof of Work (PoW) when handling 255 requests out of 1000 transactions. The practical Byzantine Fault Tolerance (pBFT) method recommended here completed the task in 3812 seconds, whereas PoW took 5448 seconds. Additionally, the pBFT's confidence interval is nearly half the size of PoW's, indicating lower network latency in the recommended platform. Consequently, it's clear that the suggested platform surpasses the competition in terms of performance.

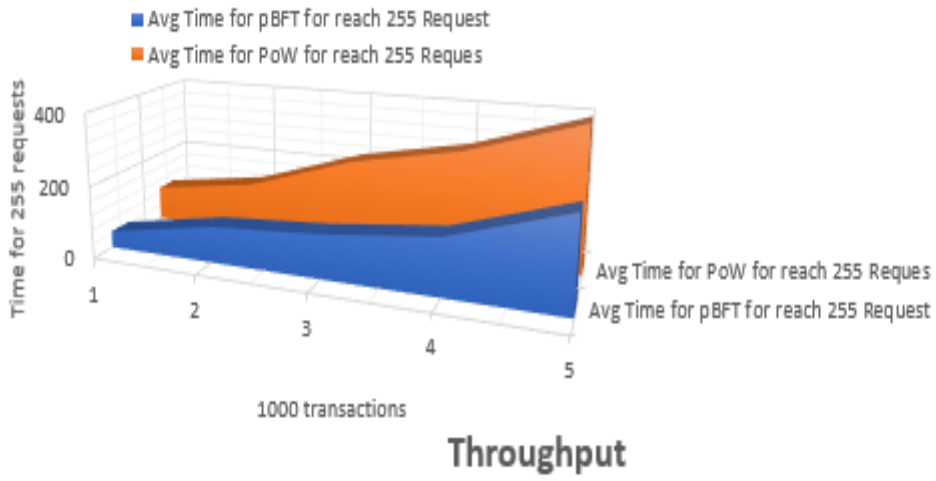


Figure 5.5. pBFT throughput performance against PoW.

Table 5.4. The outcomes of network design

Variable	pBFT in recommended platform	PoW in recommended platform
Sum (Second)	3812	5448
Minimum	38	62
Maximum	214	400
Range	181	339
Mean	131.54	187.45
Standard Error	12.65	20.72
95% confidence interval	22.99	42.01
Standard Deviation	63.13	111.54

Figure 5.6 illustrates the monitoring data for the cloud environment. The graph presents the results of six distinct metrics linked to the cloud environment: CPU usage, incoming and outgoing network traffic and packets, as well as instances of status check failures.

