IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 December 2023, accepted 19 December 2023, date of publication 1 January 2024,
date of current version 16 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3349022

RESEARCH ARTICLE

A Systematic Analysis of Enhancing Cyber Security Using Deep Learning for Cyber Physical Systems

SHIVANI GABA[1], ISHAN BUDHIRAJA[1], (Member, IEEE), VIMAL KUMAR[1], (Member, IEEE), SHESHIKALA MARTHA[2], (Member, IEEE), JEBREEL KHURMI[3], AKANSHA SINGH[1], (Member, IEEE), KRISHNA KANT SINGH[4], S. S. ASKAR[5], AND MOHAMED ABOUHAWWASH[6,7]

[1]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh 201310, India
[2]School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana 506371, India
[3]Department of Computer Science, College of Technology, Jazan University, Jazan 45142, Saudi Arabia
[4]Delhi Technical Campus, Greater Noida 201306, India
[5]Department of Statistics and Operations Research, College of Science, King Saud University, Riyadh 11451, Saudi Arabia
[6]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura 35516, Egypt
[7]Department of Computational Mathematics, Science and Engineering, College of Engineering, Michigan State University, East Lansing, MI 48825, USA

Corresponding author: Akansha Singh (akansha1.singh@bennett.edu.in)

This project is funded by King Saud University, Riyadh, Saudi Arabia. Researchers Supporting Project number (RSP2024R167).

ABSTRACT In this current era, cyber-physical systems (CPSs) have gained concentrated consideration in various fields because of their emergent applications. Though the robust dependence on communication networks creates cyber-physical systems susceptible to deliberated cyber related attacks and detecting these cyber-attacks are the most challenging task. There is the interaction among the components of the cyber and physical worlds, so CPS security needs a distinct approach from past security concerns. Deep learning (DL) distributes better performance than machine learning (ML) due to its layered architecture and the efficient algorithm for extracting prominent information from training data. So, the deep learning models are taken into consideration quickly for detecting cyber-attacks in cyber physical systems. As numerous attack detection methods have been proposed by various authors for enforcing CPS security, this paper reviews and analyzes multiple ways of attack detection presented for CPS using deep learning. We will be putting the excellent potential for detecting cyber-attacks for CPS concerning deep learning modules. The admirable performance is attained partly as highly quality datasets are eagerly obtainable for the use of the public. Moreover, various challenges and research inclinations are also discussed in impending research.

INDEX TERMS Cybersecurity, cyberattacks, cyber physical systems (CPSs), deep learning (DL), attack detection.

I. INTRODUCTION

As there is a fast growth of technology in various communication networks and the field of computer science leads, cyber-physical systems (CPS) are rising widely in both areas, such as academia and industries. The cyber-physical systems are measured and supervised by computer-based algorithms, which are combined with networks and users. The cyber-physical systems comprise interacting network units with physical and computational devices. The applications of CPS are making a disproportionate impact on businesses, such as in industrial sectors, healthcare, and manufacturing.

As soon as the Internet of Things (IoT) initiates, various devices with security susceptibilities are connected to cyber-physical systems, resulting in multiple attacks. It has been observed in past years that the incidents of CPS attacks have increased after the Stuxnet attack back in 2010 [1]. If cyber-physical systems attacks are not perceived and reduced rapidly, they can cause massive consequences such

The associate editor coordinating the review of this manuscript and approving it for publication was Engang Tian.

as damage to equipment, financial losses, and public safety. So the security of CPS is one of the vital paradigms for this. But securing cyber-physical systems is also a challenging task due to its heterogeneity of components, complex interactions among cyber-physical systems, and the attack surface's complexities [2]. It is observed that an intruder can randomly interrupt the dynamism of systems or encourage agitations to cyber-physical systems deprived of the security of various strategies of hardware or software, which leads to substantial social victims or the lives of humans [3], [4], [5], [6], [7], [8], [9]. If cyberattacks are perceived and positioned quickly, the loss to overall systems will be measured within the acceptable time limit. Much of the existing literature on the detection of attacks is dependent on centralized architectures [10], [11], [12], [13].The attack detection schemes are usually categorized into knowledge-based and data-driven approaches [14]. The residual generation method is one of the representative detection strategies in many knowledge-based systems [15], [16], [17]. Usually, residual is intended by comparison of measurements of sensors and systematic model of the system. Afterward, it is equated with the static or time-variant threshold for determining whether it is an attack or not. In the case of data-driven methods, deep learning approach and heuristic algorithms are used for building models of cyber-physical systems [18], [19]. If this does not follow these associations, then the attack is assumed. Apart from centralized systems, many kinds of distributed systems appear nowadays. The main challenge of designing a distributed attack detection method is monitoring cyber-physical systems without adequate information. Most cyber-physical systems lack various cyber security mechanisms, such as message authentication, which results in numerous challenges for detecting data injection attacks [20]. The absence of worldwide encryption, mainly on systems engaging in dated technologies, makes it exciting to secure in contradiction of eavesdropping attacks. So, it is required to refer replay attacks. According to the report on the global cyber-physical system market and data bridge market research, the historical market and forecast CAGR is 7.8%. The traffic in global cyber-physical systems is expected to account for USD 12,356.23 million by 2028. This increase in traffic increases the burden on the CPS systems as the market increases. To overcome this problem, the researchers of both academia and industry explored this market, and as a result, the various privacy preservation methods are explored.

A. PROBLEM FORMULATION

Although there are various advantages of cyber-physical systems, these systems are susceptible to numerous cyber or physical security threats, attacks, and challenges. This occurs due to its non-homogeneous nature and dependency on sensitive and private data. This kind of planned or accidental acquaintance with these systems leads to terrible effects, which results in complex security measures. Though this leads to the undesirable overhead of networks. So the security measures of a cyber-physical system are required to formulate. Figure 1 represents the review methodology of this paper. It represents the searching process and reviewing results. The authors have read the various papers for collecting the noticeable information and deliberate the cyber physical systems, fault and failures, cyber security standards, and various challenges.

B. WHY DEEP LEARNING FOR CYBER PHYSICAL SYSTEMS (CPS)

Deep Learning (DL) [21], [22], [23] gives better results as compared to machine learning (ML). In case of passable data, deep learning models provide the best results. Even deep learning models are applied for solving cyber-physical system cybersecurity issues compared to other fields. It is also experiential that various deep learning models are anticipated in current publications for detecting cyber-physical systems' cyber-attacks. The main is not only the way to describe the difficulty of cyber-attack detections on cyber-physical systems; the main complexity arises when superimposing cyber security over cyber-physical systems [24]. Various authors have not had a detailed discussion on applying deep learning methods for detecting cyber-attacks contrary to cyber-physical systems. The brief survey was given by authors [25] with a four-step framework that uses deep learning methods for detecting cyber-physical systems cyber-attacks. The biggest concern nowadays is the security of CPS. Deep Learning approaches are precisely intended to handle large datasets compared to small datasets with numerous features. These methods can approximate any function as deep learning has a rich class of models. All these methods are appropriate in cyber-physical systems due to the following reasons:

- Information gathered from CPSs is commonly high layered as information from countless physical sensors and cyber sensors.
- A steady development of information because of upgrades and openness to novel susceptibilities are there.
- The models should be continually refreshed with novel information to represent the drifting of the framework and further vector assaults.

1) DEEP LEARNING WITH CPS

Deep learning has emerged as a powerful technique for handling the complexities of Cyber Physical Systems (CPS). It has been applied to various CPS applications such as anomaly detection, fault diagnosis, control, and optimization.

Deep learning algorithms such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Deep Belief Networks (DBN) have been used for CPS applications. CNNs have been used for image and signal processing tasks in CPS, while RNNs have been used for time-series data analysis in CPS. DBNs have been used for fault diagnosis and anomaly detection in CPS.

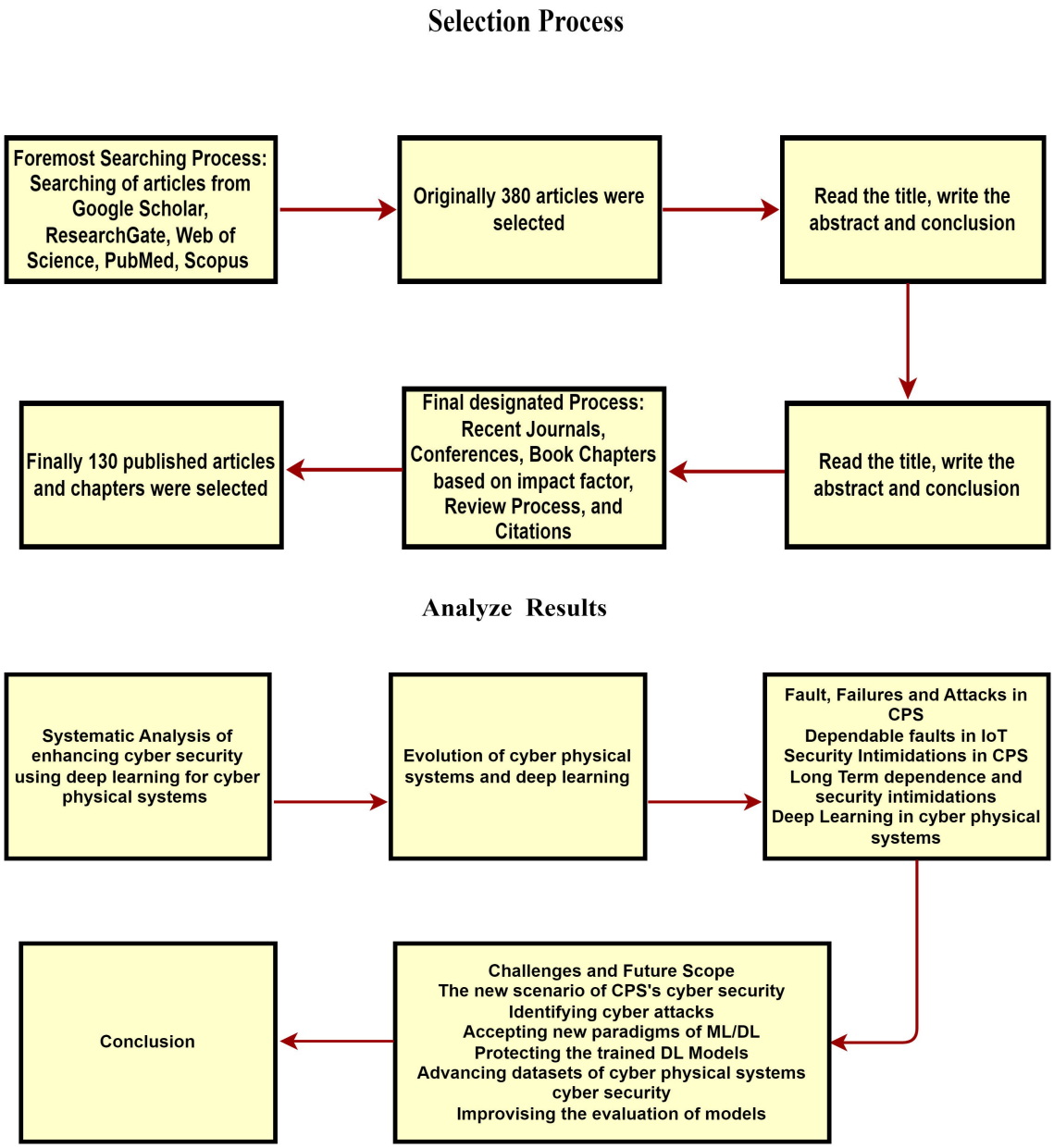

FIGURE 1. Methodology for selecting and analysing the survey.

Deep learning models require large amounts of data for training, and CPS data is often limited and expensive to collect. Transfer learning techniques have been applied to leverage pre-trained models and overcome this challenge. Additionally, the security of CPS can also be enhanced using deep learning techniques, such as using autoencoders for intrusion detection, and generative adversarial networks (GANs) for generating adversarial examples to improve the robustness of CPS. Overall, deep learning has shown promising results in various CPS applications and is expected to play a significant role in advancing the state-of-the-art in CPS.

