Cyber Security and Applications 2 (2024) 100034

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Security analysis of cyber physical system using digital forensic incident response

Pranita Binnar[a,*], Sunil Bhirud[a], Faruk Kazi[b]

[a] Dept. of Computer Engineering and Information Technology, Veermata Jijabai Technological Institute, Mumbai, Govt. of Maharashtra, India
[b] Dept. of Electrical Engineering, Veermata Jijabai Technological Institute, Mumbai, Govt. of Maharashtra, India

ARTICLE INFO

Keywords:
Digital forensics incident response (DFIR)
Industrial IoT (IIoT)
Security
Internet of Things (IoT)
SCADA
Cyber physical systems (CPS)
Industrial Control Systems (ICS)
Intrusion detection systems
Attack detection

ABSTRACT

There is a great demand for an efficient security tool which can secure IIoT systems from potential adversarial attacks. However, it is challenging to design a suitable security model for IIoT considering the closed, dynamic and distributed architecture. This motivates the researchers to focus more on investigating the role of forensic tools such as DFIR in the designing of security models. A brief analysis of the security issues, challenges and attacks on IIoT systems is presented in this paper with an emphasis of DFIR for the security of ICS, CPS, and SCADA. The security recommendations for IIoT, forensic challenges in SCADA, ICS and CPS are discussed. The study suggests that forensic tools can overcome the drawbacks of conventional security solutions in terms of maintaining the privacy of data while sharing information with other systems. The study discusses different models, overview, comparisons, and summarization of DFIR and intrusion detection systems (IDS)-based techniques for IIoT security. In addition, this review analyzes the challenges and research gaps based on the existing literary works.

Introduction

Background of the study

Industrial IoT (IIoT) or Industry 4.0 is one of the advanced, automated and intelligent technologies that make use of smart sensors and actuators to enhance manufacturing and industrial processes [1]. IIoT incorporates several progressive technologies such as cloud computing, Internet of Things (IoT), artificial intelligence (AI) and modern solutions such as industrial automation and monitoring. These technologies collectively augment manufacturing and industrial processes by improving efficiency, reliability, and cost-effectiveness. Network security and data integrity are the two main driving factors which play an important role in enhancing the automated IIoT environment [2]. With the increasing adoption of IIoT applications, the need for security in IIoT is growing extensively [3]. Although IIoT systems are vulnerable to cyber-attacks due to their dynamic and ad-hoc nature, these systems can be secured by perpetual supervision and analysis and thereby taking preventive measures, reducing possible risks, and protecting confidential data [4–6]. Some of the effects of network security are network failure, unprecedented attacks, data manipulation and exploitation from the IoT system.

In addition to the existing cybersecurity issues, the threats and data breaches on the IIoT applications due to the unreliable machine-to-machine (M2M) communication should also be considered [7]. M2M communication systems are termed as the next generation network which connects several heterogeneous devices using wireless communication [8]. M2M networks are characterized by their self-operated and automated learning characteristics. These characteristics enable the M2M devices to operate autonomously without any human intervention and make appropriate decisions using AI. Since M2M communication involves the interaction of several heterogeneous devices, these networks are highly susceptible to cybersecurity threats [9].

Some of the prominent security threats for M2M communication systems are due to the unauthorized data breaching caused by the injection of malicious entities into the network system. In addition, the substantial difference between the existing operational technology and M2M communication make the IIoT platform more susceptible to the security problems [10,11]. The security problem in M2M communication systems becomes more complex due to the interconnection of billions of IoT devices. It is highly challenging to identify the cybersecurity threats and requires effective techniques to classify the impact of cyber threat and manipulation of device data. Therefore, identifying data breach in the early stages is essentially critical in the IIoT environment. The potential threats and attacks that affect the privacy and integrity of the IIoT system are illustrated in Fig. 1. Correspondingly, different types of security attacks that occur in different layers of IIoT architecture are tabulated in Table 1.

[*] Corresponding author
E-mail addresses: pbbinnar_p19@ce.vjti.ac.in (P. Binnar), sgbhirud@ce.vjti.ac.in (S. Bhirud), fskazi@el.vjti.ac.in (F. Kazi).

https://doi.org/10.1016/j.csa.2023.100034
Received 7 July 2023; Received in revised form 10 November 2023; Accepted 14 December 2023
Available online 16 December 2023

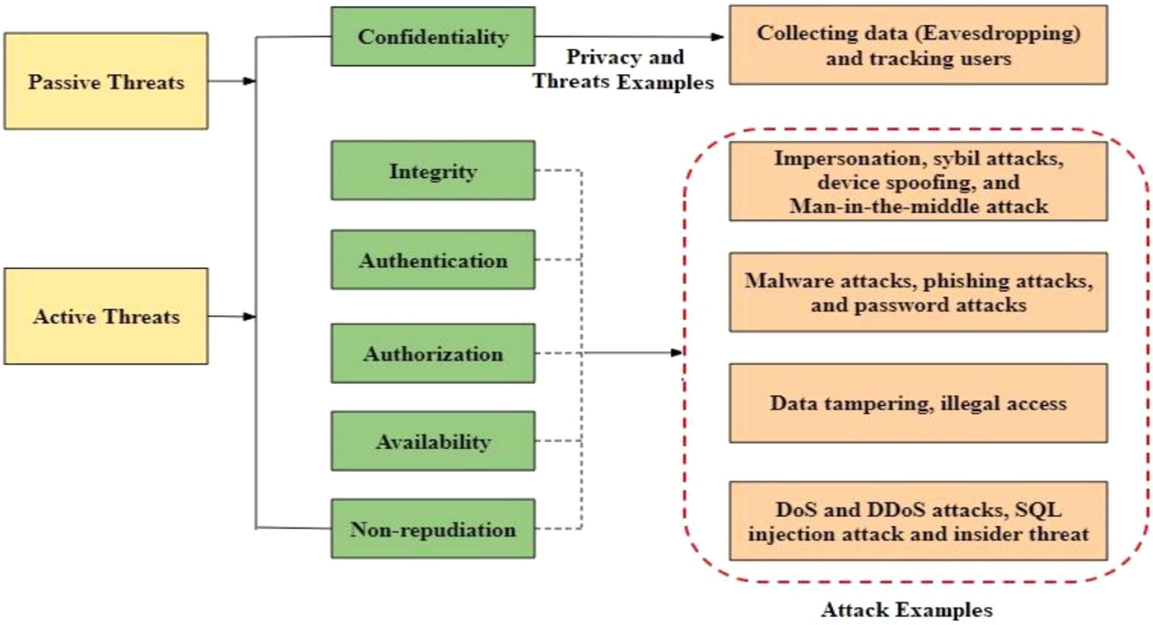
Passive Threats
Active Threats
Confidentiality
Integrity
Authentication
Authorization
Availability
Non-repudiation
Privacy and Threats Examples
Collecting data (Eavesdropping) and tracking users
Impersonation, sybil attacks, device spoofing, and Man-in-the-middle attack
Malware attacks, phishing attacks, and password attacks
Data tampering, illegal access
DoS and DDoS attacks, SQL injection attack and insider threat
Attack Examples

Fig. 1. Potential security attacks and threats in IIoT.