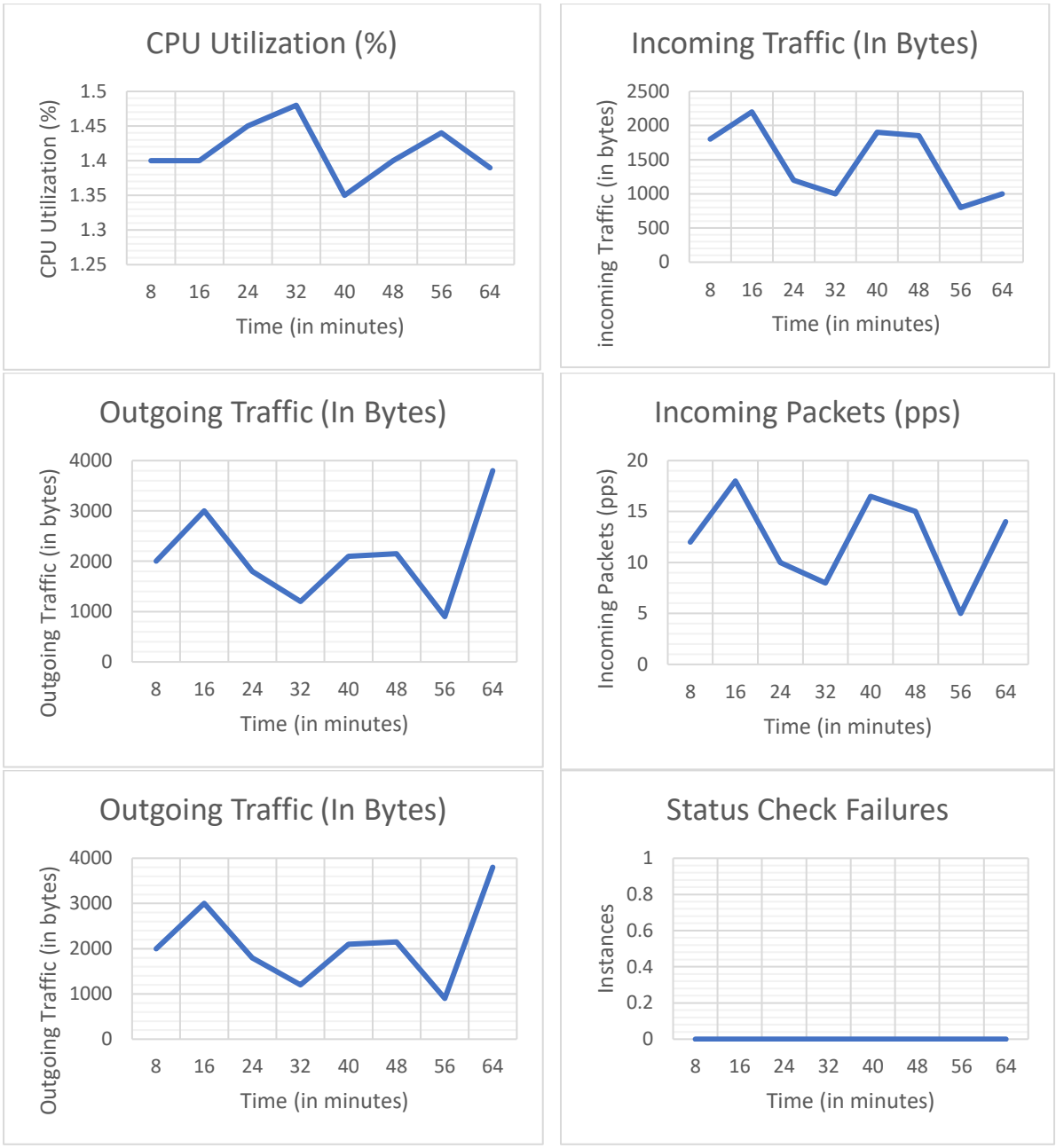


Figure 5.6. Data from network monitoring collected in a built cloud environment

These results suggest that the proposed platform can sustain industrial applications without requiring excessive CPU utilization. Consequently, the system developed demonstrates ample scalability to manage significant volumes of data.

5.5.1 Challenges in Implementing BCPS in Industrial Systems

The advancement of blockchain technology is still in its early stages, and there may be particular hurdles in adapting it to industrial processes that will need additional exploration and improvement. Figure 5.7 outlines some of the existing concerns.

5.6 Summary

The research suggests a framework utilizing blockchain technology to address the limitations of real-time execution in cyber-physical systems within industrial settings. The proposed integration aims to improve communication and data flow within the current Cyber-Physical Production Systems (CPPS) framework, ensuring the secure and dependable operation of industrial systems.

Figure 5.7. Blockchain implementation challenges in industrial systems

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

To summarize, for real-time mission critical applications, now Cyber-Physical Systems (CPS), Edge Computing, Block chain & Internet of Things combined offers a solution to address the challenges. The actuators require a rapid message transfer time with absolute reliability, which is especially critical in CPS. This is crucial when it comes to immediate-need sectors such as healthcare, where urgent care counts.

This thesis investigates key aspects in the design of smart CPSs: (i) accounting for sensor/actuator delays; and ensuring energy efficiency via DVFS control; (ii) disturbance estimation, compensator design , and allocation of the state-space to the VFIs . The importance of these elements cannot be stressed enough to maintain overall CPS resilience and performance and, in some cases, the deliverance to compliances like in healthcare.

The thesis also provided new idea of combining blockchain with edge computing to enhance the security and performance of CPS. We elaborate the potential advantages of this integration flexibly, integrating with trust and hiding, backed by both a solid theoretical support and architectural design.

Our ultimate aim was to develop a more secure and efficient solution for the Internet of Things, powered by both edge computing and blockchain. By further show this combination enables secure data archiving and network infrastructure protection across IoT devices, edge nodes and cloud servers. This in turn allows their integration into peer-to-peer networks by means of smart contracts, that delivers a platform that scales for millions of connected, autonomy, and CPS applications.

Some advanced technologies, like ethereum's layered solution and raiden network, already incorporated these solutions to address the issues on availability, portability, and privacy. This piece of the blockchain is then differences based compared in with another record with regard to a compressible bucket, using a method that makes the blockchain more scalable yet still ensure those devices with little processing power store only the parts they need.

6.2 Future Scope

The possibility of refining DCS (Distributed Control System) and SCADA (Supervisory Control and Data Acquisition) also is achieved by the proposed paradigm. Such a model may be further extended by integration of self-aware actuation and computing in SCPS (Self-aware Cyber-Physical Systems), for both dynamic and static operations, in future research works. In addition, expansion of CPS can strengthen its deliverable in more application areas like defence, oil and gas exploration, robotics, space exploration which leads to the advancement of technology limits which in turn help the welfare of society. We may discover fresh opportunities and exceed limits to what can be achieved in Cyber-Physical Systems by iteratively evolving these ideas.

In the near future, we will optimize memory usage, CPU usage, and energy consumption of the advice running on edge servers in the upcoming future. We shall get through dev-side these creations to assess and check how resilient and how right this strategy can survive through an unbias test)), by creating first a prototype system and a decentralized application site. By laying this foundation for further attempts in the future, we aim to stimulate more research and innovation around the convergence of edge computing and blockchain to CPS applications.