C. QUANTUM LEARNING WITH CPS

Quantum machine learning is an emerging field that combines quantum computing and machine learning techniques to solve complex problems. However, quantum computing technology is still in its early stages of development, and its practical applications in the field of cybersecurity and CPS are still largely theoretical.

One of the potential advantages of quantum machine learning for CPS security is its ability to perform complex calculations faster than classical computing, which could potentially speed up the detection and response to cyber attacks. However, the development of quantum machine

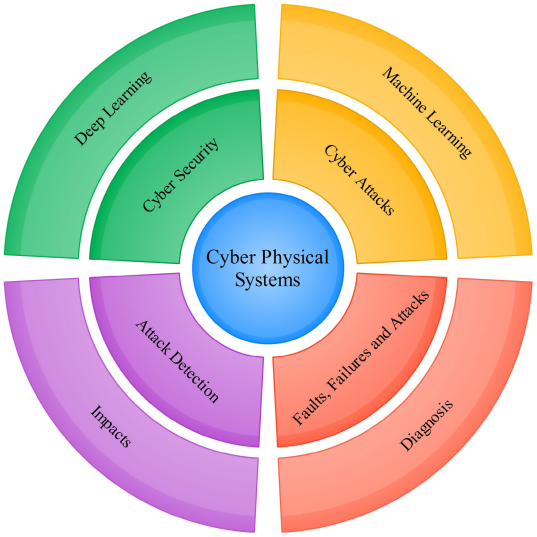

FIGURE 2. Broad division of concepts discussed in the paper.

learning algorithms and their integration into CPS systems is still a topic of ongoing research. Quantum learning with CPS is a promising area of research, but its practical applications in the field of cybersecurity and CPS are still largely speculative, and much work is needed to develop and test quantum machine learning algorithms for real-world CPS systems.

D. DEEP LEARNING AND QUANTUM LEARNING WITH CPS

Deep learning and quantum learning are two areas of research that can have potential applications in Cyber-Physical Systems (CPS).

Deep learning involves training deep neural networks to perform complex tasks, such as image and speech recognition, natural language processing, and even autonomous decision-making. In CPS, deep learning can be used to analyze large volumes of data generated by sensors and devices in real-time, detect anomalies and potential threats, and make accurate and timely decisions to ensure the safety and security of the system.

Quantum learning, on the other hand, uses the principles of quantum mechanics to process and analyze data. It involves the use of quantum algorithms and quantum computers to solve problems that are computationally infeasible using classical computers. In CPS, quantum learning can be used to optimize the performance of the system, reduce energy consumption, and enhance security by developing quantum-resistant encryption algorithms.

While both deep learning and quantum learning have potential applications in CPS, they are still in the early stages of development and require further research to fully understand their capabilities and limitations in this domain.

E. CONTRIBUTIONS

In this paper, we undertake an extensive investigation into the application of deep learning for cyber-attack detection within cyber-physical systems (CPS). Our contributions encompass:

- Here in this paper, authors have performed an exhaustive survey of contemporary methods and techniques for cyber-attack detection in CPS, harnessing the capabilities of deep learning.
- The authors have introduced a rigorous methodological framework that serves as the cornerstone of the research. This framework not only positions our work within the current landscape but also facilitates the systematic analysis and evaluation of recent developments in this domain.
- A comprehensive examination of reliability failures and security threats, specifically tailored to the various layers of CPS architecture.
- The authors have delved into the realm of solutions with meticulous attention to technical intricacies. The discussions provide in-depth insights into the implementation of security measures, considering factors such as encryption algorithms, anomaly detection thresholds, and real-time monitoring mechanisms.
- In an alignment with the core theme, the authors have engaged in a technical discourse surrounding challenges and future trends. This includes embracing novel paradigms in machine learning (ML) and deep learning (DL), devising techniques to safeguard trained DL models from adversarial attacks, advancing the construction of CPS cybersecurity datasets with a focus on data diversity and volume, and enhancing the technical rigor of model evaluation methodologies.

F. MOTIVATIONS

As soon as the intelligent computing systems introduce predictable intelligence towards the issues of cyber, so the researchers are more inclined to use intelligent computing for secure computations, as there are various challenges for detecting attacks also. The question is whether computation spectacle can help improve security concerns. The security of Cyber physical systems is a significant concern, and that's why it is mandated to study the safety of cyber physical systems. So an analysis of cyber security of the cyber physical system is required, and it is presented in this work.The taxonomy of paper is shown in Figure 3.

G. ORGANIZATION

The rest of the paper is categorized into various subsections: Section II describes the literature review of evolution of cyber physical systems and deep learning. Section III discusses the Mathematical Modeling Framework for Enhancing Cyber Security in Cyber-Physical Systems using Deep Learning. Section IV describes the fault, failures and attacks in cyber physical systems. Open issues for securing CPS are described in Section V.Challenges and Future Scope is described in Section VI. Finally paper is concluded in Section VII.

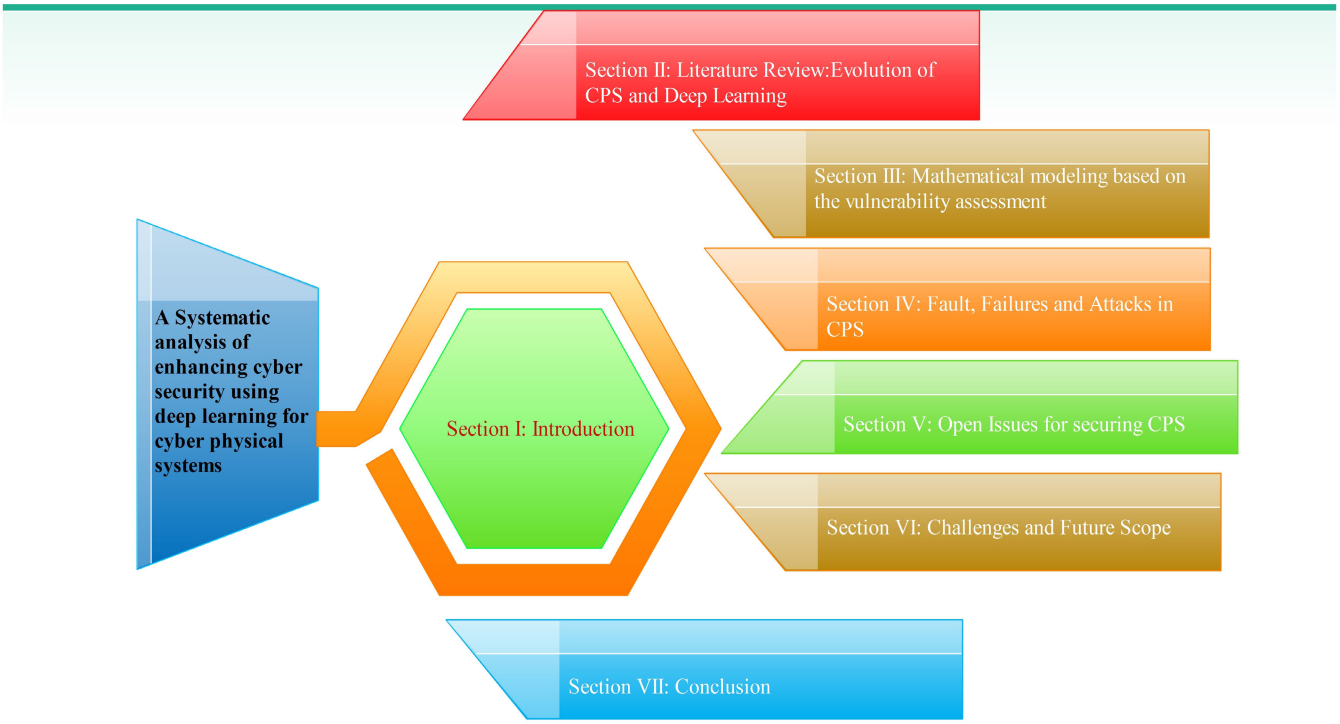

FIGURE 3. Organization of paper.

II. LITERATURE REVIEW: EVOLUTION OF CYBER PHYSICAL SYSTEMS AND DEEP LEARNING

Cyber-Physical System (CPS) is the coordination of computers with existing frameworks. The embedded computer screen, the actual control cycles, the feedback loops, and the physical approaches also influence calculations. Cyber-Physical System is near to convergence, with no association of the physical and the cyber world as a conceptual motivation. It consolidates designing representations and strategies from mechanical, ecological, typical, electrical, biomedical, compound, aeronautical, and modern designing with the models and techniques for software engineering. As the expressions ''the internet'' and ''cyber-physical system'' originate via a similar root, ''computer science,'' which is authored by Norbert Wiener [5], an American statistician who enormously affected the advancement of control frameworks theory, would be more precise. Wiener spearheaded innovation for the programmed pointing and shooting of hostile airplane weapons. Albeit the components he utilized didn't include computerized PCs, the standards contained are like those pre-owned nowadays in computer-based criticism controller frameworks [26]. The control rationale is a calculation, though one has done via simple circuits and mechanical portions, and consequently, computer science is the combination of actual cycles, analysis, and correspondence. The similitude is adept for control frameworks.

CPS is here and is mistaken for ''online protection,'' which concerns the secrecy, uprightness, and accessibility of information and has no characteristic association with actual cycles. The expression ''network protection'' along these lines is about the security of the internet and is subsequently, by implication, associated with computer science. CPS includes many testings security and protection concerns, yet these are in no way, shape, or form the main worries.

It is an innovation in that intelligence associates our actual world with our data world. Cyber Physical Systems is more essential and solid than these as it doesn't directly reference either execution draws near or precise applications like ''Industry'' in Industry 4.0. It centers as a substitute to the principal scholarly issue of adjoining the designing customs of the digital and an actual universe. One could discuss a CPS hypothesis like the ''direct frameworks hypothesis.'' CPS has turned out to be a common factor in critical infrastructure because of its massive influence and commercial assistance [6]. The growing reliance of crucial infrastructure on cyber-based skills has turned them susceptible to cyber-assaults like interference, auxiliary, and exclusion of data from the communique networks [7], [8], [9].' Therefore, the sanctuary of cyber-physical systems has become a perilous concern. A brief history of computer systems and cyber physical systems is illustrated in Figure 3.

Deep Learning (DL) has acquired huge consideration in previous years. It has worked on the state-of-art execution of numerous claims, remembering applications related to security for basic designs, like interruption identification, malware discovery, access control, and peculiarity recognition and orders [6]. DL was presented in the late twentieth era, which was begun with the investigation of Artificial Neural

FIGURE 4. Taxonomy of survey.

Networks (ANNs). Deep Neural Networks (DNN) comprise a set of layers that gain proficiency with a progression of hidden portrayals progressively [27], [28]. Higher-level descriptions contain enhanced parts of information tests that are helpful for segregation and stifle unessential highlights. Deep Learning models have worked on the cutting-edge execution in various assignments [10], [11]. The summary of related works of various methods and applications are shown in Table 1.

Figure 4 delineates the general idea of cyber-physical systems and the IoT for cyber physical systems. It displays current cyber-physical systems, how elements could be separated from such frameworks, conceivable deep learning models, and the benefits of utilizing deep learning [29]. Furthermore, the information gathered from existing digital frameworks is ordinarily high layered. Deep Learning models are explicitly intended to manage high layered information. Different attributes of CPS incorporate, proceed with the development of data, information float, and openness to new framework dangers. This way, it is crucial to assemble deep learning-based sanctuary models which are versatile and extendible with the information float, nonstop disclosure of new framework dangers and weaknesses [12].