Table 1
Security attacks in IIoT architecture.

Attacks	Layer	Security challenges
DoS, DDoS attacks	Network layer, Application layer	Secure IoT offloading, Access control, Data Availability, and Heterogeneity
Jamming	Physical layer	Identity, Leak of Private Data, Confidentiality
Phishing	Application layer	Authentication, Prediction and Prevention
Intrusion	Application layer	Access control
Malware	Application layer	Malware detection and Access control
Eavesdropping	Physical layer	Confidentiality, Device Integration,

Security analysis in IIoT environment

The research related to the security of the IIoT environment also includes the analysis of its subsidiaries such as Cyber Physical Systems (CPS), Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA). The Cyber-Physical Systems (CPS) are the integration of computation, networking, and physical processes. Due to the physical constraints, integration of CPS components might pose a significant threat to the security of CPS environments [12]. From a technological perspective, CPSs are a unification of different networking systems, ubiquitous computation, effective communication, physical mechanisms and efficient control. Some of the CPSs depend on internet and ad hoc networks for exchanging the data and control signals between the system components. This increases the vulnerability of the system towards attacks which are mainly launched in the network region. It is not necessary that these attacks happen in the network domain but there are chances that these attacks can occur in the physical environment too. This makes CPS more sensitive towards attacks on all components [13].

Industrial control systems (ICS) are responsible for controlling the production process and monitoring the operation of smart devices which have constant access to the communication networks [14]. ICS is an eclectic network which is an integration of different configuration systems such as Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), and SCADA, which are extensively adopted in industrial applications. SCADA is a control system architecture that consists of computer systems, communication network and graphical user interfaces for supervising the manufacturing process in several industrial applications. The interaction of different components in SCADA increases the risk of cybersecurity threats [15].

In general, the vulnerability of ICS systems are mainly due to the issues in the network configuration, faults in the system components, irregular maintenance, and malfunctioning of network parameters including hardware, and software components. Several security mechanisms are available for minimizing the vulnerabilities and potential threats in ICS systems such as identification of coordinated physical and cyber-attacks, network attacks, intrusion detection etc. [16]. ICS are more prone towards cyber-attacks because of its poor compliance with the security requirements such as confidentiality, integrity, and availability (CIA). Lack of data integrity results in the leakage of sensitive information to unauthorized entities, while the lack of confidentiality in ICS allows intruders to eavesdrop confidential information [17]. Hence it is highly significant to assess cybersecurity in the early stages to mitigate the effects. The CPS, ICS, and SCADA are all interconnected within the IIoT environment and are responsible for allowing remote monitoring and controlling of different operation processes. Although the interconnection of these systems maximizes the operational efficiency of the IIoT, they introduce potential threat to the system architecture in terms of CIA parameters [18]. Besides, the advanced industrial facilities increase the security vulnerabilities towards cyber-attacks.

Need for digital forensics incident response (DFIR)

Since the security threats are becoming more advanced and sophisticated, it requires an effective countermeasure for identifying and mitigating the attacks [19,20]. The security mechanism must be resilient to sustain cybersecurity threats without affecting the operation system. Although all cyberattacks are not identifiable the incident response (IR) becomes an integral part of the security of IIoT, CPS, and ICS including the requirement of digital evidence. Forensic digital evidence must be conducted without affecting the authenticity and verifiability of the digital evidence in order to maintain its integrity. In this context, the application of DFIR for the security of IIoT is gaining a lot of significance in recent times [21,22]. It is important to explore and develop more sophisticated digital forensic models which can assist in the development of robust countermeasures for cybersecurity attacks. This is mainly due to the fact that during IR, a cyberattack or threat has to be accredited to a potential attacker. The concept of digital forensics in IIoT lacks standard techniques and measures which illustrates the significance of how the threats can be handled during the occurrence of cyberattacks. While the conventional CPS, ICS, and SCADA platforms can be implemented individually, it has become apparent to integrate these components to achieve a competent industry 4.0 environment. As discussed previously, this integration can increase the security risks and the landscape of security attacks has widened.

In this context, this paper emphasizes the implementation of DFIR for identifying security threats in the IIoT environment. In particular, the paper discusses related approaches and techniques that addresses cyber resilience and advanced DFIR. However, there is a lack of available research works which comprehensively evaluates the security protocols and provides quality assessment. This paper aims to address this research gap by systematically reviewing relevant and prominent research works.

The main contributions of this research are summarized as follows:

- ***Comprehensive analysis of DFIR:*** A broad analysis of DFIR for the security of ICS, CPS, and SCADA are discussed in this paper. This paper presents a systematic overview of various works done on the analysis of DFIR for IIoT and discusses various methodologies used for IIoT, SCADA, ICS, and CPS with prominent observations.
- ***Investigation of potential vulnerabilities in IIoT:*** A detailed investigation on the security issues, security challenges and attacks on IIoT systems is presented in this paper.
- ***Summary and comparison:*** A brief summary and comparison of different research works are presented in this paper which provides a clear analysis of the application of DFIR to IIoT security.
- ***Challenges related to DFIR based IIoT Security:*** The prominent research challenges related to the implementation of DFIR models for ensuring the privacy and security of IIoT is outlined in this paper.

The rest of the paper is structured as follows: Section 2 provides the methodology used for the systematic literature review. Section 3 outlines the related works with respect to the analysis of DFIR for different applicants with an emphasis on IIoT security. Section 4 discusses the challenges and research gaps associated with DFIR models for security threat IIoT and other applications. Section 5 concludes the paper with prominent conclusion points.

Systematic literature review

The preliminary aim of this study is to provide an evidence-based systematic literature review (SLR) to evaluate the prominent DFIR aspects in IIoT and its subsidiaries such as SCADA, ICS, and CPS. The SLR is conducted to identify critical challenges and research gaps which can provide a productive insight for the researchers carrying out their research in the DFIR domain.

Methodology for conducting SLR

A SLR is conducted by searching the relevant articles based on the keywords and search strings. This is the first step involved in the literature review process. The keywords and strings are searched on four search engines namely Springer, Research Gate, IEEE Xplore and Google scholar. In addition to this, the keywords are formulated using Google search trends. These sources are considered as the most valuable sources used for obtaining high quality research articles and journals. The SLR conducted in this study involved a five stage approach which are as follows:

Table 2
Online database, search engines and their respective URLs.

Sl. No.	Database name/ Search engine and URL
1	Springer https://link.springer.com/
2	Research Gate https://www.researchgate.net/search
3	IEEE Xplore https://ieeexplore.ieee.org/Xplore/home.jsp
4	Google Scholar https://scholar.google.com/

(i) Dimensions of focus for literature selection.
(ii) Data source selection and search process.
(iii) Inclusion and exclusion criteria.
(iv) Study quality assessment.
(v) Data extraction and synthesis strategy.

Dimensions of focus for literature selection

The main focus for finding existing literary works related to the current topic is the application of DFIR for the security of IIoT, CPS, ICS, and SCADA applications.