References

1. Marković, D., Mizrahi, A., Querlioz, D., & Grollier, J. (2020). Physics for neuromorphic computing. *Nature Reviews Physics, 2*(9), 499-510.
2. Furber, S. (2016). Large-scale neuromorphic computing systems. *Journal of Neural Engineering, 13*(5), 051001.
3. Davies, M., Wild, A., Orchard, G., Sandamirskaya, Y., Fonseca Guerra, G. A., Joshi, P., Plank, P., & Risbud, S. R. (2021). Advancing neuromorphic computing with Loihi: A survey of results and outlook. *Proceedings of the IEEE, 109*(5), 911-934.
4. van de Burgt, Y., Melianas, A., Keene, S. T., Malliaras, G., & Salleo, A. (2018). Organic electronics for neuromorphic computing. *Nature Electronics, 1*(7), 386-397.
5. Roy, K., Jaiswal, A., & Panda, P. (2019). Towards spike-based machine intelligence with neuromorphic computing. *Nature, 575*(7784), 607-617.
6. Burr, G. W., Shelby, R. M., Sebastian, A., Kim, S., Kim, S., Sidler, S., Virwani, K., et al. (2017). Neuromorphic computing using non-volatile memory. *Advances in Physics: X, 2*(1), 89-124.
7. Shastri, B. J., Tait, A. N., de Lima, T. F., Pernice, W. H. P., Bhaskaran, H., Wright, C. D., & Prucnal, P. R. (2021). Photonics for artificial intelligence and neuromorphic computing. *Nature Photonics, 15*(2), 102-114.
8. Esser, S. K., Appuswamy, R., Merolla, P., Arthur, J. V., & Modha, D. S. (2015). Backpropagation for energy-efficient neuromorphic computing. *Advances in Neural Information Processing Systems, 28*.
9. Shi, L., Pei, J., Deng, N., Wang, D., Deng, L., Wang, Y., Zhang, Y., et al. (2015). Development of a neuromorphic computing system. In *2015 IEEE International Electron Devices Meeting (IEDM)*, pp. 4-3. IEEE.
10. Marković, D., & Grollier, J. (2020). Quantum neuromorphic computing. *Applied Physics Letters, 117*(15).
11. Thiem, C., Wysocki, B., Bishop, M., McDonald, N., Bohl, J., & Air Force Research Lab Rome NY Information Directorate. (2013). *Foundations of neuromorphic computing* (Tech. Rep. AFRL-RI-RS-TR-2013-125). Air Force Research Laboratory, Rome, NY.
12. Zenke, F., & Neftci, E. O. (2021). Brain-inspired learning on neuromorphic substrates. *Proceedings of the IEEE, 109*(5), 935-950.

13. Li, J., Shen, Z., Cao, Y., Tu, X., Zhao, C., Liu, Y., & Wen, Z. (2022). Artificial synapses enabled neuromorphic computing: From blueprints to reality. *Nano Energy*, 107744.
14. Neftci, E. O. (2018). Data and power efficient intelligence with neuromorphic learning machines. *iScience, 5*, 52-68.
15. Indiveri, G., Linares-Barranco, B., Hamilton, T. J., van Schaik, A., Etienne-Cummings, R., Delbruck, T., Liu, S.-C., et al. (2011). Neuromorphic silicon neuron circuits. *Frontiers in Neuroscience, 5*, 73.
16. Li, J., Liu, L., Zhao, C., Hamedani, K., Atat, R., & Yi, Y. (2017). Enabling sustainable cyber physical security systems through neuromorphic computing. *IEEE Transactions on Sustainable Computing, 3*(2), 112-125.
17. Fang, H., Shrestha, A., Zhao, Z., Li, Y., & Qiu, Q. (2019). An event-driven neuromorphic system with biologically plausible temporal dynamics. In *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 1-8. IEEE.
18. Zenke, F., & Neftci, E. O. (2020). Brain-inspired learning on neuromorphic substrates. *arXiv preprint arXiv:2010.11931*.
19. Brown, K. A., Brittman, S., Maccaferri, N., Jariwala, D., & Celano, U. (2019). Machine learning in nanoscience: big data at small scales. *Nano Letters, 20*(1), 2-10.
20. Yang, J.-Q., Wang, R., Ren, Y., Mao, J.-Y., Wang, Z.-P., Zhou, Y., & Han, S.-T. (2020). Neuromorphic engineering: from biological to spike-based hardware nervous systems. *Advanced Materials, 32*(52), 2003610.
21. Sztipanovits, J., Koutsoukos, X., Karsai, G., Kottenstette, N., Antsaklis, P., Gupta, V., Goodwine, B., Baras, J., & Wang, S. (2011). Toward a science of cyber-physical system integration. *Proceedings of the IEEE, 100*(1), 29-44.
22. Jirkovský, V., Obitko, M., & Mařík, V. (2016). Understanding data heterogeneity in the context of cyber-physical systems integration. *IEEE Transactions on Industrial Informatics, 13*(2), 660-667.
23. Khujamatov, H., Reypnazarov, E., Khasanov, D., & Akhmedov, N. (2021). IoT, IIoT, and cyber-physical systems integration. In *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation* (pp. 31-50). Cham: Springer International Publishing.
24. Hehenberger, P., Vogel-Heuser, B., Bradley, D., Eynard, B., Tomiyama, T., & Achiche, S. (2016). Design, modelling, simulation and integration of cyber physical systems: Methods and applications. *Computers in Industry, 82*, 273-289.