This idea of "Generalization" is one significant issue for constructing security-based requests in cyber-physical systems as creating AI models for one situation is almost difficult to use, experiencing the same thing even in a similar setting. In this manner, it is a quintessence to zero in on speculation that deep learning models utilized in such applications are ordinarily high layered. Deep Learning models are explicitly intended to manage high-layered information. Different attributes of CPS incorporate, proceed

with the development of data, information float, and openness to new framework dangers. This way, it is crucial to assemble deep learning-based security models which are versatile and extensible by the information float, nonstop disclosure of new framework dangers and weaknesses [12]. This idea of ''Generalization'' is one significant issue for constructing security-based requests in cyber-physical systems as creating AI models for one situation is almost difficult to use, experiencing the same thing even in a similar setting. It is illustrative to zero in on speculation of deep learning models utilized in such applications [30], [31].

III. MATHEMATICAL MODELING BASED ON THE VULNERABILITY ASSESSMENT

The mathematical modeling framework for enhancing cyber security in Cyber-Physical Systems (CPS) using deep learning, based on the vulnerability assessment are stated below and explained in figure 5.

1) **Problem Formulation:** Minimize the objective function $J(\Theta)$, representing the cost or vulnerability.
2) **System Representation:** Define the CPS system as $CPS = \{C_1, C_2, \ldots, C_n\}$. Enumerate vulnerabilities as $Vulnerabilities = \{V_1, V_2, \ldots, V_m\}$.
3) **Threat Modeling:** Define a Threat Vector $T = [T_1, T_2, \ldots, T_k]$ representing potential threats.
4) **Deep Learning Integration:** Integrate deep learning models to process system information. Define the model's output as f_Θ(Input).
5) **Data Requirements:** Specify the dataset $D = \{(Input_1, Label_1), \ldots, (Input_N, Label_N)\}$ for model training.
6) **Mathematical Equations:** Develop equations to quantify vulnerability levels.

$$\text{Vulnerability Level} = g(\text{Threat Vector, Deep Learning Output})$$

7) **Quantification of Vulnerabilities:** Assign a vulnerability score based on the vulnerability level.

$$\text{Vulnerability Score} = h(\text{Vulnerability Level})$$

8) **Validation and Verification:** Establish validation metrics to evaluate model performance. $ValidationMetric = ValidationFunction(ModelOutput, GroundTruth)$
9) **Sensitivity Analysis:** Assess model sensitivity to parameter changes. $Sensitivity = \frac{\partial J}{\partial \Theta}$
10) **Limitations and Assumptions:** Clearly state any assumptions and limitations in the model.

$$\text{Assumption}_i : \ldots$$
$$\text{Limitation}_j : \ldots$$

11) **Comparative Analysis:** Develop metrics for comparing the model against other approaches.

$$\text{Comparison Metric} = \text{Compare(Model, Other Models)}$$

12) **Implications and Recommendations:** Discuss the implications of the findings. Provide recommendations for practical applications.

IV. FAULT, FAILURES AND ATTACKS IN CYBER PHYSICAL SYSTEMS

A failure is an occurrence that arises when an organization diverges as of its planned performance. The failure establishes because of its inadvertent state. The origin of a fault might be internal or external. The internal faults occur due to their physical nature (such as brokerage of the component connector), and faults occur due to their design (software or hardware-related bugs) [55]. Peripheral faults (External) initiate from the environmental cause like noise. Faults may be categorized into permanent and temporary faults. However, a temporary fault occurs for short time span. It may create an error, and this may lead to perpetual failure. Similarly, Physical faults and inputs can be temporary or it can be permanent, whereas the design faults are constantly permanent. The faults which could not be analytically imitated are usually known as irregular faults. This kind of fault can be led to soft errors.

The cyber-physical systems/Internet of Things (CPS/IoT) infrastructure is shown in the figure. Faults might arise at diverse layers of architecture, such as the physical layer or control layer, respectively [13]. The physical layer is susceptible to interruption, direct interference, or demolition of physical items. The network layer can make the connection of devices. The monitors and controllers in the control layer are susceptible to environmental uncertainties and handling of extents and control signals [55], [56]. The collection of information can be done by the information layer and is mainly vulnerable to issues related to secrecy and integrity.

A. DEPENDABLE FAULTS IN IoT

Internet of Things tends to communicate failures primarily due to its extent and heterogeneousness. Previously, traditional cyber-physical systems used to ignore or remove such failures by validating and verifying the design. Though IoT is involved in technology, it is growing in size with time. The subsequent faults might arise per cyber-physical systems layer:

- **Physical Layer: - Intrusion:** Interference of a signal. The quantity of associated devices and the radiation rises, affecting measurements of sensors, conveyed communications, or control indications.
- **Network Layer: - Collision of Messages:** In correspondence to intrusion, the quantity of interactive devices may activate communique failures such as crashes or overloading of the net- ' work. - Violation of Protocol:

TABLE 1. Summary of different methods and applications in the context of Deep Learning and CPS by various authors, along with challenges in ML algorithms.

Methods	Deep Learning	Application	Cyber Physical Systems	Reference	Challenges in ML Algorithms
Classification based techniques, Clustering based techniques, Statistical, anomaly recognition approaches	No	Cyber Interruption Detection, Detection of Fraud, etc	No	[32]	Limited labeled data, imbalanced datasets, model interpretability
Program Analysis	No	Commodity Internet of Things	Related but not fully covered	[33]	Scalability, real-time processing
Physical properties	No	Cyber Physical Systems	Yes	[34]	Sensor noise, environmental variability
Deep learning	Yes	Cyber Interruption Detection, Detection of Fraud	No	[35]	Model complexity, computational resources
Attack Based Tree, Model-based technique	No	Cyber Physical Systems (focus on SCADA)	Yes	[36]	Security of control systems, attack detection
Deep learning	Yes	Cyber Physical Systems	Yes	[37]	Scalability, real-time processing
Knowledge-Based technique, Behaviour-Based Interruption Recognition system	No	Cyber Physical Systems	Yes	[38]	Knowledge representation, anomaly detection
Interruption Detection system, Machine learning	No	Cyber Physical Systems	Yes	[39]	False positives, adaptive adversaries
-	-	Smart home IoT	Related but not fully covered	[40]	Privacy, device heterogeneity
Plant models based technique, Noise-based detection, State estimation based technique	No	Cyber Physical Systems	Yes	[41]	Model accuracy, noise robustness
Deep learning	Yes	Internet of Things	No	[42]	Energy efficiency, resource constraints

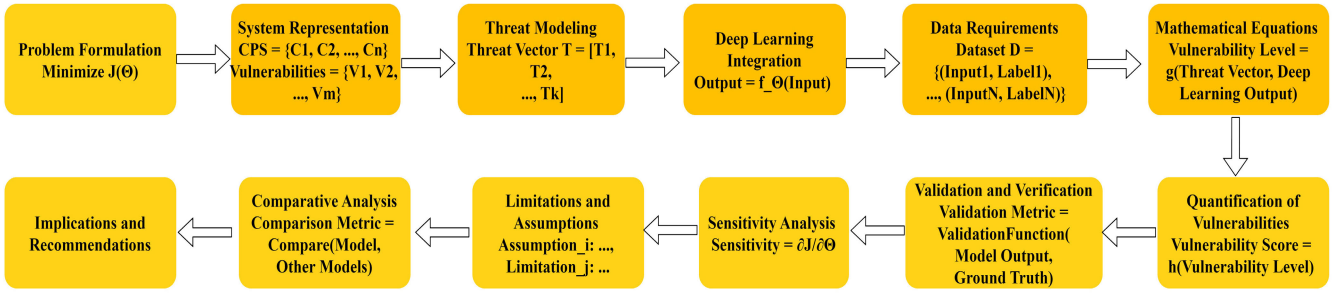

FIGURE 5. Mathematical modeling framework for enhancing cyber security in cyber-physical systems using deep learning.

The protocol violation occurs due to incorrect message content.

- **Control Layer: - Deadline Miss:** Delayed in the response of control signal. The Control loops has to survey the restraints related to timing of a cyber-physical system application. - Misusage: Sending erroneous inputs to a component
- **Information Layer: - Inaccessibility:** Lost data instigated by a skill apprise. The things might be linked, detached, or updated in the Internet of Things.

B. SECURITY INTIMIDATIONS IN CYBER-PHYSICAL SYSTEMS

Security has been one of the biggest concerns in computer networks to identify susceptibilities and avoid malicious attacks on the devices. Whereas in cyber-physical systems, more and more susceptibilities arise in the physical area and the indeterminate behavior of the physical atmosphere. The categorization of attacks applied per cyber-physical systems layer is given below:

- **Physical Layer: - Information Leakage:** Stealing perilous information from various devices such as private keys - Denial of Service: Manipulating various parameters for performing DoS attacks.
- **Network Layer: - Jamming:** Overloading the communication protocol by introducing false traffic. - Collision: Manipulation of timing, the power which leads to collision of data or violation of communication protocol. - Routing misdirects: Manipulating the routing mechanism leads to collision of data, flooding of data, and discriminating promoting of facts [57], [58].
- **Control Layer: - Desynchronizing:** Violating the timing or manipulation of clocks. This could lead to denial of service and leakage of information.
- **Information Layer: - Eavesdropping:** Stealing or sniffing of information. It is one of the biggest intimidations associated with confidentiality. Furthermore, data could also be deployed to accomplish various attacks. The potential intimidations and penalties could be stated in sanctuary intimidation models for cyber-physical systems.

TABLE 2. A systematic analysis of enhancing cyber security using deep learning for cyber physical systems" vs. existing survey papers.

Paper Reference	Scope and Focus	Methodological Approach	Technical Depth	Contributions	Originality
[43]	Smart Grid attacks, vulnerabilities, detection and defences	Review, analysis, and synthesis	Moderate	Identify key challenges, proposed solutions	Focused on existing attacks and defenses
[44]	IoT intrusion detection methods	Review, analysis, and synthesis	Moderate	Classification and detection techniques	Explores existing methods
[45]	ML techniques in CPS cyber security	Review, analysis, and synthesis	Moderate	Comparative analysis of methods	Emphasis on existing ML techniques
[46]	Survey on deep learning-based attack detection in CPS cybersecurity	Analytical survey of existing literature, summarizing key techniques and challenges	High technical depth, covers a wide range of deep learning techniques in the context of CPS security	Comprehensive analysis and insights into the state-of-the-art in deep learning -based attack detection for CPS cybersecurity	Original in presenting a holistic view of deep learning in CPS attack detection
[47]	Review of security analysis in CPS using machine learning	Literature review and analysis of machine learning applications in CPS security	Moderate technical depth, focuses on summarizing existing research in the domain	Provides a comprehensive review of security analysis in CPS using machine learning techniques	Original in presenting a consolidated overview of ML applications in CPS security
[25]	Survey on the generalization of deep learning for CPS security	Analytical survey of deep learning generalization techniques in CPS security	Moderate technical depth, emphasizing generalization aspects	Offers insights into the challenges and opportunities in applying deep learning for CPS security with a focus on generalization	Original in exploring generalization aspects in deep learning for CPS security
[48]	Survey on resilient machine learning for networked CPS	Analytical survey of machine learning security in the context of networked CPS	High technical depth, covers a range of resilient machine learning techniques	Provides a comprehensive survey on securing machine learning in networked CPS environments	Original in addressing resilience challenges in machine learning for networked CPS
[49]	Survey on deep learning-based anomaly detection in CPS	Analytical survey of progress, challenges, and opportunities in deep learning-based anomaly detection	High technical depth, explores various deep learning-based approaches	Offers a comprehensive overview of the progress and potential in deep learning-based anomaly detection for CPS	Original in presenting a state-of-the-art survey on anomaly detection in CPS using deep learning
[50]	Federated deep learning for intrusion detection in industrial cyber–physical systems	DeepFed: Federated deep learning	High	Intrusion detection, Federated learning	Novel approach in applying federated learning to industrial CPS
[51]	Attack graph model for cyber-physical power systems using hybrid deep learning	Hybrid deep learning approach	High	Attack graph modeling, Smart Grid security	Integration of deep learning into attack graph modeling for power systems
[52]	Real-time stability assessment in smart cyber-physical grids: a deep learning approach	Deep learning for real-time stability assessment	Moderate	Stability assessment in smart grids	Application of deep learning to real-time stability analysis in smart grids
[53]	Blockchain-based deep learning approach for cybersecurity in next-generation industrial cyber-physical systems	Blockchain and deep learning integration	High	Cybersecurity, Blockchain, Industrial CPS	Unique combination of blockchain and deep learning for enhanced cybersecurity
[54]	Deep learning-based DDoS-attack detection for cyber–physical system over 5G network	Deep learning for DDoS attack detection	High	DDoS attack detection, 5G networks	Application of deep learning for DDoS detection in 5G- enabled CPS
Our Paper	CPS security using DL	Systematic analysis	High	Innovative solutions, key challenges, and insights	Emphasis on original insights

C. LONG-TERM DEPENDENCE AND SECURITY INTIMIDATIONS

The Internet of things and cyber-physical systems will endure deviations over time, particularly when imperiled by a long operational period. Following features of the change might cause faults such as changes in the environment, functional changes, and changes in technology.The catagories of attacks implied on different CPS systems are mentioned below:

- **Physical Layer:**At this layer there is material decay and environmental effects issues at this layer and this voilates the environment.
- **Network Layer:**It overloads the information by putting false traffic on the network. Due to this the communication through protocol also voilates.
- **Control Layer:**It disturbs the timing or manipulates the clocks this leads to the aging effects and uncertainity effects.