Data source selection and search process

The selection of articles are mainly based on the finalized keywords and search strings which are described in Section 2.1.1. The relevant articles are sourced from the electronic database. The search engines and online database used in the SLR are listed in Table 2.

In this stage, the results of the search process and access of literary works are listed and analyzed. Based on the results, the content and keywords of the obtained literary works are finalized. Majority of the references are collected from recent years (not older than 2015) and the corresponding authors, objective and content of the articles, preferred techniques, and methodologies are discussed. Since this research emphasizes the deployment of DFIR for the security of the IIoT environment, the relevant articles, journals are selected and the main intent of the article is summarized. While selecting the sources, the keywords related to DFIR adoption for IIoT applications, digital forensics for ICS, SCADA, and CPS are searched and relevant results are retrieved. The obtained results were shortlisted based on the keywords and strings such as Cybersecurity, Security threats and Security attacks in IIoT environment. Further, the shortlisted articles are investigated and verified to filter duplicate articles. The terms used for the search process are tabulated in Table 3. A detailed search strategy is applied to obtain a maximum number of relevant articles and most probably recent articles. The search process is carried out using Boolean operators such as “AND” and “OR” operators. The “AND” operator is used to combine the search terms from different categories and the “OR” operator is used to sort multiple keywords belonging to the same category.

Since a large number of results are obtained and it is challenging to explore all literary works, a filtration and assessment criteria is applied. The stages of filtration and criteria used for assessing the articles are summarized in Table 4. The search results after each filtration stage for each journal is discussed below:

The first filtration search stage includes the results consisting of all keywords. If the articles consist of one or more keywords in the title and keyword list, the journal was considered, else it was not considered for the literature review. In the second stage, the keywords and search strings were reviewed and if they are present in the title then they were considered for the evaluation. This research intends to consider only recent articles i.e., articles not older than 2015 and based on this the third filtration stage was applied. In addition to the titles, the articles were also reviewed based on the abstract. Based on this the fourth filtration

Table 3
Search category, search strings, and keywords.

Search category	Search strings	Keywords
Industrial Internet of Things (IIoT)	(TITLE-ABS-KEY (Industrial Internet of Things") OR (TITLE-ABS-KEY ("Security of IIoT") TITLE-ABS-KEY ("DFIR for Security"), AND PUBYEAR > 2015	IIoT architecture, Cybersecurity, Threats and Solutions
Industrial Control Systems (ICS), SCADA	(TITLE-ABS-KEY ("Industrial Control Systems") OR TITLE-ABS-KEY ("SCADA") OR TITLE-ABS-KEY ("DFIR for ICS and SCADA"), AND PUBYEAR > 2015	ICS Security, Security threats, SCADA
Cyber Physical Systems (CPS)	(TITLE-ABS-KEY ("Cyber Physical Systems ") (TITLE-ABS-KEY ("DFIR for CPS"), AND PUBYEAR > 2015	CPS architecture, DFIR, Cybersecurity

Table 4
Stages of filtration and assessment criteria.

Filtration stage	Process involved	Assessment criteria
First stage of filtration	Search the relevant articles from the search engines and online databases using related keywords	All keywords are considered

Second stage of filtration	Excluded articles and journals based on the keywords, search strings, and titles	If the title contains keywords and search strings;
		Yes = include articles
		No = exclude articles

Third stage of filtration	Excluded articles based on year of publication and journal of publication	If the articles published are not older than 2015 and are from IEEE Xplore, Springer, and Research gate;
		Yes = include articles
		No = exclude articles

Fourth stage of filtration	Excluded articles based on the abstract	Is the abstract relevant to the study;
		Yes = include articles
		No = exclude articles

Fifth stage of filtration	Exclude articles based on their study area and objectives	If it is about security of IIoT using DFIR
		Yes = include articles
		No = exclude articles

stage was applied. In this stage, the articles were read based on their study area and objectives. In this stage, the entire content of the finalized papers were read to ensure that the text contained content related to the security of IIoT using DFIR or papers that have implemented DFIR for the security of ICS, SCADA, and CPS applications. The objective of the SLR is to review more works related to the security of IIoT using DFIR technology and at the end of fifth stage of filtration, 70 papers were considered for the review.

Inclusion and exclusion criteria

As discussed in the previous section, the assessment criteria is discussed and these criteria's are applied for conducting SLR. Papers which can help to analyze the concept of DFIR application in the security of IIoT are analyzed. The journals and articles that did not meet the requirements are excluded from analysis. In addition, the articles not written in English, duplicate articles, articles published in conference papers and journals other than IEEE, Springer and Research gate, non-academic articles and articles older than 2015 are excluded from the SLR.

Study quality assessment

The articles considered for the SLR are subjected for quality appraisal from the respective journals and only high quality articles published in high impact factor journals were considered for the SLR. The articles were searched from Google scholar engine for reference and are reviewed in detail.

Data extraction and synthesis strategy

The papers finalized for SLR were selected based on the inclusion and exclusion criteria to make sure that all papers are relevant to the study. All papers that were considered for the SLR were based on the implementation of DFIR for strengthening the security of IIoT architecture and its components. After finalizing the paper for SLR, the important content from the papers were extracted and are analyzed based on the research questions. A brief overview of the finalized papers are discussed in the section below.

Analysis of DFIR

This section discusses the analysis of DFIR for IIoT and other elements of the industrial environment such as SCADA, ICS and CPS.

IIoT and Industry 4.0

Industry 4.0, also termed as the fourth industrial revolution, was introduced to transform the product customization in a cost-efficient manner [23]. As a prominent part of Industry 4.0, smart and automated manufacturing processes are gaining prominence because of their capability to integrate various physical resources and network technologies. Industry 4.0 makes the manufacturing process more precise by enhancing the quality, reliability, security, performance, transparency and controllability of the process. This has led to the development of Industrial Internet of Things (IIoT) technology that incorporates various operational technologies such as SCADA, ICS and CPS. These technologies are not only integrated with advanced Internet and Communication Technologies (ICT) and automates the process of multiple networking devices and applications that work on a shared intelligence concept [24]. The relationship between IoT, IIoT, and Industry 4.0 is illustrated in Fig. 2 [25].

Industry 4.0 incorporates IIoT devices and operational technology (OT) devices for achieving better connectivity, reliability and interoperability. Due to the longer span of OT devices, the legacy-related issues must also be considered. Due to its integration with various heterogeneous elements, Industry 4.0 suffers from different problems such as communication buffer, complex authentication [26], lack of security solutions, difficulty in upgrading the legacy systems without impacting the performance and interoperability [27]. Not addressing these drawbacks might result in security violations, data leakage or privacy issues.