25. Singh, H. (2021). Big data, industry 4.0 and cyber-physical systems integration: A smart industry context. *Materials Today: Proceedings, 46*, 157-162.
26. Leitao, P., Karnouskos, S., Ribeiro, L., Lee, J., Strasser, T., & Colombo, A. W. (2016). Smart agents in industrial cyber–physical systems. *Proceedings of the IEEE, 104*(5), 1086-1101.
27. Liu, Y., Peng, Y., Wang, B., Yao, S., & Liu, Z. (2017). Review on cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica, 4*(1), 27-40.
28. Sha, L., Gopalakrishnan, S., Liu, X., & Wang, Q. (2008). Cyber-physical systems: A new frontier. In *2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008)*, pp. 1-9. IEEE.
29. Mosterman, P. J., & Zander, J. (2016). Cyber-physical systems challenges: a needs analysis for collaborating embedded software systems. *Proceedings of the IEEE, 104*(5), 5-16.
30. Colombo, A. W., Karnouskos, S., & Bangemann, T. (2014). Towards the next generation of industrial cyber-physical systems. In *Industrial Cloud-Based Cyber-Physical Systems: The IMC-AESOP Approach*, pp. 1-22. Cham: Springer International Publishing.
31. Sanislav, T., & Miclea, L. (2012). Cyber-physical systems-concept, challenges and research areas. *Journal of Control Engineering and Applied Informatics, 14*(2), 28-33.
32. Konstantinou, C., Maniatakos, M., Saqib, F., Hu, S., Plusquellic, J., & Jin, Y. (2015). Cyber-physical systems: A security perspective. In *2015 20th IEEE European Test Symposium (ETS)*, pp. 1-8. IEEE.
33. Derler, P., Lee, E. A., & Sangiovanni Vincentelli, A. (2011). Modeling cyber–physical systems. *Proceedings of the IEEE, 100*(1), 13-28.
34. Shi, J., Wan, J., Yan, H., & Suo, H. (2011). A survey of cyber-physical systems. In *2011 International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1-6. IEEE.
35. Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W., & Ueda, K. (2016). Cyber-physical systems in manufacturing. *CIRP Annals, 65*(2), 621-641.
36. Törngren, M., & Grogan, P. T. (2018). How to deal with the complexity of future cyber-physical systems? *Designs, 2*(4), 40.
37. Serpanos, D. (2018). The cyber-physical systems revolution. *Computer, 51*(3), 70-73.
38. Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences, 8*(6), 898.

39. Anumba, C. J., Akanmu, A., & Messner, J. (2010). Towards a cyber-physical systems approach to construction. In *Construction Research Congress 2010: Innovation for Reshaping Construction Practice*, pp. 528-537.
40. Karnouskos, S. (2011). Cyber-physical systems in the smartgrid. In *2011 9th IEEE International Conference on Industrial Informatics*, pp. 20-23. IEEE.
41. Lee, E. A. (2008). Cyber physical systems: Design challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pp. 363-369. IEEE.
42. Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry, 100*, 212-223.
43. Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). Cyber-physical systems: The next computing revolution. In *Proceedings of the 47th Design Automation Conference*, pp. 731-736.
44. Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). Challenges for securing cyber physical systems. In *Workshop on Future Directions in Cyber-Physical Systems Security*, vol. 5, no. 1.
45. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal, 4*(6), 1802-1831.
46. Kim, K.-D., & Kumar, P. R. (2012). Cyber–physical systems: A perspective at the centennial. *Proceedings of the IEEE, 100*(Special Centennial Issue), 1287-1308.
47. Wan, J., Yan, H., Suo, H., & Li, F. (2011). Advances in cyber-physical systems research. *KSII Transactions on Internet & Information Systems, 5*(11), 1891-1908.
48. Neuman, C. (2009). Challenges in security for cyber-physical systems. In *DHS Workshop on Future Directions in Cyber-Physical Systems Security* (pp. 22-24). Edited by Nabil Adam: US Department of Homeland Security.
49. Gunes, V., Peter, S., Givargis, T., & Vahid, F. (2014). A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Transactions on Internet and Information Systems, 8*(12), 4242-4268.
50. Chen, H. (2017). Applications of cyber-physical system: A literature review. *Journal of Industrial Integration and Management, 2*(03), 1750012.
51. Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems, 77*, 103201.

52. Jazdi, N. (2014). Cyber physical systems in the context of Industry 4.0. In *2014 IEEE International Conference on Automation, Quality and Testing, Robotics* (pp. 1-4). IEEE.
53. Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters, 3*, 18-23.
54. Lu, Y. (2017). Cyber physical system (CPS)-based industry 4.0: A survey. *Journal of Industrial Integration and Management, 2*(03), 1750014.
55. Wang, L., & Wang, G. (2016). Big data in cyber-physical systems, digital manufacturing and Industry 4.0. *International Journal of Engineering and Manufacturing (IJEM), 6*(4), 1-8.
56. Jiang, J.-R. (2018). An improved cyber-physical systems architecture for Industry 4.0 smart factories. *Advances in Mechanical Engineering, 10*(6), 1687814018784192.
57. Bagheri, B., Yang, S., Kao, H.-A., & Lee, J. (2015). Cyber-physical systems architecture for self-aware machines in Industry 4.0 environment. *IFAC-PapersOnLine, 48*(3), 1622-1627.
58. Zhou, K., Liu, T., & Liang, L. (2016). From cyber-physical systems to Industry 4.0: Make future manufacturing become possible. *International Journal of Manufacturing Research, 11*(2), 167-188.
59. Tao, F., Qi, Q., Wang, L., & Nee, A. Y. C. (2019). Digital twins and cyber–physical systems toward smart manufacturing and Industry 4.0: Correlation and comparison. *Engineering, 5*(4), 653-661.
60. Pivoto, D. G. S., de Almeida, L. F. F., da Rosa Righi, R., Rodrigues, J. J. P. C., Lugli, A. B., & Alberti, A. M. (2021). Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. *Journal of Manufacturing Systems, 58*, 176-192.
61. Colombo, A. W., Karnouskos, S., & Hanisch, C. (2021). Engineering human-focused industrial cyber-physical systems in Industry 4.0 context. *Philosophical Transactions of the Royal Society A, 379*(2207), 20200366.
62. Alohali, M. A., Al-Wesabi, F. N., Hilal, A. M., Goel, S., Gupta, D., & Khanna, A. (2022). Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in Industry 4.0 environment. *Cognitive Neurodynamics, 16*(5), 1045-1057.
63. Matsunaga, F., Zytkowski, V., Valle, P., & Deschamps, F. (2022). Optimization of energy efficiency in smart manufacturing through the application of cyber–physical systems and industry 4.0 technologies. *Journal of Energy Resources Technology, 144*(10), 102104.