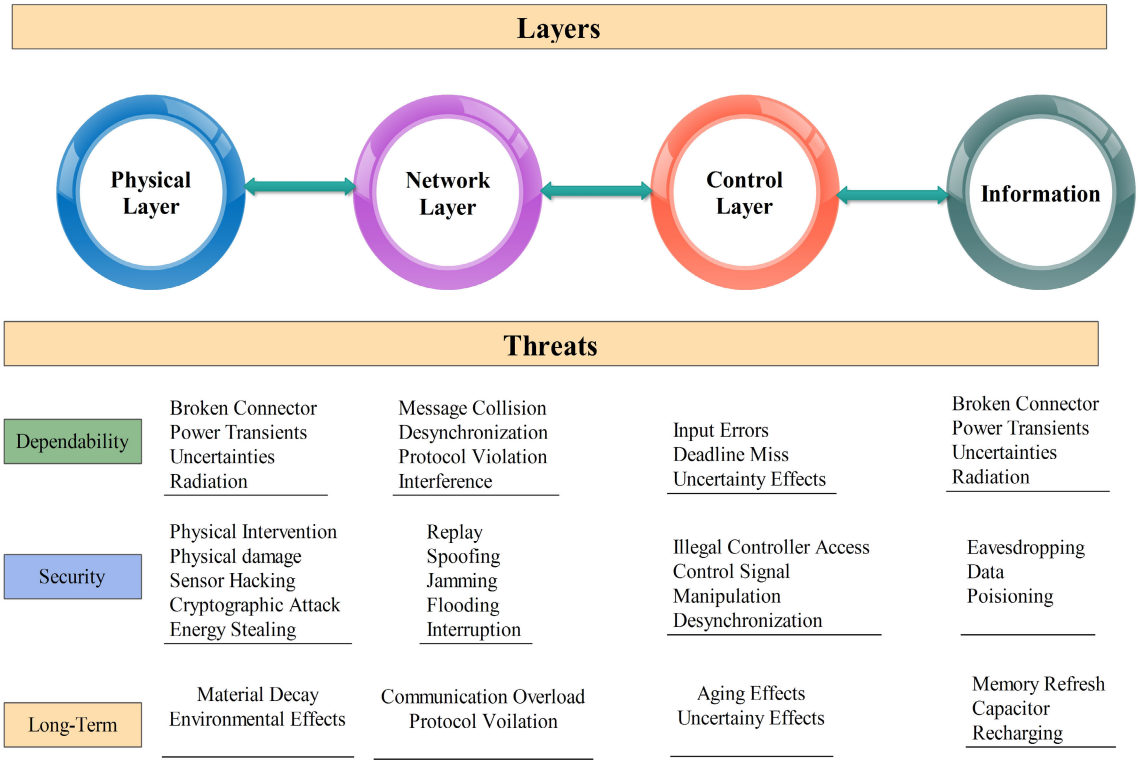

FIGURE 6. Reliability failures and sanctuary intimidations with reference to cyber physical systems layers.

TABLE 3. Threat models for different CPS layers.

Layers	Physical Layer	Sensor/Actuator Layer	Communic-ation Layer	Control Layer	Information Layer	Integration level Layer
Attacks	Manufacturer, Designer, External Attacker	Manufacturer, Designer, External Attacker	Manufacturer, Designer, External Attacker	Manufacturer, Designer, External Attacker	Manufacturer, Designer, External Attacker	Manufacturer, Designer, External Attacker
Methodology	Physical Interference	Hacking, Control Access, Information Influences	Replay, Sybil, Congestion, Implosion, Deceiving	Eavesdropping, Control Access	Eavesdropping	All conceivable control & Communication assaults
Payloads	Denial of Service, Aging Consistency	Energy Stealing, Denial of Service, Data Leakage, Desynchro-nization	Energy Thieving, Denial of Service, Information Leakage, Desynchro-nization	Leakage of Information, Denial of Service, Desynch-ronization	Leakage of Information	Stealing of energy, Denial of Service, Leakage of Information, Desynchron-ization

- **Information Layer:**The biggest itimidation concerned with confidentiality is stealing of information. The refershing of memory, recharging is theissues relaed to this layer.

D. DEEP LEARNING IN CYBER-PHYSICAL SYSTEMS

Here we discuss how deep learning can be applied in CPS. So, the introduction of deep learning is required for how it is used in security-related applications such as CPSs. Nowadays, DL is gaining huge focus in data science to enhance performance in various applications [12]. Deep Learning Algorithms contain hierarchical architectures with many layers in which higher-level features are explained in standings of lower-level features capable for the extraction of features and concepts from underlying data [14]. These architectures can produce outstanding results in applications like cyber-physical systems security [12], [15]. Figure 5 presents various applications of DL for CPS. The deep architectures are formed of various hidden layers [4]. Deep Learning methods can represent additional abstract illustrations of information due to the multi-level architecture.

Deep Learning models have revealed better generalization competence in many practical applications than shallow ANNs.

There are some major fields where deep learning has been effectively applied in cyber-physical systems for security-related determinations such as detection of anomaly, detection of malware and threat hunting, susceptibility recognition, interruption detection, prevention of blackouts, assaults, and destructions in CPSs.

E. CYBER ATTACKS

In current years, there was a hike in the proportion of cyber attacks aiming cyber physical systems with distressing significances. As per recent studies [86], [97], cyber physical systems are susceptible to malicious code injection attacks [66] and code reuse attacks [76]in addition with false data injection attacks [77], zero-control data attacks [83]. These kinds of attacks can lead to black out targeting cyber physical system's industrial devices and systems as shown in Table 4.

V. OPEN ISSUES FOR SECURING CPS

There are several open issues and research directions related to securing Cyber Physical Systems (CPS) using Deep Learning (DL). Some of the key areas of focus include:

- **Data Collection and Preparation:** CPS typically generate vast amounts of data that are relevant to the security of the system [31], [55]. However, collecting and preparing this data for use in DL models can be challenging, particularly when the data is highly heterogeneous and distributed across multiple sources [105].
- **Model Selection and Development:** There is a need to identify the most appropriate DL models for securing CPS and to develop these models so that they can be effectively applied to real-world scenarios [106]. This includes choosing the right type of model, such as CNNs or RNNs, and optimizing the model's architecture and parameters to improve its performance.
- Integration with Other Security Measures: DL models need to be integrated with other sanctuary procedures to ensure that they are effective in detecting and mitigating cyber threats [107], [108]. This may include integrating DL models with intrusion detection systems, firewalls, or access control systems, or incorporating additional data sources such as log data or network traffic data to improve the accuracy of the models.
- **Scalability and Real-Time Processing:** CPS generate huge quantities of data in real-time, which makes it challenging to use DL models to detect and answer to cyber intimidations in real-time [109], [110]. There is a need for DL models that are able to scale to handle large amounts of data and that can be implemented in real-time to detect and reply to cyber intimidations in real-time.
- **Explainability and Trustworthiness:** One of the challenges of using DL models for security purposes is the lack of transparency and interpretability of the models. There is a need to develop DL models that are more transparent and interpretable, so that security experts and decision-makers can understand the basis for the models' predictions and decisions [55], [56].
- **Adversarial Robustness:** CPS are often targeted by sophisticated cyber-attackers who use techniques such as adversarial machine learning to evade detection. There is a need for DL models that are robust to these attacks and that can continue to operate effectively even in the presence of adversarial inputs [111].

These are some of the key areas of focus for securing CPS using DL, and there is a growing body of research aimed at addressing these challenges. By developing DL models that are effective in detecting and mitigating cyber threats, and by integrating these models with other security measures, it is possible to improve the sanctuary of CPS and reduce the risk of cyber-attacks.

A. RESEARCH DIRECTIONS IN SECURING CPS USING DL

There are several open issues and research directions for securing CPS using DL techniques. Some of these include:

- **Development of robust and accurate DL-based intrusion detection systems for CPS:** This involves the usage of DL methods such as CNNs and RNNs to detect and classify various types of cyber-attacks in CPS.
- **Improving the interpretability of DL-based CPS security models:** Currently, one of the main limitations of deep learning models is their absence of interpretability, making it hard to comprehend how they attain at their decisions. Research is needed to make DL models more transparent and interpretable [57].
- **Anomaly detection in CPS using unsupervised DL techniques:** Unsupervised DL techniques such as Autoencoders and Variational Autoencoders (VAEs) could be utilized to detect anomalies in CPS by learning the normal behavior of the system and identifying nonconformities from this normal behavior [112].
- **Adversarial attacks on DL-based CPS security models:** Adversarial attacks are a major concern in DL, and they pose a threat to the security of CPS systems. Research is needed to develop defense mechanisms against these attacks and to enhance the robustness of DL-based security models [113].
- **Integration of DL with other security techniques:** DL-based security models can be combined with other security techniques such as firewall, detection of intrusion and anticipation systems, and encryption to create a more comprehensive and effective security system for CPS [114].
- **Handling large and complex data in CPS using DL:** CPS systems generate large amounts of data, and this data is often complex and unstructured. Research is needed to develop DL models that can handle this data effectively and efficiently [58], [115].

TABLE 4. Different CPS system with different types of anamolies.