It is essentially important to understand the performance requirements of the networks before developing a robust fault-tolerant model. The need for a fault-tolerant model and longer lifespan is required more in OT networks compared to IT networks [28]. These aspects should be

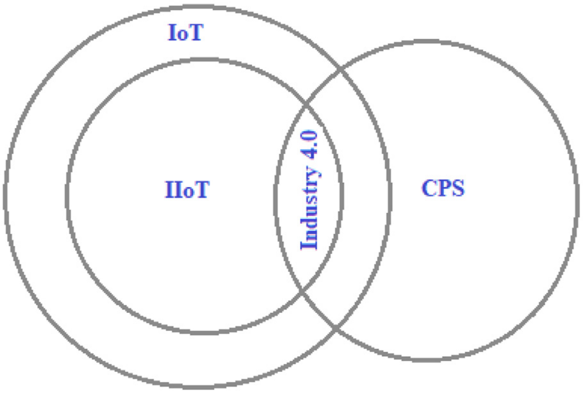

Fig. 2. Relationship between IoT, IIoT, CPS and Industry 4.0.

considered while implementing IT solutions to the OT systems in IIoT and industry 4.0 environments.

Security recommendations for IIoT

It can be inferred from existing studies that there is a great need for effective security recommendations for both IT and OT systems [29]. The lack of security practice and poor availability of resources to invest in developing efficient security solutions is the need of the hour [30]. This research identifies and recommends some of the prominent security practices for IT and OT systems in the IIoT environment. The specific requirements in industrial manufacturing applications demand additional resources while designing security solutions for IIoT systems. Some of the fundamental security requirements identified in this research are confidentiality, integrity, authentication, authorization, availability and nonrepudiation, which are discussed in below points.

(i) ***Confidentiality:*** Unverified modification of information can have a malicious impact on the users in the IIoT systems. This risks the confidentiality of the system data and restricts the adaptability of the IIoT environment [31]. Hence, it is important to ensure that the information is not modified and its confidentiality is maintained during different stages of data transmission such as capture, update, storage, retrieval, and exchange. Confidentiality ensures that only authorized entities can access the information and modify it.

(ii) ***Integrity:*** Similar to confidentiality, the integrity of the data can be protected by enabling verified access to the device information. Since a significant amount of data is communicated via wireless networks, the IIoT system becomes more vulnerable to security threats. The changes in the communication is detected via a thorough verification process in an insecure wireless network. Poor integrity affects the performance efficiency of the IIoT systems [2] and hence it is important to detect the changes in the early stages.

(iii) ***Authentication:*** Authentication of the user or device is important before performing any task. The authentication process is not the same for all systems in IIoT and are tailored according to the device attributes and functionalities [32]. The heterogeneity of devices in IIoT systems makes it complex to design a suitable authentication process and it is also difficult to satisfy different security constraints. Several authentication processes have been discussed by different authors which are summarized in Table 5.

(iv) ***Authorization:*** The preliminary objective of the data authorization techniques is to protect the confidential and private information of the users and devices by allowing verified access to the data. The techniques used for authorization incorporate different policies to develop a customized control action and authorize them to perform on IIoT applications [7]. Most of the authorization techniques are categorized into two schemes namely policy based and token based schemes. Policy and token based authorization techniques are designed for centralized systems and decentralized systems respectively, wherein token based systems are considered to be more advantageous compared to policy based techniques because of their adaptability in decentralized architectures [33].

(v) ***Availability:*** The availability of data must be ensured in order to allow better accessibility to the information. Most of the IT and OT systems use private or public clouds for storing the data. Both hardware and software data should be available and must be readily accessed by the smart devices in IIoT to provide better quality of service in terms of reliable data transmission.

(vi) ***Non-repudiation:*** Non-repudiation guarantees that the authenticity of the data transmitted from source to destination cannot be questioned later [34] since it validates the data source, reliability and integrity.

As mentioned in Fig. 1, attacks such as DoS, DDoS, malware injection, eavesdropping, impersonation etc. affects the security of the IIoT environment. Several research works have developed potential solutions leveraging DFIR for protecting IIoT against the attacks. The prominence of DFIR in IIoT is due to the dependence on multiple interconnected industrial systems and the increasing number of security threats and attacks on these systems [43]. IIoT and its components such as ICS/CPS/SCADA are critical infrastructures which needs to be secured from cyberattacks and ensure the privacy and security of these systems [44–46]. The work presented in [47] discussed the vulnerabilities of IIoT and the application of forensic technologies to prevent them. The study emphasized the adoption of Artificial Intelligence (AI) technologies for enhancing the forensic investigation process by securing the evidence. Many works have suggested the application of digital forensics along with AI-based deep learning (DL) model for detecting different types of cyberattacks such as DoS, DDoS, device spoofing, insider threats, malwares etc. in IIoT systems [48–50]. During attack occurrences, the digital forensic system helps in determining the primary cause of the attack and assists in obtaining the complete information about the attack. In addition, the DFIR model assists in understanding how IIoT components can be manipulated and thereby helps in anticipating such attacks in the near future. A multi-layer IIoT architecture is presented in [51] which is accompanied with digital forensics applied at different levels. Digital evidence about the attacks on IIoT was collected based on the attributes of the attack. The proposed DFIR-based approach was tested with respect to different sets of security breach in IIoT. A comprehensive analysis of different IIoT components such as ICS/CPS/SCADA are discussed in below sections.

SCADA forensics within IIoT

The SCADA is a system which integrates several hardware and software elements. In general, SCADA is used to control and monitor different industrial processes in local environments and remote locations [52]. SCADA collects real-time information and measurements from the devices such as pumps, motors, valves and smart devices such as sensors and actuators. SCADA is connected with other devices via a software component which automates the monitoring process and increases the adaptability of SCADA in different industrial applications such as recycling process, electrical energy distribution, waste management, manufacturing process and transportation. SCADA monitors and controls a network of Programmable Logical Controllers (PLCs), Real-Time Automation Controllers (RTACs), and Remote Terminal Units (RTUs) which adopt sensors for measuring the recordings of the operational and automation process [53]. The architecture of the SCADA environment is illustrated in Fig. 3.

The convergence of IIoT with SCADA systems has witnessed tremendous advancements in recent years. Initially, SCADA systems were operated on closed environments wherein the system was physically sepa-

Table 5
Summary of security parameters for IIoT.