64. Lee, J., Azamfar, M., & Singh, J. (2019). A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems. *Manufacturing Letters, 20*, 34-39.
65. Krugh, M., & Mears, L. (2018). A complementary cyber-human systems framework for industry 4.0 cyber-physical systems. *Manufacturing Letters, 15*, 89-92.
66. Fantini, P., Pinzone, M., & Taisch, M. (2020). Placing the operator at the centre of Industry 4.0 design: Modelling and assessing human activities within cyber-physical systems. *Computers & Industrial Engineering, 139*, 105058.
67. Singh, H. (2021). Big data, industry 4.0 and cyber-physical systems integration: A smart industry context. *Materials Today: Proceedings, 46*, 157-162.
68. Yan, J., Zhang, M., & Fu, Z. (2019). An intralogistics-oriented Cyber-Physical System for workshop in the context of Industry 4.0. *Procedia Manufacturing, 35*, 1178-1183.
69. Navickas, V., Kuznetsova, S. A., & Gruzauskas, V. (2017). Cyber–physical systems expression in industry 4.0 context. *Financial and Credit Activity: Problems of Theory and Practice, 2*(23), 188-197.
70. Nounou, A., Jaber, H., & Aydin, R. (2022). A cyber-physical system architecture based on lean principles for managing industry 4.0 setups. *International Journal of Computer Integrated Manufacturing, 35*(8), 890-908.
71. Sinha, D., & Roy, R. (2020). Reviewing cyber-physical system as a part of smart factory in industry 4.0. *IEEE Engineering Management Review, 48*(2), 103-117.
72. Xu, L. D., & Duan, L. (2019). Big data for cyber physical systems in industry 4.0: A survey. *Enterprise Information Systems, 13*(2), 148-169.
73. Cogliati, D., Falchetto, M., Pau, D., Roveri, M., & Viscardi, G. (2018). Intelligent cyber-physical systems for industry 4.0. In *2018 First International Conference on Artificial Intelligence for Industries (AI4I)*, pp. 19-22. IEEE.
74. Savtschenko, M., Schulte, F., & Voß, S. (2017). IT governance for cyber-physical systems: The case of Industry 4.0. In *Design, User Experience, and Usability: Theory, Methodology, and Management: 6th International Conference, DUXU 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings, Part I 6*, pp. 667-676. Springer International Publishing.
75. Sinha, D., & Roy, R. (2020). Reviewing cyber-physical system as a part of smart factory in industry 4.0. *IEEE Engineering Management Review, 48*(2), 103-117.
76. Abikoye, O. C., Bajeh, A. O., Awotunde, J. B., Ameen, A. O., Mojeed, H. A., Abdulraheem, M., Oladipo, I. D., & Salihu, S. A. (2021). Application of internet of thing and cyber physical system in Industry 4.0 smart manufacturing. In *Emergence of Cyber*

Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation (pp. 203-217). Cham: Springer International Publishing.

77. Mosterman, P. J., & Zander, J. (2016). Industry 4.0 as a cyber-physical system study. *Software & Systems Modeling*, *15*, 17-29.
78. Frontoni, E., Loncarski, J., Pierdicca, R., Bernardini, M., & Sasso, M. (2018). Cyber physical systems for industry 4.0: Towards real time virtual reality in smart manufacturing. In *Augmented Reality, Virtual Reality, and Computer Graphics: 5th International Conference, AVR 2018, Otranto, Italy, June 24–27, 2018, Proceedings, Part II 5* (pp. 422-434). Springer International Publishing.
79. Ahmadi, A., Sodhro, A. H., Cherifi, C., Cheutet, V., & Ouzrout, Y. (2019). Evolution of 3C cyber-physical systems architecture for industry 4.0. In *Service Orientation in Holonic and Multi-Agent Manufacturing: Proceedings of SOHOMA 2018* (pp. 448-459). Springer International Publishing.
80. Sbaglia, L., Giberti, H., & Silvestri, M. (2019). The cyber-physical systems within the industry 4.0 framework. In *Advances in Italian Mechanism Science: Proceedings of the Second International Conference of IFToMM Italy* (pp. 415-423). Springer International Publishing.
81. Sony, M. (2020). Design of cyber physical system architecture for industry 4.0 through lean six sigma: Conceptual foundations and research issues. *Production & Manufacturing Research*, *8*(1), 158-181.
82. Zhou, Z., Wang, B., Dong, M., & Ota, K. (2019). Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(1), 43-57.
83. Latif, S. A., Wen, F. B. X., Iwendi, C., Wang, F. W. L., Mohsin, S. M., Han, Z., & Band, S. S. (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Computer Communications*, *181*, 274-283.
84. Khalil, A. A., Franco, J., Parvez, I., Uluagac, S., Shahriar, H., & Rahman, M. A. (2022). A literature review on blockchain-enabled security and operation of cyber-physical systems. In *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1774-1779). IEEE.
85. Yu, C., Jiang, X., Yu, S., & Yang, C. (2020). Blockchain-based shared manufacturing in support of cyber physical systems: concept, framework, and operation. *Robotics and Computer-Integrated Manufacturing*, *64*, 101931.