CPS System	Existing Work	Type of Anomalies								
		Attacks					Faults			
		DoS	MITM	Packet Injection	Malware	FALSE Control Signals	Sensor Layer	Network Layer	Control System	Manually Created
Industrial Control System	[37]	Yes	Yes	X	No	No	No	No	No	No
	[59]	No	Yes	No	No	Yes	No	No	No	No
	[60]	No	No	No	No	No	No	No	No	X
	[61]	No	No	No	No	No	Yes	No	No	No
	[62]	No	No	No	No	No	Yes	No	No	Yes
	[63]	No	Yes	No	No	Yes	No	No	No	No
	[64]	Yes	No	Yes	No	Yes	No	No	No	No
	[65]	No	Yes	No	No	Yes	No	No	No	No
	[66]	No	No	No	No	No	No	Yes	No	No
	[67]	No	No	No	No	No	Yes	No	No	No
	[68]	No	No	No	No	No	Yes	No	No	No
	[69]	No	No	No	No	No	Yes	No	No	Yes
	[70]	No	No	No	No	No	Yes	No	No	Yes
	[71]	No	No	No	Yes	No	Yes	No	No	Yes
	[72]	Yes	No	Yes	Yes	X	No	No	No	Yes
	[73]	No	No	Yes	No	No	No	No	No	
	[74]	No	Yes	No	No	Yes	No	No	No	No
Smart Grid and ITS	[75]	No	No	No	No	No	No	No	No	Yes
	[76]	Yes	X	Yes	Yes	Yes	No	No	No	Yes
	[77]	No	Yes	No	No	No	No	No	No	Yes
	[78]	No	Yes	No	No	No	No	No	No	Yes
	[79]	No	Yes	No	No	No	No	No	No	Yes
	[80]	No	Yes	No	No	No	No	No	No	Yes
	[81]	No	Yes	No	No	No	No	No	No	Yes
	[82]	No	No	No	No	No	Yes	No	No	No
	[83]	No	Yes	No	No	No	No	No	No	Yes
	[84]	No	No	No	No	No	No	No	No	No
	[85]	No	Yes	No	No	No	Yes	No	No	Yes
	[86]	No	No	Yes	No	Yes	No	No	No	Yes
	[20]	Yes	No	Yes	No	Yes	No	No	No	Yes
	[87]	No	No	Yes	No	No	X	No	No	Yes
	[88]	Yes	Yes	Yes	No	Yes	No	No	No	No
	[89]	No	Yes	Yes	No	No	No	No	No	Yes
Aerial System	[90]	No	No	No	No	Yes	No	No	No	No
	[91]	No	No	No	No	Yes	No	No	No	No
	[92]	No	No	X	Yes	No	No	No	No	No
	[93]	No	No	No	No	No	No	Yes	No	No
	[94]	No	No	No	No	No	No	No	Yes	Yes
	[95]	No	No	No	No	No	No	No	No	Yes
	[96]	No	No	No	No	No	No	No	No	Yes

Note*: X belongs to Not Clear but inferred to be Yes

VI. CHALLENGES AND FUTURE SCOPE

The major potential fields are shown in the figure where the research areas may arise. The seven steps of the research methodology are already shown in the figure. The research literature can be improvised with our research methodology, and with the help of this, the comparative analysis can be done appropriately. The further challenges can be categorized into different directions, which are:

A. THE NEW SCENARIOS OF CYBER-PHYSICAL SYSTEM'S CYBERSECURITY

The various articles analyzed communication networks in the scenarios of cyber-physical systems [25], [103]. Most of the survey papers have examined the methods of cyber-physical systems in the intelligent grids or the water treatments of plants described in the 13/27 survey papers. It is the emergent way to apply deep learning in the current industry. Deep Learning is used for detecting the faults and defects in the industrial sector of complex items [97]. But these were not considered as there were no issues of cyber security covered in this. The cyber-attacks and threats usually exist in the cloud server where design models are stored. We suggest that the blockchain will be analyzed more in a broader way in collaboration with cyber-physical systems, and the variety and development of cyber-physical systems scenarios will lead to intense analysis of cyber security [116], [117], [118].

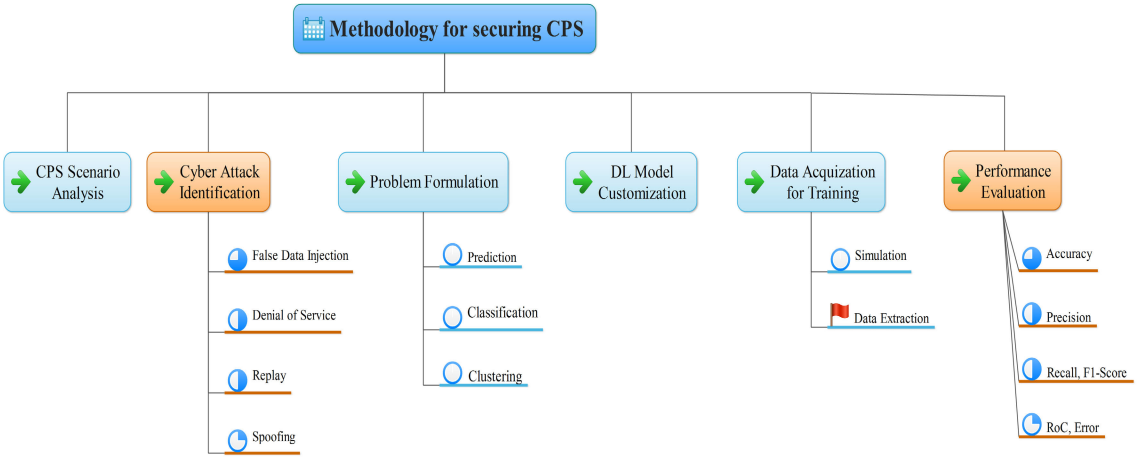

FIGURE 7. The deep learning driven methodology for security of cyber physical systems.

TABLE 5. Real cyber physical systems attacks.

Country	Nature of Attack	Type	Target	Motives	Date
USA	Slammer Worm Sensors Failure	Malware-DoS Accident	Ohio Nuke Plant Network [98] Taum Sauk Hydroelectric Failure of Power Station [99]	Criminal N/A	Jan 25,2003 14 Dec 2005
	Installed Software Update	Undefined Software	Georgia Nuclear Power Shutdown of Plant [100]	Unclear	Mar 7, 2008
	Reconnaissance	Undefined Software Programs	US Electricity Grid [101]	Political	Apr 8, 2009
	Backdoor	Unauthorised Access	Springfield Pumping Station [97]	Criminal	Nov 8, 2011
	Physical Breach	Unauthorised Access	Georgia Water Treatment Plant [102]	Criminal	Apr 26, 2013
Iran	Stuxnet [103]	Worm	Iranian nuclear facilities	Political	Nov,2007
	Stuxnet-2	worm	power plant and another industry	Political	25 Dec 2012
	DDoS	Disruptive	Iranian Infrastructure and communications companies	Political	03 Oct 2012
	Computer Virus	Malware	Iranian key oil facilities	Political	23 Apr 2012
Saudi Arabia	Shamoon-1	Malware	Saudi infrastructure in the energy industry	Religio-Political	15 Aug 2012
	Shamoon-2	Malware	Saudi government computers and targets	Religio-Political	17 Nov 2016
	Shamoon-3	Malware	Tasnee and other petrochemical firms, National Industrialization Company, Sadara Chemical Company	Religio-Political	23 Jan 2017
Qatar	Shamoon	Malware	Qatar's RasGas	Political	30 Aug 2012
United Arab Emirates	Trojan Laziok	Malware	UAE energy sector	Political	Jan-Feb 2015
Australia	Remote Access	Unauthorised Access	Maroochy Water Breach [73]	Criminal	March, 2000
Canada	Security Breach	Exploited Vulnerability	Telvent Company [104]	Criminal	Sept 10, 2012

B. IDENTIFYING CYBER ATTACKS

Most of the survey papers have analyzed the false data injection attacks. Recognizing surreptitious untruthful data injection attacks is challenging as a considerable amount of noise is being formed in the cyber-physical systems, and there is a deficiency in the mechanisms of cyber security for authenticating the devices and messages which are transmitted over the network. Some categories of false injection attacks depend on the information of invaders [119], [120]. As no such advanced information is needed to initiate a denial of services attacks, individually logged packets are required for replay attacks, scanned tools for penetrating attacks, and automated tools for fuzzy attacks. However, the cyber security of cyber-physical systems is a vast area compared to cyber-attacks in contradiction to cyber-physical systems. Detection of cyber-attacks that are initiated in cyberspace and infiltrate the physical domain is a challenging task [22], [121]. We assume that emergent cyber-attacks will head the defense devices, but the risk could be moderated via the data-driven approach.

C. ACCEPTING NEW PARADIGMS OF MACHINE LEARNING/DEEP LEARNING

Usually, all analyzed papers follow conventional machine learning standards, includes supervised and unsupervised learning. Around 4 papers inspected problems of regression, 3 papers are related to problems of clustering, and others are based on problems of classification. The directing usage of supervised learning reflects the value of using well-labeled data [21], [122], [123]. Particularly, network packets were labeled as usual or attack traffic, and the kinds of attacks were distinguished. This dependence on labeled data is limited to the broader acceptance of machine learning or deep learning methods. We suggest that the researchers and authors use new machine learning/deep learning paradigms [124]. It includes reinforcement and self-supervised learning to improve the explainability of the model. We suggest self-supervised learning flourishes in the cyber-physical system's domain as deep learning models suffer from deprived explainability. We are expectant about predicting that the deep learning models will be further reasonable when new tools and techniques are conceived and utilized [125].

D. PROTECTING THE TRAINED DEEP LEARNING MODELS

No survey papers are measured for defending the trained deep learning models, contrary to numerous attacks. In contrast, we highlight the significance of protecting the trained deep learning models due to the computational expenditures for introducing the deep learning models [126], [127]. The attackers can acquire adequate data to imitate a machine learning/deep learning model by generating many inquiries and conglomerating the outcomes. The removed data can be utilized to construct a mirroring model for the assailant to find conceivable avoidance assaults. We emphatically advocate that cyber defense be led quickly because of the ignorance of adversarial assaults in the cyber physical systems situations.

E. ADVANCING DATASETS OF CYBER PHYSICAL SYSTEMS CYBERSECURITY

Between the reviewed papers, datasets gathered in the area ruled the simulation with a proportion of 14:6. Simulated information was explored in the 2 cyber physical systems situations – shrewd matrices and vehicular organizations [128]. Five papers utilizing field information picked the Smack dataset, two reports the CICIDS2017 dataset, and the other diverse datasets [129], [130], [131].

Additionally, new datasets will constantly be essential and appreciated. In a perfect world, the new datasets are publicly released field information gathered from physical testbeds. A few cyber physical system testbeds are proposed to work with recognizing cyber assaults [24].The new pattern of expanding interest in building cyber physical system testbeds may help specialists to gather superior-grade assault and defense information [132], [133]. The new datasets are enormous enough to take advantage of deep learning models' power, and both new and old cyber assaults should be incorporated because cyber assaults advance rapidly. If naming information is tested, sequentially isolating the assaults from the typical traffic is a practical thought. Falsely mixing the information passages addressing assaults into a bunch of ordinary traffic records should be kept away from because the basic information increase strategy doesn't consider practicality, going after groupings, and potential connections changes. To help the headway of exploration and information, we emphatically energize more high-quality datasets increasingly to be made accessible to the local area [134], [135].

F. IMPROVISING THE EVALUATION OF MODELS

Standard execution measurements were utilized in the vast majority of the reviewed papers. Misleading up-sides were examined, precision and fault rate. This is demonstrated by authors [65] that it is fundamentally further hard to distinguish the seldom-happened assaults than the normal ones determined by the Bayesian regulations [136], [137].

Moreover, time is essential in ongoing investigations since each prepared machine learning or deep learning model's presentation will unavoidably corrupt over the long run. When the cyber develops quickly, the models prepared with old information will battle with identifying new assaults. A period rot metric was proposed in to assess a prepared model's presentation misfortune. By concentrating on the time rot, we will want to choose when the model should be retrained. We want to see future work like about cyber physical systems and cyber assaults. When top-to-bottom information is created and acquired, we might hope to relieve the risk of cyber-physical systems' cyber assaults.

VII. CONCLUSION

This review gives an ongoing perspective on recognizing cyber-attacks in the cyber physical systems.In particular, an inclusive perception is obtained through analyzing the cyber-physical systems situations, recognizing cybersecurity issues, interpreting the exploration issue to the machine learning/deep learning space, developing the deep learning model, planning datasets, and lastly, assessing the model. The Cyber attacks endure as a constant and conspicuous danger to the safety and betterment of cyber-physical systems. The work shows extraordinary potential to take advantage of cyber physical system's cyber information through deep learning models as a result of their promising demonstrations. We distinguished favorable examination issues, incorporating blockchain, identifying cutting-edge, steady dangers, taking on new machine learning and deep learning standards, avoiding adversarial and attacks of model extraction, enhancing datasets, and utilizing different execution measurements. We are hopeful and sure that the examination in this field will thrive.