Security parameters	References	Objectives	Limitations
Confidentiality	[31]	Context-based confidentiality is analyzed using a metamodel	The adaptability and error-proneness needs more attention along with an improvement in the scalability
	[35]	An Attribute Based Encryption (ABE) technique is proposed to achieve better access control, integrity, and confidentiality	The performance of ABE technique is not validated over other cryptographic approaches
Integrity	[2]	To investigate the role of evolutionary process in understanding the evolution of attackers by leveraging wireless cyber physical simulator (WCPS)	Performance evaluation metrics such as Area under curve (AUC), communication noise, and attack classification accuracy needs to be improved.
	[36]	To discuss different security threats and possible solutions for IIoT architecture	Intrusion detection systems (IDS) for industry 4.0 and IIoT along with preventive mechanisms are not comprehensively evaluated.
	[37]	A peer-to-peer (P2P) architecture is designed to strengthen the security of IIoT in terms of CIA parameters	The specific requirements of the P2P IIoT architecture in terms of industrial manufacturing are not addressed.
Authentication	[32]	A Distributed Ledger Technology (DLT) and Secure Multi-Party Computation (SMPC) is integrated to strengthen the security in industrial IIoT devices	The implementation of DLT needs to be validated using smart contracts and more dynamic approach utilizing machine learning is required to enhance DLT for security
	[38]	A two-factor authentication scheme is proposed for IIoT environment	The authentication scheme needs to be validated using more criteria set
	[39]	An authentication scheme based on lightweight operations such as XOR is implemented for resource constrained IIoT devices	Though there are no significant limitations, it was observed that the implementation of the authentication scheme is more complex, which can be resolved using parallel computations
Authorization	[7]	A novel authorization technique based on Message Queuing Telemetry Transport (MQTT) is proposed to ensure the authenticity and authorization in IIoT networks by achieving a secure interoperability	The proposed authorization scheme is not evaluated against different cyber-physical attacks considering real-time scenarios
	[40]	A reliable authorization approach is proposed for ensuring authorized access into IIoT devices	The recognition accuracy has to be improved considering the collaboration of multiple forms of identity
Availability	[41]	The challenges associated with the security of IIoT are analyzed with respect to integrity and availability of device data	There is a need to explore more security solutions which does not affect the latency of the attack detection approaches
Non-repudiation	[42]	The concerns related to CIA parameters along with non-repudiation is discussed with an emphasis on IIoT security	The security measures discussed in this work is for IIoT network as a whole and does not focus on individual components such as devices, networks and clouds

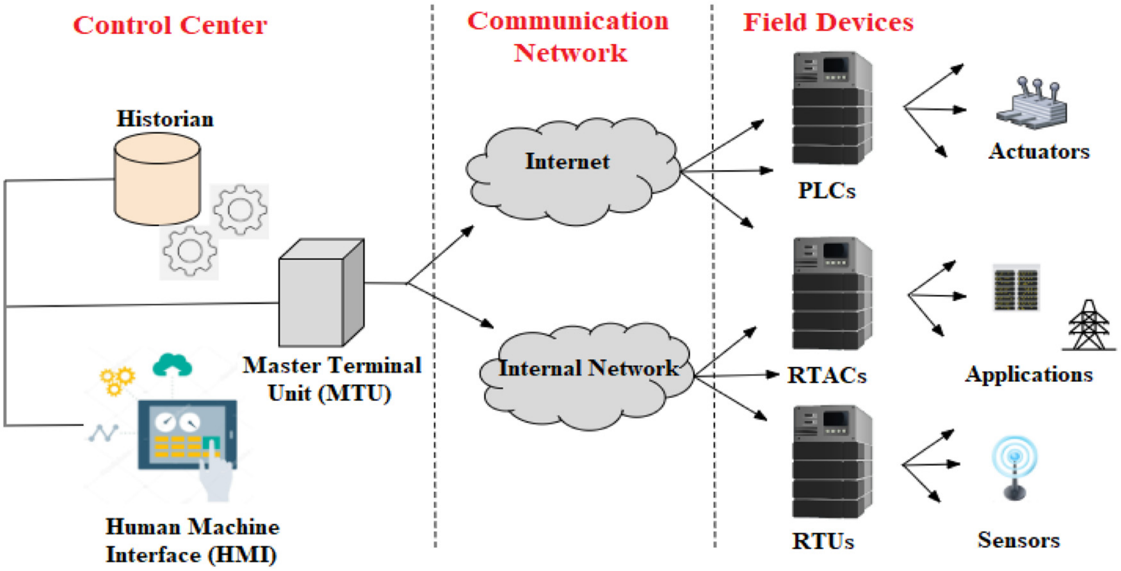

Fig. 3. Schematic representation of SCADA architecture.

rated from local environment and internet. This reduced the risk of cyber threats and unauthorized intrusions from external entities. With the integration of cutting-edge technologies such as IoT and IIoT, SCADA systems are also becoming more susceptible to security attacks [54]. During attack occurrences, it is important to conduct a comprehensive forensic investigation to identify the root cause of the attack and possible attackers. However, the dynamic and resource specific nature of SCADA systems makes it difficult for the conventional IT forensic solutions and techniques to detect and classify security attacks. Hence it is essential to adopt a potential digital forensic incident response (DFIR) model to prevent the failure of SCADA systems from cyber security threats. The stages involved in the design of a DFIR model for SCADA systems are illustrated in Fig. 4.

The design of a DFIR model for the SCADA environment involves multiple stages which are discussed in below points:

Stage 1: Prepare

It is the preliminary stage wherein it is essential to understand the system requirements in order to predict the possible attacks on the system. Since each SCADA system has a unique architecture, it is important to gather detailed information about network configuration, hardware and software details etc. The details about the network configuration includes details about the network map, and data exchange points into

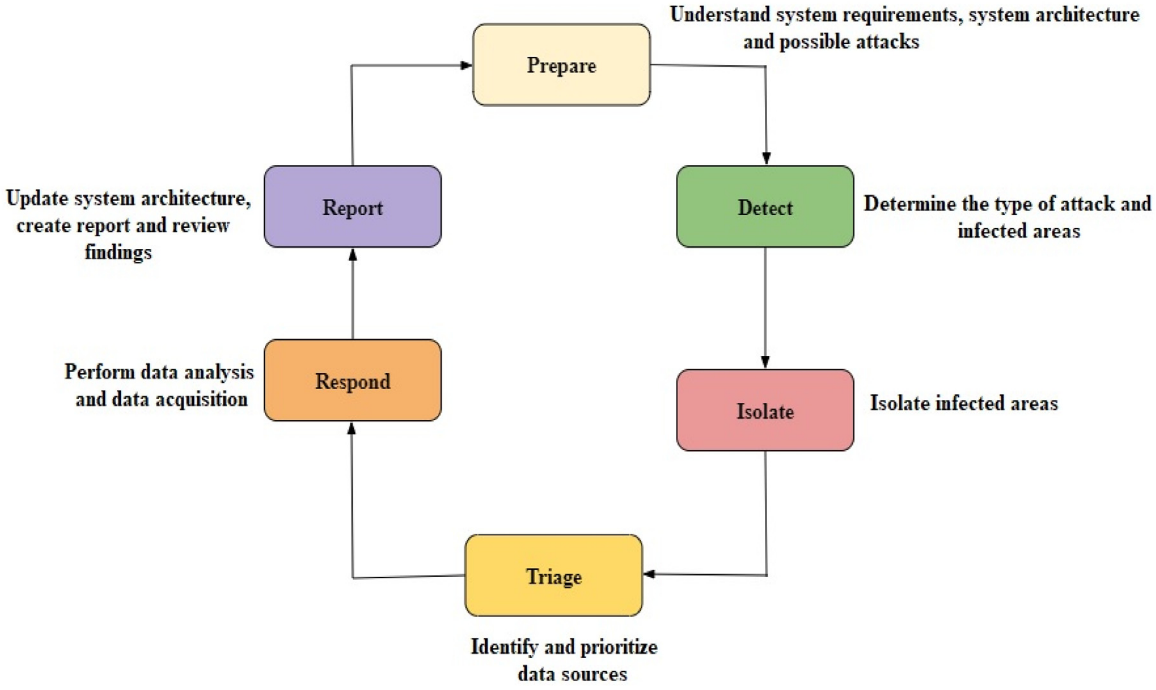
Understand system requirements, system architecture and possible attacks
Prepare
Update system architecture, create report and review findings
Report
Detect
Determine the type of attack and infected areas
Perform data analysis and data acquisition
Respond
Isolate
Isolate infected areas
Triage
Identify and prioritize data sources

Fig. 4. DFIR model for SCADA environment.

the system. In addition to this, the details about the type of hardware devices and software requirements must also be analyzed to identify back-up devices and devices which can run continuously without fail. It is also important to understand the types of attacks that can occur in different areas of the system.