86. Xue, H., Chen, D., Zhang, N., Dai, H.-N., & Yu, K. (2023). Integration of blockchain and edge computing in internet of things: A survey. *Future Generation Computer Systems, 144*, 307-326.
87. Al-Ghuraybi, H. A., AlZain, M. A., & Soh, B. (2023). Exploring the integration of blockchain technology, physical unclonable function, and machine learning for authentication in cyber-physical systems. *Multimedia Tools and Applications, 1-44*.
88. Zhao, W., Jiang, C., Gao, H., Yang, S., & Luo, X. (2020). Blockchain-enabled cyber–physical systems: A review. *IEEE Internet of Things Journal, 8*(6), 4023-4034.
89. Hazra, A., Alkhayyat, A., & Adhikari, M. (2022). Blockchain-aided integrated edge framework of cybersecurity for Internet of Things. *IEEE Consumer Electronics Magazine*
90. Wang, J., Chen, W., Ren, Y., Alfarraj, O., & Wang, L. (2020). Blockchain based data storage mechanism in cyber physical system. *Journal of Internet Technology, 21*(6), 1681-1689.
91. Ali, R. A., Ali, E. S., Mokhtar, R. A., & Saeed, R. A. (2022). Blockchain for IoT-Based Cyber-Physical Systems (CPS): Applications and Challenges. In *Blockchain based Internet of Things* (pp. 81-111).
92. Rathore, H., Mohamed, A., & Guizani, M. (2020). A survey of blockchain enabled cyber-physical systems. *Sensors, 20*(1), 282.
93. Al-Ghuraybi, H. A., AlZain, M. A., & Soh, B. (2023). Ensuring authentication in Medical Cyber-Physical Systems: A comprehensive literature review of blockchain technology integration with machine learning. *Multimedia Tools and Applications, 1-35*.
94. Mei, Q., Xiong, H., Chen, Y.-C., & Chen, C.-M. (2022). Blockchain-enabled privacy-preserving authentication mechanism for transportation cps with cloud-edge computing. *IEEE Transactions on Engineering Management*.
95. Rahman, Z., Khalil, I., Yi, X., & Atiquzzaman, M. (2021). Blockchain-based security framework for a critical industry 4.0 cyber-physical system. *IEEE Communications Magazine, 59*(5), 128-134.
96. Lampropoulos, G., & Siakas, K. (2023). Enhancing and securing cyber-physical systems and Industry 4.0 through digital twins: A critical review. *Journal of Software: Evolution and Process, 35*(7), e2494.
97. Yang, W., Tan, Y., Yoshida, K., & Takakuwa, S. (2017). Digital twin-driven simulation for a cyber-physical system in Industry 4.0. *DAAAM International Scientific Book, 201*, 227-234.

98. Rathore, S., & Park, J. H. (2020). A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems. *IEEE Transactions on Industrial Informatics, 17*(8), 5522-5532.

99. Xu, Q., Su, Z., & Yang, Q. (2019). Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system. *IEEE Internet of Things Journal, 7*(2), 1098-1110.

100. Mei, Q., Xiong, H., Chen, Y.-C., & Chen, C.-M. (2022). Blockchain-enabled privacy-preserving authentication mechanism for transportation cps with cloud-edge computing. *IEEE Transactions on Engineering Management*.

101. Wang, D., Song, B., Liu, Y., & Wang, M. (2022). Secure and reliable computation offloading in blockchain-assisted cyber-physical IoT systems. *Digital Communications and Networks, 8*(5), 625-635.

102. Lu, C., Saifullah, A., Li, B., Sha, M., Gonzalez, H., Gunatilaka, D., Wu, C., Nie, L., & Chen, Y. (2015). Real-time wireless sensor-actuator networks for industrial cyber-physical systems. *Proceedings of the IEEE, 104*(5), 1013-1024.

103. Liu, J., & Lin, J. (2019). Design optimization of WirelessHART networks in Cyber-Physical Systems. *Journal of Systems Architecture, 97*, 168-184.

104. Liu, W., Gong, Q., Han, H., Wang, Z., & Wang, L. (2018). Reliability modeling and evaluation of active cyber physical distribution system. *IEEE Transactions on Power Systems, 33*(6), 7096-7108.

105. Yu, X., & Xue, Y. (2016). Smart grids: A cyber–physical systems perspective. *Proceedings of the IEEE, 104*(5), 1058-1070.

106. Bhuiyan, M. Z. A., Wu, J., Wang, G., & Cao, J. (2016). Sensing and decision making in cyber-physical systems: The case of structural event monitoring. *IEEE Transactions on Industrial Informatics, 12*(6), 2103-2114.

107. Cortez, R. A. (2009). A cyber-physical system for situation awareness following a disaster situation. In *Realtime Systems Symposium* (pp. 37-44). Washington, DC: IEEE.

108. Liu, H., & Wang, L. (2020). Remote human–robot collaboration: A cyber–physical system application for hazard manufacturing environment. *Journal of Manufacturing Systems, 54*, 24-34.

109. Wang, X. V., Kemény, Z., Váncza, J., & Wang, L. (2017). Human–robot collaborative assembly in cyber-physical production: Classification framework and implementation. *CIRP Annals, 66*(1), 5-8.

110. Wang, L., Gao, R., Váncza, J., Krüger, J., Wang, X. V., Makris, S., & Chryssolouris, G. (2019). Symbiotic human-robot collaborative assembly. *CIRP Annals, 68*(2), 701-726.