REFERENCES

[1] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," Secur. Response, Symantec Corp., Cupertino, CA, USA, White Paper, Version 1.4, Feb. 2011, p. 29, vol. 5, no. 6.

[2] A. Humayed and B. Luo, "Cyber-physical security for smart cars: Taxonomy of vulnerabilities, threats, and attacks," in *Proc. ACM/IEEE 6th Int. Conf. Cyber-Phys. Syst.*, Seattle, WA, USA, Apr. 2015, pp. 252–253.

[3] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in *Proc. Int. Conf. Crit. Infrastruct. Protection*. Boston, MA, USA: Springer, 2007, pp. 73–82.

[4] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[5] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, Feb. 2011.

[6] C.-H. Lee, B.-K. Chen, N.-M. Chen, and C.-W. Liu, "Lessons learned from the blackout accident at a nuclear power plant in Taiwan," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2726–2733, Oct. 2010.

[7] J. P. Conti, "The day the samba stopped [power blackouts]," *Eng. Technol.*, vol. 5, no. 4, pp. 46–47, Mar. 2010.

[8] Y. Liu and S. Hu, "Cyberthreat analysis and detection for energy theft in social networking of smart homes," *IEEE Trans. Computat. Social Syst.*, vol. 2, no. 4, pp. 148–158, Dec. 2015.

[9] Y. Liu and S. Hu, "Smart home scheduling and cybersecurity: Fundamentals," in *Smart Cities and Homes*. Amsterdam, The Netherlands: Elsevier, 2016, pp. 191–217.

[10] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[11] S. Li, Y. Yilmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.

[12] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[13] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Inform.*, vol. 13, no. 2, pp. 411–423, Sep. 2016.

[14] K. Paridari, N. O'Mahony, A. E.-D. Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg, "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration," *Proc. IEEE*, vol. 106, no. 1, pp. 113–128, Jan. 2018.

[15] A.-Y. Lu and G.-H. Yang, "Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer," *Inf. Sci.*, vol. 417, pp. 454–464, Nov. 2017.

[16] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[17] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, and G. Ferrari-Trecate, "Distributed cyber-attack detection in the secondary control of DC microgrids," in *Proc. Eur. Control Conf. (ECC)*, Limassol, Cyprus, Jun. 2018, pp. 344–349.

[18] S. Altaf, A. Al-Anbuky, and H. GholamHosseini, "Fault diagnosis in a distributed motor network using artificial neural network," in *Proc. Int. Symp. Power Electron., Electr. Drives, Autom. Motion*, Ischia, Italy, Jun. 2014, pp. 190–197.

[19] B. M. Sanandaji, E. Bitar, K. Poolla, and T. L. Vincent, "An abrupt change detection heuristic with applications to cyber data attacks on power systems," in *Proc. Amer. Control Conf.*, Portland, OR, USA, Jun. 2014, pp. 5056–5061.

[20] M. Russo, M. Labonne, A. Olivereau, and M. Rmayti, "Anomaly detection in Vehicle-to-Infrastructure communications," in *Proc. IEEE 87th Veh. Technol. Conf. (VTC Spring)*, Porto, Portugal, Jun. 2018, pp. 1–6.

[21] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[22] D. Xiong, D. Zhang, X. Zhao, and Y. Zhao, "Deep learning for EMG-based human-machine interaction: A review," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 3, pp. 512–533, Mar. 2021.

[23] L. Kuwatly, M. Sraj, Z. Al Masri, and H. Artail, "A dynamic honeypot design for intrusion detection," in *Proc. IEEE/ACS Int. Conf. Pervasive Services (ICPS)*, Beirut, Lebanon, Jul. 2004, pp. 95–104.

[24] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, pp. 1–29, Apr. 2014.

[25] C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe, and M. Manic, "Generalization of deep learning for cyber-physical system security: A survey," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2018, pp. 745–751.

[26] S. Gaba, H. Khan, K. J. Almalki, A. Jabbari, I. Budhiraja, V. Kumar, A. Singh, K. K. Singh, S. S. Askar, and M. Abouhawwash, "Holochain: An agent-centric distributed hash table security in smart IoT applications," *IEEE Access*, vol. 11, pp. 81205–81223, 2023.

[27] A. Barnawi, S. Gaba, A. Alphy, A. Jabbari, I. Budhiraja, V. Kumar, and N. Kumar, "A systematic analysis of deep learning methods and potential attacks in Internet-of-things surfaces," *Neural Comput. Appl.*, vol. 35, no. 25, pp. 18293–18308, Sep. 2023.

[28] H. Sharma, N. Kumar, I. Budhiraja, and A. Barnawi, "Secrecy rate maximization in THz-aided heterogeneous networks: A deep reinforcement learning approach," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13490–13505, Oct. 2023.

[29] V. Vishnoi, P. Consul, I. Budhiraja, S. Gupta, and N. Kumar, "Deep reinforcement learning based energy consumption minimization for intelligent reflecting surfaces assisted D2D users underlaying UAV network," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2023, pp. 1–6.

[30] V. Vishnoi, I. Budhiraja, S. Ishan, and N. Kumar, "A deep reinforcement learning scheme for sum rate and fairness maximization among D2D pairs underlaying cellular network with NOMA," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13506–13522, 2023, doi: 10.1109/TVT.2023.3276647.

[31] S. Singh, A. Bhardwaj, I. Budhiraja, U. Gupta, and I. Gupta, "Cloud-based architecture for effective surveillance and diagnosis of COVID-19," in *Convergence of Cloud With AI for Big Data Analytics: Foundations and Innovation*. Hoboken, NJ, USA: Wiley, 2023, pp. 69–88.

[32] L. Cheng, K. Tian, and D. Yao, "Orpheus: Enforcing cyber-physical execution semantics to defend against data-oriented attacks," in *Proc. 33rd Annu. Comput. Secur. Appl. Conf.*, Orlando, FL, USA, Dec. 2017, pp. 315–326.

[33] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," 2019, *arXiv:1901.03407*.

[34] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. R. J. Fontaine, A. Filippoupolitis, and E. Roesch, "A taxonomy of cyber-physical threats and impact in the smart home," *Comput. Secur.*, vol. 78, pp. 398–428, Sep. 2018.

[35] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, 2009.

[36] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, Jul. 2019.

[37] P. Schneider and K. Böttinger, "High-performance unsupervised anomaly detection for cyber-physical system networks," in *Proc. Workshop Cyber-Phys. Syst. Secur. PrivaCy*, Jan. 2018, pp. 1–12.

[38] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2923–2960, 4th Quart., 2018.

[39] E. M. Veith, L. Fischer, M. Tröschel, and A. Nieße, "Analyzing cyber-physical systems from the perspective of artificial intelligence," in *Proc. Int. Conf. Artif. Intell., Robot. Control*, Dec. 2019, pp. 85–95.

[40] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Comput. Surv.*, vol. 54, no. 5, pp. 1–36, Jun. 2022.

[41] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surveys*, vol. 46, no. 4, pp. 1–29, Apr. 2014.

[42] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," *Comput. Secur.*, vol. 70, pp. 436–454, Sep. 2017.

[43] B. Siciliano, A. G. Scaglione, and L. Galluccio, "A survey of cyber-physical attacks and defenses in the smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3231–3240, Jun. 2020.

[44] I. Ndiaye, J. G. Nijlla, and I. Balogun, "A survey of intrusion detection in Internet of Things," *IEEE Access*, vol. 9, pp. 73900–73917, 2021.

[45] L. Yu, H. Wu, Z. Liu, Y. Li, and W. Zhao, "A review of machine learning methods in cybersecurity," *IEEE Access*, vol. 8, pp. 135695–135718, 2020.
[46] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022.
[47] A. A. Jamal, A.-A. M. Majid, A. Konev, T. Kosachenko, and A. Shelupanov, "A review on security analysis of cyber physical systems using machine learning," *Mater. Today*, vol. 80, pp. 2302–2306, Jan. 2023.
[48] F. O. Olowononi, D. B. Rawat, and C. Liu, "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 524–552, 1st Quart., 2021.
[49] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Comput. Surv.*, vol. 54, no. 5, pp. 1–36, Jun. 2022.
[50] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.
[51] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4007–4020, 2023, doi: 10.1109/TSG.2023.3237011.
[52] F. Darbandi, A. Jafari, H. Karimipour, A. Dehghantanha, F. Derakhshan, and K. Raymond Choo, "Real-time stability assessment in smart cyber-physical grids: A deep learning approach," *IET Smart Grid*, vol. 3, no. 4, pp. 454–461, Aug. 2020.
[53] S. Rathore and J. H. Park, "A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5522–5532, Aug. 2021.
[54] B. Hussain, Q. Du, B. Sun, and Z. Han, "Deep learning-based DDoS-attack detection for cyber–physical system over 5G network," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 860–870, Feb. 2021.
[55] A. M. Aslam, R. Chaudhary, A. Bhardwaj, I. Budhiraja, N. Kumar, and S. Zeadally, "Metaverse for 6G and beyond: The next revolution and deployment challenges," *IEEE Internet Things Mag.*, vol. 6, no. 1, pp. 32–39, Mar. 2023.
[56] M. Gupta, B. Gupta, A. Jabbari, I. Budhiraja, D. Garg, K. Kotecha, and C. Iwendi, "A novel computer assisted genomic test method to detect breast cancer in reduced cost and time using ensemble technique," *Human-Centric Comput. Inf. Sci.*, vol. 13, no. 18, pp. 1–16, Feb. 2023, doi: 10.22967/HCIS.2023.13.008.
[57] A. Bhardwaj, I. Budhiraja, and U. Gupta, *Cloud-Based Architecture for Effective Surveillance and Diagnosis of COVID-19*. Hoboken, NJ, USA: Wiley, 2023.
[58] A. Bhardwaj, U. Gupta, I. Budhiraja, and R. Chaudhary, "Container-based migration technique for fog computing architecture," in *Proc. Int. Conf. Adv. Technol. (ICONAT)*, Jan. 2023, pp. 1–6.
[59] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," in *Proc. Workshop Cyber-Phys. Syst. Secur. PrivaCy*, Jan. 2018, pp. 72–83.
[60] Z. Zohrevand, U. Glässer, M. A. Tayebi, H. Y. Shahir, M. Shirmaleki, and A. Y. Shahir, "Deep learning based forecasting of critical infrastructure data," in *Proc. ACM Conf. Inf. Knowl. Manage.*, Singapore, Nov. 2017, pp. 1129–1138.
[61] Y. Su, Y. Zhao, C. Niu, R. Liu, W. Sun, and D. Pei, "Robust anomaly detection for multivariate time series through stochastic recurrent neural network," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, New York, NY, USA, Jul. 2019, pp. 2828–2837.
[62] B. Eiteneuer, N. Hranisavljevic, and O. Niggemann, "Dimensionality reduction and anomaly detection for CPPS data using autoencoder," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Melbourne, VIC, Australia, Feb. 2019, pp. 1286–1292.
[63] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng. (HASE)*, Singapore, Jan. 2017, pp. 140–145.
[64] C. Feng, T. Li, and D. Chana, "Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Singapore, Jun. 2017, pp. 261–272.
[65] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, and J. Sun, "Anomaly detection for a water treatment system using unsupervised machine learning," in *Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW)*, New Orleans, LA, USA, Nov. 2017, pp. 1058–1065.
[66] P. Ferrari, S. Rinaldi, E. Sisinni, F. Colombo, F. Ghelfi, D. Maffei, and M. Malara, "Performance evaluation of full-cloud and edge-cloud architectures for industrial IoT anomaly detection based on deep learning," in *Proc. II Workshop Metrol. Ind. IoT (MetroInd&IoT)*, Jun. 2019, pp. 420–425.
[67] A. Legrand, B. Niepceron, A. Cournier, and H. Trannois, "Study of autoencoder neural networks for anomaly detection in connected buildings," in *Proc. IEEE Global Conf. Internet Things (GCIoT)*, Naples, Italy, Dec. 2018, pp. 1–5.
[68] Z. Wu, Y. Guo, W. Lin, S. Yu, and Y. Ji, "A weighted deep representation learning model for imbalanced fault diagnosis in cyber-physical systems," *Sensors*, vol. 18, no. 4, p. 1096, Apr. 2018.
[69] Z. Li, J. Li, Y. Wang, and K. Wang, "A deep learning approach for anomaly detection based on SAE and LSTM in mechanical equipment," *Int. J. Adv. Manuf. Technol.*, vol. 103, nos. 1–4, pp. 499–510, Jul. 2019.
[70] B. Lindemann, F. Fesenmayr, N. Jazdi, and M. Weyrich, "Anomaly detection in discrete manufacturing using self-learning approaches," *Proc. CIRP*, vol. 79, pp. 313–318, Jan. 2019.
[71] M. Canizo, I. Triguero, A. Conde, and E. Onieva, "Multi-head CNN–RNN for multi-time series anomaly detection: An industrial case study," *Neurocomputing*, vol. 363, pp. 246–260, Oct. 2019.
[72] H. A. Khan, N. Sehatbakhsh, L. N. Nguyen, M. Prvulovic, and A. Zajić, "Malware detection in embedded systems using neural network model for electromagnetic side-channel signals," *J. Hardw. Syst. Secur.*, vol. 3, no. 4, pp. 305–318, Dec. 2019.
[73] Y.-J. Xiao, W.-Y. Xu, Z.-H. Jia, Z.-R. Ma, and D.-L. Qi, "NIPAD: A non-invasive power-based anomaly detection scheme for programmable logic controllers," *Frontiers Inf. Technol. Electron. Eng.*, vol. 18, no. 4, pp. 519–534, Apr. 2017.
[74] D. Li, D. Chen, B. Jin, L. Shi, J. Goh, and S.-K. Ng, "Mad-GAN: Multivariate anomaly detection for time series data with generative adversarial networks," in *Proc. Int. Conf. Artif. Neural Netw.*, Springer, 2019, pp. 703–716.
[75] N. L. Tasfi, W. A. Higashino, K. Grolinger, and M. A. M. Capretz, "Deep neural networks with confidence sampling for electrical anomaly detection," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jun. 2017, pp. 1038–1045.
[76] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, "Cyber physical security analytics for transactive energy systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 931–941, Mar. 2020.
[77] J. Wang, D. Shi, Y. Li, J. Chen, H. Ding, and X. Duan, "Distributed framework for detecting PMU data manipulation attacks with deep autoencoders," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4401–4410, Jul. 2019.
[78] Q. Deng and J. Sun, "False data injection attack detection in a power grid using RNN," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Washington, DC, USA, Oct. 2018, pp. 5983–5988.
[79] X. Niu, J. Li, J. Sun, and K. Tomsovic, "Dynamic detection of false data injection attack in smart grid using deep learning," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2019, pp. 1–6.
[80] H. Wang, J. Ruan, Z. Ma, B. Zhou, X. Fu, and G. Cao, "Deep learning aided interval state prediction for improving cyber security in energy Internet," *Energy*, vol. 174, pp. 1292–1304, May 2019.
[81] S. Basumallik, R. Ma, and S. Eftekharnejad, "Packet-data anomaly detection in PMU-based state estimator using convolutional neural network," *Int. J. Electr. Power Energy Syst.*, vol. 107, pp. 690–702, May 2019.
[82] C. Fan, F. Xiao, Y. Zhao, and J. Wang, "Analytical investigation of autoencoder-based methods for unsupervised anomaly detection in building energy data," *Appl. Energy*, vol. 211, pp. 1123–1135, Feb. 2018.
[83] Y. Wang, D. Chen, C. Zhang, X. Chen, B. Huang, and X. Cheng, "Wide and recurrent neural networks for detection of false data injection in smart grids," in *Proc. 14th Int. Conf., Wireless Algorithms, Syst., Appl. (WASA)*. Honolulu, HI, USA: Springer, 2019, pp. 335–345.