Stage 2: Detect

In the second stage of the DFIR process, the type of the attack on the system is identified and the most affected areas are located. When an attack occurs, the investigator must identify the type of attack by assessing the real-time information and determining the abnormalities in the behavior of the system.

Stage 3: Isolate

After detecting the attacks, the infected areas are isolated to prevent further damage to the system based on the observations. The isolation of attacks is based on the system requirements and operational requirements of the SCADA environment.

Stage 4: Triage

This stage involves two stages namely identification of data sources and prioritizing data sources. The triage process is initiated by determining the data sources and is carried out by documenting the preparation stage and attack detection stage together. This is a critical process in determining the effectiveness of the DFIR process. The next stage is the prioritization of the data sources which is done to strengthen the evidence available for recovery.

Stage 5: Respond

After prioritizing the data sources, the next stage is to forensically acquire the information from the relevant data sources which can be obtaining from the network data. The data is further analyzed to distinguish the forensic artefacts from other SCADA data. This can be performed using fundamental forensic analysis tools.

Stage 6: Report

After data analysis, the interrelation between the forensic artefacts can be aggregated to create a timeline of events and report the root cause of the incident. Based on the analysis, a report is created which involves the analysis of obtained artefacts and compiled results. The preparation of report involves the validation of data records and also includes the recommendations for securing the SCADA system. Some of the reasons which validates the necessity of forensic solutions for SCADA systems are as follows [53]:

- Forensic tools identify the principal reason of intrusion and the role of possible attackers or intruders.
- These tools help in determining whether the SCADA system is still at risk by analyzing the changes done to the system.
- The damages caused to the SCADA system can be identified using potential forensic tools and thereby evaluate the probability of damage.
- The security of the SCADA systems can be strengthened by minimizing the risk of attacks and preventing the recurrence of unfavorable incidents.

Forensic challenges in SCADA

As discussed previously it is important to understand the prominent aspects of digital forensics in IIoT integrated SCADA systems. The complexity of SCADA systems distinguishes it from conventional IT systems and hence there are specific forensic methods designed for SCADA systems. The taxonomy of existing forensic challenges with respect to DFIR in SCADA are summarized in table 6 [55].

Live forensics refers to the process of accessing volatile and non-volatile data while the system is operating and analyzing the system components using DFIR during offline condition. This process involves a lot of challenges at each and every step due to the continuous variations in the memory and the technical validation of the digital evidence [55]. The work in [56] proposed an effective framework for making liver forensics a feasible solution for SCADA systems. Acquiring live data is different from conventional data acquisition from the hard disks, which collects the data only when the system is offline. This increases the chances of losing important volatile data. As a result, live forensic is a viable option. However, it is challenging to validate how live forensic tools can be executed on a SCADA system to reduce the risk of disrupting essential operations. The challenges involved in live acquisition of forensic data is also highlighted in [57,58]. As inferred from these works, live forensics has a great significance in securing SCADA systems and there is a great need to address the challenges related to live forensics. Rapid

Table 6
Current forensic challenges in SCADA systems.

Forensic challenges	Description
Live Forensics	Live forensics allows data collection and analysis while the SCADA system is operating
Rapid Incident Response	Confidential information about incident occurrences must be protected from being tampered. Rapid response helps in accessing the forensic information quickly after the incident and thereby reduces the chance of losing important data.
Integrity and Validity	Maintaining the integrity of the data and its validity is highly significant in digital forensic investigations. Digital evidence is validated by matching the hash values of the evidence copy and original information. It ensures that the data is not tampered since it is not possible to change the hash values.
SCADA forensic tools	There is a lack of data acquisition tools and techniques specifically designed for SCADA systems. This is mainly due to the restrictions imposed for manufacturing such tools and techniques.

incident response is another prominent challenges in SCADA forensics which prevents the tampering of evidence. Forensic evidence is critical for analyzing any incident and with the delay there are changes that the critical evidence might be manipulated or eliminated by the attackers [59]. In such cases, rapid incident response plays a vital role. However, it is challenging to obtain rapid response when a SCADA system covers a larger distance with different places and locations. The works mentioned in [60–62] highlighted the challenges related to rapid incident response. These challenges can be effectively addressed using DFIR.

Digital evidence is usually validated by using hashing algorithms which matches the hash values of the original data with the obtained data. This ensures the integrity and validity of the digital evidence. However, it is challenging to ensure the integrity and validity of the data since the system always remain online (live) and is subjected to continuous update. Due to this, the data keeps changing from the initial to final process and thereby makes the hash value unusable [59]. The lack of effective SCADA forensic tools also raise the concerns related to the security of critical industrial systems. The work in [63] stated the need for understanding the criticality of SCADA system architecture before designing a potential solution to the forensic problems in SCADA. Presently, there is no appropriate or standard technique for acquiring data for SCADA systems to collect evidence for cyber incidents [55]. The sensitivity of industrial architecture makes it difficult for the organization and concerned authorities for acquiring relevant information and this restricts the design and development of robust digital forensic tools for SCADA systems [56].

Malware analysis tools, techniques, and methodologies used in SCADA/ICS

Different types of malwares such as ransomware, trojans, and spyware are injected in SCADA/ICS which gain unauthorized access to the system. These malware introduce attacks on ICS such as Stuxnet, Havex, BlackEnergy, Irongate, Industroyer etc. These techniques affect the control system and result in the complete shutdown of the SCADA/ICS operation. Considering the criticality of forensic investigation in SCADA/ICS environment, the authors in [64] presented a case study on an infected wastewater treatment plant (WTP). Features such as AES files, URLs, IP and Email data etc. were extracted from the live memory dump to detect DoS attacks in WTP. The vulnerability of OT networks such as PLC, and SCADA to malware injection is discussed in [59]. A DoS attack on PLC used to control the STP is investigated by injecting the malware, which can collect all information IP address, MAC address etc. The work focuses on performing an attack and does not emphasize prevention of attack. Different malware analysis tools and techniques are available to prevent malware attacks. However, it is challenging to prevent malwares since the attackers try to conceal the attacks by using evasion techniques. Techniques such as fuzz test, static taint analysis and dynamic taint analysis are used extensively in providing security against malware attacks [60].