111. Krüger, J., Lien, T. K., & Verl, A. (2009). Cooperation of human and machines in assembly lines. *CIRP Annals, 58*(2), 628-646.

112. Liu, H., Fang, T., Zhou, T., & Wang, L. (2018). Towards robust human-robot collaborative manufacturing: Multimodal fusion. *IEEE Access, 6*, 74762-74771.

113. Kirchner, E. A., de Gea Fernandez, J., Kampmann, P., Schröer, M., Metzen, J. H., & Kirchner, F. (2015). Intuitive interaction with robots–technical approaches and challenges. In *Formal Modeling and Verification of Cyber-Physical Systems* (pp. 224-248). Wiesbaden: Springer Vieweg.

114. Geravand, M., Flacco, F., & De Luca, A. (2013). Human-robot physical interaction and collaboration using an industrial robot with a closed control architecture. In *2013 IEEE International Conference on Robotics and Automation* (pp. 4000-4007). IEEE.

115. Tidwell, T., Gao, X., Huang, H.-M., Lu, C., Dyke, S., & Gill, C. (2009). Towards configurable real-time hybrid structural testing: A cyber-physical system approach. In *2009 IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing* (pp. 37-44). IEEE.

116. Zhen, S., Ma, Y., Wang, F., & Tolbert, L. M. (2019). Operation of a flexible dynamic boundary microgrid with multiple islands. In *2019 IEEE Applied Power Electronics Conference and Exposition (APEC)* (pp. 548-554). IEEE.

117. Pournazarian, B., Karimyan, P., Gharehpetian, G. B., Abedi, M., & Pouresmaeil, E. (2019). Smart participation of PHEVs in controlling voltage and frequency of island microgrids. *International Journal of Electrical Power & Energy Systems, 110*, 510-522.

118. Ogras, U. Y., Marculescu, R., Marculescu, D., & Jung, E. G. (2009). Design and management of voltage-frequency island partitioned networks-on-chip. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 17*(3), 330-341.

119. Liang, W., Long, J., Weng, T.-H., Chen, X., Li, K.-C., & Zomaya, A. Y. (2019). TBRS: A trust based recommendation scheme for vehicular CPS network. *Future Generation Computer Systems, 92*, 383-398.

120. Butts, J. A., & Sohi, G. S. (2000). A static power model for architects. In *Proceedings 33rd Annual IEEE/ACM International Symposium on Microarchitecture. MICRO-33 2000* (pp. 191-201). IEEE.

121. Chelcea, T., & Nowick, S. M. (2000). A low-latency FIFO for mixed-clock systems. In *Proceedings IEEE Computer Society Workshop on VLSI 2000. System Design for a System-on-Chip Era* (pp. 119-126). IEEE.

122. Moore, S., Taylor, G., Mullins, R., & Robinson, P. (2002). Point to point GALS interconnect. In *Proceedings Eighth International Symposium on Asynchronous Circuits and Systems* (pp. 69-75). IEEE.

123. Yang, J., Li, S., & Yu, X. (2012). Sliding-mode control for systems with mismatched uncertainties via a disturbance observer. *IEEE Transactions on Industrial Electronics, 60*(1), 160-169.

124. Profeta, J. A., Vogt, W. G., & Mickle, M. H. (1990). Disturbance estimation and compensation in linear systems. *IEEE Transactions on Aerospace and Electronic Systems, 26*(2), 225-231.

125. Yaz, E., & Ray, A. (1996). Linear unbiased state estimation for random models with sensor delay. In *Proceedings of 35th IEEE Conference on Decision and Control* (Vol. 1, pp. 47-52). IEEE.

126. Jin, M., Lee, J., & Ahn, K. K. (2014). Continuous nonsingular terminal sliding-mode control of shape memory alloy actuators using time delay estimation. *IEEE/ASME Transactions on Mechatronics, 20*(2), 899-909.

127. Lombardi, W., Altieri, M., Akgul, Y., Puschini, D., & Lesecq, S. (2014). Multivariable voltage and frequency control for DVFS management. In *2014 IEEE Conference on Control Applications (CCA)* (pp. 2028-2033). IEEE.

128. Brunton, S. L., & Kutz, J. N. (2019). *Data-driven science and engineering: Machine learning, dynamical systems, and control*. Cambridge University Press.

129. Kubendiran, M., Singh, S., & Sangaiah, A. K. (2019). Enhanced Security Framework for E-Health Systems using Blockchain. *Journal of Information Processing Systems, 15*(2), 239–250.

130. Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2018). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications, 13,* 45–58.

131. Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. In *Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA),* Agadir, Morocco, 29 November–2 December 2016.

132. Xiong, Z., Zhang, Y., Niyato, D., Wang, P., & Han, Z. (2018). When Mobile Blockchain Meets Edge Computing. *IEEE Communications Magazine, 56*(8), 33–39.

133. Zheng, J., Dike, C., Pancari, S., Wang, Y., Giakos, G. C., Elmannai, W., & Wei, B. (2022). An In-Depth Review on Blockchain Simulators for IoT Environments. *Future Internet, 14*(6), 182.

134. Dustdar, S., Avasalcai, C., & Murturi, I. (2019). Edge and fog computing: Vision and research challenges. In *Proceedings of the IEEE International Conference on Service-Oriented System Engineering (SOSE)*, San Francisco, CA, USA, April 2019, pp. 9609–9696.