[84] E. Khanapuri, T. Chintalapati, R. Sharma, and R. Gerdes, "Learning-based adversarial agent detection and identification in cyber physical systems applied to autonomous vehicular platoon," in *Proc. IEEE/ACM 5th Int. Workshop Softw. Eng. Smart Cyber-Phys. Syst. (SEsCPS)*, Montreal, QC, Canada, May 2019, pp. 39–45.

[85] F. van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 1264–1276, Mar. 2020.

[86] A. Taylor, S. Leblanc, and N. Japkowicz, "Anomaly detection in automobile control network data with long short-term memory networks," in *Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA)*, Montreal, QC, Canada, Oct. 2016, pp. 130–139.

[87] T. Kieu, B. Yang, and C. S. Jensen, "Outlier detection for multidimensional time series using deep neural networks," in *Proc. 19th IEEE Int. Conf. Mobile Data Manage. (MDM)*, Aalborg, Denmark, Jun. 2018, pp. 125–134.

[88] K. Zhu, Z. Chen, Y. Peng, and L. Zhang, "Mobile edge assisted literal multi-dimensional anomaly detection of in-vehicle network using LSTM," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4275–4284, May 2019.

[89] C. Jichici, B. Groza, and P.-S. Murvay, "Examining the use of neural networks for intrusion detection in controller area networks," in *Proc. Int. Conf. Secur. Inf. Technol. Commun.*, Springer, 2018, pp. 109–125.

[90] K. Hundman, V. Constantinou, C. Laporte, I. Colwell, and T. Soderstrom, "Detecting spacecraft anomalies using LSTMs and nonparametric dynamic thresholding," in *Proc. 24th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, London, U.K., Jul. 2018, pp. 387–395.

[91] S. Tariq, S. Lee, Y. Shin, M. S. Lee, O. Jung, D. Chung, and S. S. Woo, "Detecting anomalies in space using multivariate convolutional LSTM with mixtures of probabilistic PCA," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Anchorage, AK, USA, Jul. 2019, pp. 2123–2133.

[92] O. M. Ezeme, Q. H. Mahmoud, and A. Azim, "DReAM: Deep recursive attentive model for anomaly detection in kernel events," *IEEE Access*, vol. 7, pp. 18860–18870, 2019.

[93] L. Gunn, P. Smet, E. Arbon, and M. D. McDonnell, "Anomaly detection in satellite communications systems using LSTM networks," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Canberra, ACT, Australia, Nov. 2018, pp. 1–6.

[94] A. Nanduri and L. Sherry, "Anomaly detection in aircraft data using recurrent neural networks (RNN)," in *Proc. Integr. Commun. Navigat. Surveill. (ICNS)*, Herndon, VA, USA, Apr. 2016, p. 5C2-1.

[95] E. Habler and A. Shabtai, "Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages," *Comput. Secur.*, vol. 78, pp. 155–173, Sep. 2018.

[96] O. M. Ezeme, M. Lescisin, Q. H. Mahmoud, and A. Azim, "DeepAnom: An ensemble deep framework for anomaly detection in system processes," in *Proc. 32nd Can. Conf. Artif. Intell., Adv. Artif. Intell. (Canadian AI)*. Kingston, ON, Canada: Springer, May 2019, pp. 549–555.

[97] V. L. Do, L. Fillatre, I. Nikiforov, and P. Willett, "Security of SCADA systems against cyber–physical attacks," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 5, pp. 28–45, May 2017.

[98] K. Poulsen, "Slammer worm crashed Ohio nuke plant network," *Secur. Focus*, vol. 19, 2003.

[99] J. D. Rogers and C. M. Watkins, "Overview of the Taum Sauk pumped storage power plant upper reservoir failure, Reynolds County, MO," in *Proc. 6th Int. Conf. Case Histories Geotechnical Eng.*, Arlington, VA, USA, 2008, pp. 1–13.

[100] T. FoxBrewster, "Ukraine claims hackers caused Christmas power outage," *Forbes Secur.*, 2016.

[101] S. Gorman, "Electricity grid in us penetrated by spies," *Wall Street J.*, vol. 8, no. 8, 2009.

[102] M. J. Credeur, "FBI probes Georgia water plant break-in on terror concern," Bloomberg, 2013.

[103] J. Slay and M. Miller, *Lessons Learned From the Maroochy Water Breach*. Boston, MA, USA: Springer, 2008.

[104] F. Y. Rashid. (2012). *Telvent Hit by Sophisticated Cyber-Attack, SCADA Admin Tool Compromised*. [Online]. Available: http://www.securityweek.com/telvent-hit-sophisticated-cyber-attack-scada-admin-tool-compromised

[105] M. A. Almaiah, F. Hajjej, A. Ali, M. F. Pasha, and O. Almomani, "A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS," *Sensors*, vol. 22, no. 4, p. 1448, Feb. 2022.

[106] R. F. Mansour, "Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment," *Sci. Rep.*, vol. 12, no. 1, p. 12937, Jul. 2022.

[107] Z. A. Sheikh, Y. Singh, P. K. Singh, and K. Z. Ghafoor, "Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope," *Comput. Commun.*, vol. 193, pp. 302–331, Sep. 2022.

[108] D. M. Sharma and S. K. Shandilya, "Attack detection based on machine learning techniques to safe and secure for CPS—A review," in *Proc. Int. Conf. IoT, Intell. Comput. Secur., Select (IICS)*, pp. 273–286, Springer, 2023.

[109] A. Albasir, K. Naik, and R. Manzano, "Toward improving the security of IoT and CPS devices: An AI approach," *Digit. Threats: Res. Pract.*, vol. 4, no. 2, pp. 1–30, Jun. 2023.

[110] G. Epiphaniou, M. Hammoudeh, H. Yuan, C. Maple, and U. Ani, "Digital twins in cyber effects modelling of IoT/CPS points of low resilience," *Simul. Model. Pract. Theory*, vol. 125, May 2023, Art. no. 102744.

[111] A. Albasir, K. Naik, and R. Manzano, "Toward improving the security of IoT and CPS devices: An AI approach," *Digit. Threats, Res. Pract.*, vol. 4, no. 2, pp. 1–30, Jun. 2023.

[112] A. Aggarwal, S. Gaba, S. Nagpal, and A. Arya, "A comparative analysis among task scheduling for grouped and ungrouped grid application," in *Proc. CEUR Workshop, Int. Conf. Emerg. Technol., AI, IoT, CPS Sci. Technol. Appl.* Chandigarh, India: NITTTR, Sep. 2021, pp. 1–5.

[113] A. Aggarwal, S. Gaba, S. Nagpal, and B. Vig, "Bio-inspired routing in VANET," in *Cloud and IoT-Based Vehicular Ad Hoc Networks*, 2021, pp. 199–220.

[114] D. Aggarwal and S. Gaba, "A comparative study: Reviewing performance of routing protocols in mobile ad-hoc network," *Vol*, vol. 4, no. 8, pp. 528–532, Jun. 2018.

[115] I. Budhiraja et al., "A comprehensive review on variants of SARS-CoVs-2: Challenges, solutions and open issues," *Comput. Commun.*, vol. 197, pp. 34–51, 2023.

[116] H. Khan, I. Budhiraja, S. A. Wahaj, M. Z. Alam, S. T. Siddiqui, and M. I. Alam, "IoT and blockchain integration challenges," in *Proc. IEEE Int. Conf. Current Develop. Eng. Technol. (CCET)*, Dec. 2022, pp. 1–5.

[117] P. Rani, V. Kumar, I. Budhiraja, A. Rathi, and S. Kukreja, "Deploying electronic voting system use-case on Ethereum public blockchain," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2022, pp. 1–6.

[118] P. Consul, I. Budhiraja, R. Chaudhary, and D. Garg, "FLBCPS: Federated learning based secured computation offloading in blockchain-assisted cyber-physical systems," in *Proc. IEEE/ACM 15th Int. Conf. Utility Cloud Comput. (UCC)*, Dec. 2022, pp. 412–417.