(i) ***Static Taint Analysis:*** This analysis considers an unused branch and uses a set of variables to calculate the upper bound. If the branch is used then all the variables are considered as sensitive and the corresponding program is also marked as sensitive. This protects the non-interference and does not support arrays. However, the accuracy of static analysis is not as high as dynamic analysis.

(ii) ***Dynamic Taint Analysis:*** The dynamic analysis can be used while executing the program and propagates taint across different memory locations. This allows it to track the data flow within the software and can even detect zero day attacks and data leakage from the software. The dynamic taint analysis is based on the dynamic binary instrumentation (DBI) frameworks which use color tainting to track data flow. Each program is monitored using an Inter-process communication (IPC) and the information flow is tracked during the program execution.

(iii) ***Shadow Memory for Tag Management:*** This shows the status of the taint in a specific memory space that is used during program execution. The granularity between the shadow memory and application is mapped and any change in the result can cause corresponding change in the taint for the whole byte. Four bytes allow the tag to acquire more data and helps in aggregating the data.

(iv) ***Tag Propagation:*** Tag propagation is used to propagate the taint marking while capturing the copy of the data, analyzing the transformational dependency. If any one source element is tainted, then the destination is also tainted. If all inputs in an operation are not tainted or clear, then respective destination outputs are also marked as clear.

DFIR for ICS and CPS

The ICS and SCADA systems are combined in a complex network of cyber-physical systems (CPS). The security of both ICS and CPS can be enhanced by identifying potential security solutions which can provide a new dimension to the implementation of ICS in various applications. However, with the increasing adaptability of ICS and CPS in integrating network systems with other physical systems, the susceptibility of these two systems towards cyber-attacks is also increasing [61]. The significance of CPS security has gained huge prominence among researchers in the last decade. Though CPS are installed in a closed network environment which cannot be accessed by the public, they can still be affected by malicious attacks caused by infected software's. This happens when the attacker inserts an infected USB disk into the CPS. By doing so, the attacker can access the entire CPS network and can exploit the data. Especially, the location of the event source can be accessed irrespective of the security measures taken. The basic architecture of CPS is illustrated in Fig. 5.

With the emergence of the Internet of Things (IoT), the physical devices linked with CPS become more susceptible to adversary attacks. Some of the CPSs depend on internet and ad hoc networks for exchanging the data and control signals between the system components. This increases the vulnerability of the system towards attacks which are mainly launched in the network region [62]. It is not necessary that these attacks happen in the network domain but there are chances that these attacks can occur in the physical environment too.

This makes CPS more sensitive towards attacks on all components [63]. On the other hand, ICS is made up of three layers namely enterprise management, supervisory, and field. Similar to CPS, and SCADA, the security requirements of ICS are different from traditional systems because of its closed environment. The security features such as restricted computational resources, restrictions to real-time implementation, vulnerabilities associated with industrial protocols introduce challenges to

Table 7
Categorization of DFIR stages for CPS and ICS.

DFIR stages for CPS and ICS	Description	References
Preparation	Preparation includes creation of communication plan, evaluation of metrics and creation of incident plan. This stage helps in identifying the research gaps and optimizing the security events	[66,67]
Analysis and Detection	It is an important stage in DFIR and plays a prominent role in determining the response of the attack detection process. Since the response cannot be validated without accurate analysis, this stage helps to analyze and detect the security threats	[68–70]
Containment, Eradication and Recovery (CER)	CER is an integral process which distinguishes between models and security standards. With reference to containment, the steps involved in the security frameworks aim to prevent the security attack, while eradication stops the proliferation of cross systems. Lastly, recovery ensures that the operation of system is not perturbed due to attacks or threats	[71,72]

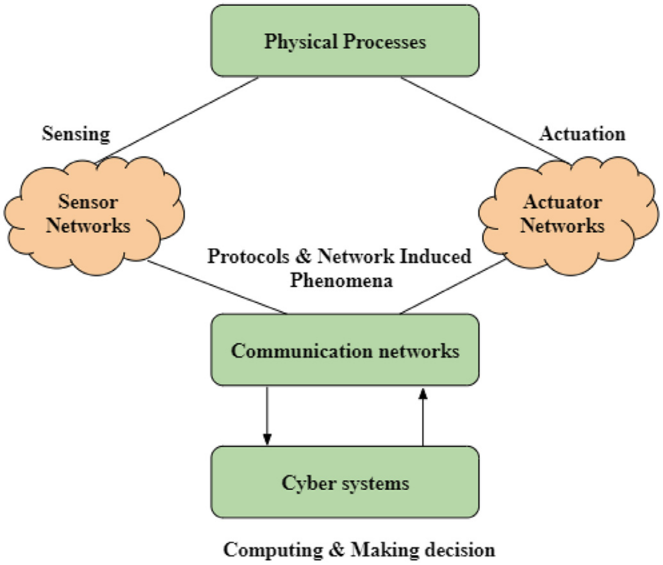

Fig. 5. Basic architecture of CPS.

the existing security protocols. For maintaining the confidentiality and integrity of ICS systems, the security protocols are categorized into technical, operational, and management based techniques, which needs to be integrated for protecting the security of ICS from adversarial attacks [64]. In CPS and ICS, incident response is a highly perplexed and multifaceted problem which affects the performance of existing security solutions. Several researchers have discussed this problem and existing studies are categorized into multiple groups based on their objectives which are formulated according to the guidelines of NIST 800–61 IR stages [65]. This research reviews some of the existing research works which focus majorly on the analysis and detection stage, as summarized in table 7.

Intrusion detection in IIoT

Most of the cyber security experts have proposed the implementation of intrusion detection systems (IDS) to protect dynamic IoT, IIoT systems [73] and its elements such as SCADA, CPS, and ICS from unauthorized entities and attacks. IDSs is considered as an effective solution for preventing attacks from malicious sources. IDS automates the intrusion detection process and provides signs of possible attacks thereby preventing the attacks at an early stage. In order to increase the efficiency of the IDS system, a dynamic approach, which has the capability to detect different types of intrusions with the help of learning algorithms is mostly preferred. Several research works have implemented IDS and intrusion prevention systems (IPS) for securing IIoT systems from potential cybersecurity threats.

The review of existing techniques for developing IDS /IPS for IIoT is presented in Table 8. It can be inferred from the review that machine learning (ML), deep learning (DL), and reinforcement learning (RL) can act as a potential solution for designing IDS to secure IIoT. However, most of the existing solutions are not validated on real-time and larger datasets. This can be a potential research gap and needs to be addressed.

Vulnerability, risk analysis and risk assessment

There are several techniques and methodologies for vulnerability analysis and risk assessment in SCADA/ICS systems. Different risk analysis models have been discussed. The objective of vulnerability and risk analysis is to analyze possible security attacks and identify the weaknesses of the SCADA/ICS systems.

3.5.1 Vulnerability and risk analysis

A four-staged approach is suggested in this research for analyzing the vulnerabilities and risks associated with SCADA/ICS systems towards possible security attacks.