135. Yahuza, M., Idris, M. Y. I. B., Wahab, A. W. B. A., Ho, A. T. S., Khan, S., Musa, S. N. B., & Taha, A. Z. B. (2020). Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities. *IEEE Access, 8*, 76541–76567.

136. Caprolu, M., Di Pietro, R., Lombardi, F., & Raponi, S. (2019). Edge computing perspectives: Architectures, technologies, and open security issues. In *Proceedings of the IEEE International Conference on Edge Computing (EDGE)*, Milan, Italy, July 2019, pp. 116–123.

137. Abdellatif, A. A., Mohamed, A., Chiasserini, C. F., Tlili, M., & Erbad, A. (2019). Edge computing for smart health: Context-aware approaches, opportunities, and challenges. *IEEE Network, 33*(3), 196–203.

138. Kamruzzaman, M. M., Yan, B., Sarker, M. N. I., Alruwaili, O., Wu, M., & Alrashdi, I. (2022). Blockchain and Fog Computing in IoT-Driven Healthcare Services for Smart Cities. *Journal of Healthcare Engineering, 2022,* Article ID 5169204.

139. Lee, J., Bagheri, B., & Kao, H. A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters, 3,* 18-23. https://doi.org/10.1016/j.mfglet.2014.12.001

140. Li, Z., Barenji, A. V., & Huang, G. Q. (2018). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robotics and Computer-Integrated Manufacturing, 54*, 133-144. https://doi.org/10.1016/j.rcim.2018.05.011

141. Lee, J., Kao, H. A., & Yang, S. (2014). Service innovation and smart analytics for Industry 4.0 and big data environment. *Procedia CIRP, 16*, 3-8. https://doi.org/10.1016/j.procir.2014.02.001

142. Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., & Reinhart, G. (2016). Cyber-physical systems in manufacturing. *CIRP Annals*. https://doi.org/10.1016/j.cirp.2016.06.005

143. Yang, L. (2017). Industry 4.0: A survey on technologies, applications, and open research issues. *Journal of Industrial Information Integration, 6*, 1-10.

144. Xu, X. (2012). From cloud computing to cloud manufacturing. *Robotics and Computer-Integrated Manufacturing, 28,* 75-86. https://doi.org/10.1016/j.rcim.2011.07.002

145. Sethi, A., & Sethi, S. (1990). Flexibility in manufacturing: A survey. *International Journal of Flexible Manufacturing Systems, 2*. https://doi.org/10.1007/BF00186471

146. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28,* 583-592. https://doi.org/10.1016/j.future.2010.12.006

147. Li, Z., Barenji, A. V., & Huang, G. Q. (2018). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robotics and Computer-Integrated Manufacturing, 54*, 133-144. https://doi.org/10.1016/j.rcim.2018.05.011

148. Swan, M. (2015). Rezension Blockchain: Blueprint for a New Economy. *O'Reilly Media, Inc*. https://doi.org/10.1365/s40702-018-00468-4

149. Lakhani, K. R., & Iansity, M. (2017). The Truth About Blockchain. *Harvard Business Review, 95,* 119-127. https://doi.org/10.1016/j.annals.2005.11.001

150. Montes, G. A., & Goertzel, B. (2019). Distributed, decentralized, and democratized artificial intelligence. *Technological Forecasting and Social Change, 141,* 354-358. https://doi.org/10.1016/j.techfore.2018.11.010

151. Luncai, & Josephlin, F. (2018). Distributed Artificial Intelligence Enabled by oneM2M and Fog Networking. In *2018 IEEE Conference on Standards for Communications and Networking (CSCN)* (pp. 1-8). https://doi.org/10.1109/CSCN.2018.8581775

152. Salah, K., Rehman, M. H., & Nizamuddin, N. (2018). Blockchain for AI: Review and Open Challenges. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2890507

153. Li, Z., Guo, H., Wang, W., Guan, Y., Barenji, A. V., & Huang, G. Q. (2019). A Blockchain and AutoML Approach for Open and Automated Customer Service. *IEEE Transactions on Industrial Informatics, 15*. https://doi.org/10.1109/TII.2019.2900987

154. Hedgebeth, D. (2007). Data-driven decision making for the enterprise: An overview of business intelligence applications. *Vine, 37,* 414-420

LIST OF PUBLICATIONS

Journal Publications:

Published:

1. Thakur, Payal & Sehgal, Vivek. (2021). Emerging Architecture for Heterogeneous Smart Cyber-Physical Systems for Industry 5.0. Computers & Industrial Engineering. 162. 107750. 10.1016/j.cie.2021.107750.

[SCI/SCOPUS INDEXED]

2. Thakur, Payal & Sehgal, Vivek. (2024). Synergizing edge computing and blockchain for cyber-physical systems. Concurrency and Computation: Practice and Experience. 10.1002/cpe.8066.

[SCI/SCOPUS INDEXED]

Under Review/Communicated

1. Thakur, Payal, and Vivek Kumar Sehgal. "Enhancing Trust and Security in Industry 4.0 Cyber-Physical Systems through Blockchain Integration" SN Computer Science (Under Review)

[SCIE/SCOPUS INDEXED]

Paper presented in Conferences:

1. Thakur, Payal & Sehgal, Vivek. (2022). Temperature Management Using Smart Thermostat in Cyber Physical Systems. 1-5. 10.1109/DELCON54057.2022.9752874.
2. Thakur, Payal & Sehgal, Vivek. (2022). A framework for IoT based on Blockchain and Edge Computing in Cyber Physical Systems. 1-6. 10.1109/INDICON56171.2022.10040170.