[119] R. Nijhawan, M. Juneja, N. Kaur, A. Yadav, and I. Budhiraja, "Automated deep learning based approach for albinism detection," in *Proc. Int. Conf. Recent Trends Image Process. Pattern Recognit.* Kingsvilla, TX, USA: Springer, 2022, pp. 272–281.

[120] A. Aggarwal, S. Gaba, S. Chawla, and A. Arya, "Recognition of alphanumeric patterns using backpropagation algorithm for design and implementation with ANN," *Int. J. Secur. Privacy Pervasive Comput.*, vol. 14, no. 1, pp. 1–11, Feb. 2022.

[121] S. Gaba, A. Aggarwal, and S. Nagpal, "Role of machine learning for ad hoc networks," in *Cloud and IoT-Based Vehicular Ad Hoc Networks*. Hoboken, NJ, USA: Wiley, 2021, pp. 269–291.

[122] A. Aggarwal, S. Gaba, J. Kumar, and S. Nagpal, "Blockchain and autonomous vehicles: Architecture, security and challenges," in *Proc. 5th Int. Conf. Comput. Intell. Commun. Technol. (CCICT)*, Jul. 2022, pp. 332–338.

[123] S. Gaba, S. Nagpal, and A. Aggarwal, "A comparative study of convolutional neural networks for plant phenology recognition," in *Advanced Sensing in Image Processing and IoT*. Boca Raton, FL, USA: CRC Press, 2022, pp. 109–136.

[124] A. Barnawi, I. Budhiraja, K. Kumar, N. Kumar, B. Alzahrani, A. Almansour, and A. Noor, "A comprehensive review on landmine detection using deep learning techniques in 5G environment: Open issues and challenges," *Neural Comput. Appl.*, vol. 34, no. 24, pp. 21657–21676, Dec. 2022.

[125] S. Gaba, D. Kumar, S. Nagpal, and A. Aggarwal, "A quick analysis on cyber physical systems for sustainable development," *Grenze Int. J. Eng. Technol.*, vol. 8, no. 1, pp. 621–627, 2022.

[126] P. Consul, I. Budhiraja, R. Chaudhary, and N. Kumar, "Security reassessing in UAV-assisted cyber-physical systems based on federated learning," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2022, pp. 61–65.
[127] A. Verma, P. Bhattacharya, I. Budhiraja, A. K. Gupta, and S. Tanwar, "Fusion of federated learning and 6G in internet-of-medical-things: Architecture, case study and emerging directions," in *Proc. 4th Int. Conf. Futuristic Trends Netw. Comput. Technol.* Ahmedabad, India: Springer, Jul. 2022, pp. 229–242.
[128] P. Arpaia, C. Manna, and G. Montenero, "Ant-search strategy based on likelihood trail intensity modification for multiple-fault diagnosis in sensor networks," *IEEE Sensors J.*, vol. 13, no. 1, pp. 148–158, Jan. 2013.
[129] I. Budhiraja, N. Kumar, H. Sharma, M. Elhoseny, Y. Lakys, and J. J. P. C. Rodrigues, "Latency-energy tradeoff in connected autonomous vehicles: A deep reinforcement learning scheme," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 11, pp. 13296–13308, 2023, doi: 10.1109/TITS.2022.3215523.
[130] A. Barnawi, N. Kumar, I. Budhiraja, K. Kumar, A. Almansour, and B. Alzahrani, "Deep reinforcement learning based trajectory optimization for magnetometer-mounted UAV to landmine detection," *Comput. Commun.*, vol. 195, pp. 441–450, Nov. 2022.
[131] Deepanshi, I. Budhiraja, D. Garg, N. Kumar, and R. Sharma, "A comprehensive review on variants of SARS-CoVs-2: Challenges, solutions and open issues," *Comput. Commun.*, vol. 197, pp. 34–51, Jan. 2023.
[132] S. Gaba, S. Nagpal, A. Aggarwal, S. Kumar, and P. Singh, "A modified approach for accuracy enhancement in intruder detection with optimally certain features," in *Proc. 3rd Mobile Radio Commun. 5G Netw. (MRCN)*. Kurukshetra, India: Springer, 2023, pp. 149–157.
[133] S. Gaba, I. Buddhiraja, V. Kumar, and A. Makkar, "Federated learning based secured computational offloading in cyber-physical IoST systems," in *Proc. Int. Conf. Recent Trends Image Process. Pattern Recognit.* Kingsvilla, TX, USA: Springer, 2022, pp. 344–355.
[134] S. Gaba, S. Nagpal, A. Aggarwal, R. Kumar, and S. Kumar, "An analysis of Internet of Things (IoT) malwares and detection based on static and dynamic techniques," in *Proc. 7th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC)*, Nov. 2022, pp. 24–29.
[135] P. Singh, G. Bathla, D. Panwar, A. Aggarwal, and S. Gaba, "Performance evaluation of genetic algorithm and flower pollination algorithm for scheduling tasks in cloud computing," in *Proc. Int. Conf. Signal Process. Integr. Netw.* Noida, India: Springer, 2022, pp. 139–154.
[136] H. Sharma, I. Budhiraja, P. Consul, N. Kumar, D. Garg, L. Zhao, and L. Liu, "Federated learning based energy efficient scheme for MEC with NOMA underlaying UAV," in *Proc. 5th Int. ACM Mobicom Workshop Drone Assist. Wireless Commun. 5G Beyond*, Oct. 2022, pp. 73–78.
[137] P. Consul, I. Budhiraja, D. Garg, and A. Bindle, "Power allocation scheme based on DRL for CF massive MIMO network with UAV," in *Proc. Innov. Inf. Commun. Technol. (ICIICT)*. Thailand: Springer, 2022, pp. 33–43.

SHIVANI GABA received the B.Tech. and M.Tech. degrees from Kurukshetra University, in 2015 and 2017, respectively. She is currently an Educator, a Researcher, and a Philanthropist. She is also a Microsoft Technology Associate (MTA) and a Microsoft Office Specialist (MOS) Certified. She is also a Research Scholar with the School of Computer Science and Engineering, Bennett University, Greater Noida. She has presented and published abundant papers and chapters in national/international conferences and journals. Her research interests include AI, blockchain, deep learning, and cyber-attacks.

ISHAN BUDHIRAJA (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Uttar Pradesh Technical University, Lucknow, India, in 2008, the M.Tech. degree in electronics and communication engineering from Maharishi Dayanand University, Rohtak, Haryana, in 2012, and the Ph.D. degree in computer science engineering from the Thapar Institute of Engineering & Technology, Patiala, India, in 2021. He was a Research Associate on the Project Energy Management of Smart Home Using Cloud Infrastructure-A Utility Perspective, funded by CSIR, New Delhi, India. Some of his research findings are published in top-cited journals, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE INTERNET OF THINGS JOURNAL, *IEEE Wireless Communication Magazine*, and IEEE SYSTEMS JOURNAL, and various international top-tiered conferences, such as IEEE GLOBECOM, IEEE ICC, IEEE WCMC, ACM, and IEEE Infocom. His research interests include device-to-device communications, the Internet of Things, non-orthogonal multiple access, femtocells, deep reinforcement learning, and microstrip patch antenna.

VIMAL KUMAR (Member, IEEE) received the M.Tech. and Ph.D. degrees from MNNIT Allahabad, Prayagraj, Uttar Pradesh, India. He is currently an Assistant Professor in SCSET with Bennett University (Times of India Group), Greater Noida. He has more than 17 years of teaching and research experience. His past research work is more focused on multipath mobile computing in heterogeneous networks for multi-interface enabled smart mobile devices to improve the QoE of end users. He has published 17 research papers in various reputed SCI/Scopus/WoS/ESCI indexed journals and conferences and his papers are awarded best papers in conferences. He is currently passionate about innovations in blockchain use cases and use of IoT devices in various domains. He is also a member of Internet Society.

SHESHIKALA MARTHA (Member, IEEE) received the Ph.D. degree from K. L. University. She has been a Professor and the Head of SR University, since 2012, and having total experience of more than 18 years. She has published more than 50 publications in reputed research journals. Her research interests include data mining, machine learning, deep learning, and cyber-physical systems.

JEBREEL KHURMI received the B.S. degree in Computer Engineering and Networking from Jazan University, Jazan, Kingdom of Saudi Arabia, the M.S. degree in Computer Science Networks and Telecommunications from University of Missouri–Kansas City, MO, USA. Currently, he is a Lecturer with Jazan College of Technology, Saudi Arabia. His research interests are the IoT, Smart Applications, and Sensors Enhancements.

AKANSHA SINGH (Member, IEEE) received the B.Tech. and M.Tech. degrees in computer science and the Ph.D. degree in image processing and machine learning from IIT Roorkee. She is also a Professor with the School of Computer Science and Engineering, Bennett University, Greater Noida, India. She has also undertaken government funded project as a principal investigator. Her research interests include image processing, remote sensing, the IoT, and machine learning. She has served as an associate editor and a guest editor for several journals.

KRISHNA KANT SINGH received the B.Tech., M.Tech., M.S., and Ph.D. degrees in image processing and machine learning from IIT Roorkee. He is currently working as the Director with Delhi Technical Campus, Greater Noida, UP, India. He has wide teaching and research experience. He has authored more than 116 research articles in Scopus and SCIE indexed journals of repute. He has also authored 25 technical books. He is an Associate Editor of *Journal of Intelligent and Fuzzy Systems* (SCIE Indexed) and IEEE Access (SCIE Indexed) and a Guest Editor of *Open Computer Science* and *Wireless Personal Communications*. He is serving as a member of Editorial Board for *Applied Computing and Geoscience* (Elsevier).

S. S. ASKAR received the B.Sc. degree in mathematics and the M.Sc. degree in applied mathematics from Mansoura University, Egypt, in 1998 and 2004, respectively, and the Ph.D. degree in operation research from Cranfield University, U.K., in 2011. He has been an Associate Professor with Mansoura University, since 2016. He has joined King Saud University, in 2012, where he is currently a Professor with the Department of Statistics and Operation Research. His main research interests include game theory and its applications that include mathematical economy, dynamical systems, and network analysis.

MOHAMED ABOUHAWWASH received the B.Sc. and M.Sc. degrees in statistics and computer science from Mansoura University, Mansoura, Egypt, in 2005 and 2011, respectively, and the joint Ph.D. degree in statistics and computer science from Michigan State University, East Lansing, MI, USA, and Mansoura University, Egypt, in 2015. Currently, he holds significant academic positions at Distinguished Institutions, including Computational Mathematics, Science, and Engineering (CMSE), Biomedical Engineering (BME), and Radiology, Institute for Quantitative Health Science and Engineering (IQ), Michigan State University. Additionally, he serves as an Associate Professor at the Department of Mathematics, Faculty of Science, Mansoura University. During 2018, he dedicated to advancing knowledge transcends geographical boundaries, as evidenced by his role as a Visiting Scholar at the Department of Mathematics and Statistics, Faculty of Science, Thompson Rivers University, Kamloops, BC, Canada. He is a Distinguished Researcher and an Academician, widely recognized for his outstanding contributions to the fields of computational intelligence, machine learning, and image reconstruction. With an illustrious career, he has published over 160 papers in esteemed journals, including notable publications like IEEE Transactions on Evolutionary Computation, IEEE Transactions on Medical Imaging, IEEE Transactions on Emerging Topics in Computational Intelligence, Artificial Intelligence Review, Expert Systems with Applications, Swarm and Evolutionary Computation, Knowledge-Based Systems, and Applied Soft Computing. In addition to his prolific research output, he has showcased his expertise by authoring several edited books published by reputable academic publishers such as *Springer, Wiley, Taylor, and Francis*. His impact on the academic community is further amplified through his editorial board service in numerous prestigious journals and conferences. Throughout his illustrious career, he has received recognition for his academic excellence, notably being honoured with the best master's and Ph.D. Thesis Awards from Mansoura University in 2012 and 2018, respectively.