(i) *Identifying vulnerabilities:* After identifying the type of security attack on SCADA/ICS, the vulnerabilities of the system are identified and based on this the data collected is analyzed.
(ii) *Identifying attack methods:* It is important to identify how the security attacks are causing perturbations in the system's operation and how the system is getting affected.
(iii) *Implement immediate risk reduction:* Based on the type of attack and the method, specific risk reduction actions should be taken immediately.
(iv) *Implementation of solution:* There is a need to implement a long-term solution for preventing the SCADA/ICS system from security attacks.

These stages can be considered as a systematic approach for assessing the vulnerabilities and risks. The identification and analysis of different risk reduction scenarios and identification of long-term solutions can be considered for future research works.

Operational technology risk assessment (OTRA)

With the increasing complexity of process control, system architecture, and manufacturing process, it is highly important to identify, prioritize, and mitigate the risks in ICS and SCADA systems [81]. The risks associated with these systems can be accessed to analyze different security threats, and resolve vulnerabilities in ICS and SCADA systems. In addition to the previously identified security threats and requirements that distinguish IT and OT environments, the complex infrastructure and properties of CPS increases the complexity of the risk assessment and risk management process [82]. A modern ICS and SCADA infrastructure incorporates advanced control and monitoring systems to ensure smooth operation and robust security against external threats. In general, ICS and SCADA systems are not directly affected by the cyber-attacks unless and until they are integrated with internet based communication systems or controlled by digital controllers. The integration of complex CPS elements, different control mechanisms (such as analog and electromagnetic controllers), and complicated CPS properties makes it difficult to analyze how the attacker can manipulate the controlling process.

Table 8
Review of IDS/IPS for security of IIoT.

Reference	Type of IDS	Objectives	Limitations
[74]	Machine learning (ML) based IDS	The IDS is developed to detect malicious intrusions in DNP3 layers in SCADA systems	The attack classification accuracy of ML-based IDS is not tested and validated considering different datasets
[75]	Autoencoder based IDS (AE-IDS)	A feature extraction based IDS to monitor network activity in SCADA systems	The effect of data sparsity on the performance of AE-IDS was not tested
[76]	Hybrid IDS based on ML	An effective IDS is developed for edge-based IIoT using lightweight LightGBM algorithm	The model is trained offline, which affects its accuracy and restricts its adaptability for real-time intrusion detection
[77]	Genetic Algorithm (GA) and Random forest (RF) model based IDS	A feature extraction based IDS is implemented to ensure security, privacy and integrity of IIoT	The performance of the GA-RF model is not tested for minority classes of UNSW-NB15 dataset
[78]	A pretraining Wasserstein generative adversarial network intrusion detection system (PWGIDS)	The PWG-IDS is designed to overcome the issue of class imbalance in IIoT systems	The model needs to be pre-trained for each dataset and hence the process becomes computationally intensive and less robust
[79]	Deep Reinforcement Learning (DRL) based IDS	A reinforcement learning is used for developing IDS instead of using supervised or unsupervised learning, in order to improve the decision-making capacity of IDS	The DRL based IDS is implemented for centralized architecture and there is a need to explore the effectiveness of IDS for distributed IIoT networks
[80]	Deep Neural Network (DNN) based IPS	A behavior based IPS is designed for OT networks	The DNN based IPS exhibits performance delay when deployed in real-time environment

This also increases the risks associated with the ICS and SCADA systems from cyber-attacks and makes the system more vulnerable towards the attacks.

The OTRA process in ICS and SCADA systems consists of different activities such as (i) risk assessment (ii) penetration testing and (iii) risk prioritization. The risk assessment is carried out using active and passive techniques. Passive methodologies only observe and collect information without actually considering network traffic of the system. Hence, these methods are more appropriate for assessing the risks in actual ICS architectures. On the other hand, active methods inject traffic into the ICS and SCADA infrastructures in order to identify security threats and analyze the response of the system. Hence, active methods for risk assessment should be implemented carefully in actual systems. The OTRA in ICS/SCADA systems should follow industry specific risk assessment principles and are extensively carried out in three phases:

- Independent technical risk assessment in OT systems
- Conduct a comprehensive risk assessment for functions and processes that are supported by the OT infrastructures.
- Provide ongoing cybersecurity support for OT systems.

Challenges and research gaps

Challenges

Industry 4.0 lacks effective convergence of IT and OT networks at the operational level. As discussed previously, the security requirements of IT and OT in IIoT are different and have to be designed specifically based on the industry constraints. This is exploited by the attackers to introduce malicious attacks such as Denial-of-Service (DoS), distributed DoS (DDoS), unauthorized intrusions etc. Existing research gaps related to IIoT is due to the inclusion of inappropriate security protocols/standards, and interoperability issues. If the applied protocols are assessed explicitly, existing security strategies might fail to detect attacks and threats [10]. The forensic data extraction and the role of digital evidence [83] needs to be explored for strengthening the security of OT networks. Security threats in IIoT, SCADA, ICS, and CPS have been extensively studied in recent times and it can be observed from these studies that existing security solutions fail to achieve desired performance at the operational technology (OT) level [84]. The IDS and other security tools in ICS perform better at the network level and they do not resist potential threats in OT. After identifying the security breach, assessing and mitigating the attacks is another prominent challenge for existing solutions. Some of the major challenges that make SCADA/ICS systems more vulnerable to security threats are as follows:

- Secure extraction of data from ICS/SCADA is a highly complex task that needs to be addressed in IIoT and industry 4.0 applications. The main reason is the outdated and fundamental system architecture that does not emphasize security aspects [85]. In these systems, the data is transmitted without implementing any security approaches.
- Extraction of data from PLCs, sensors, and actuators in ICS/SCADA systems located in remote locations can be challenging due to the incompatibility between IT and OT systems.
- Few commercial systems and technologies such as edge-based IIoTs allow extraction of data from PLCs. However, the security of such extracted data is questionable.

There is a lack of a standard model in the field of digital forensics. Since each IIoT system is developed using different hardware and software platforms, it is challenging to develop a standard forensic framework which is suitable for all IIoT system components. In addition, the large amount of data generated by the IIoT systems and its diverse nature increases the complexity of forensic analysis. Due to the diversity, it is challenging to collect evidence and poses difficulty in communicating and collaborating with different organizations and systems for information sharing. These challenges hinder the performance of forensic tools developed for IIoT/CPS/ICS/SCADA and restricts their effectiveness in responding to incidents and preventing them. These challenges can be addressed by providing quality training to the resources and strengthen their incident response performance. Furthermore, enabling collaboration between multiple organizations might enhance the performance of forensic tools. Addressing these challenges is highly important since it helps the researchers and industrialists to develop potential tools and technologies for securing IIoT environments from cyber-threats. In addition to challenges, this research also identifies some of the prominent research gaps, which are summarized as follows:

Research gaps

- It can be inferred from existing works that there is no standard DFIR approach designed specifically for the security of IIoT of future manufacturing 4.0 processes. This affects the attack detection mechanism and reduces the credibility of digital evidence used in the attack detection process [86].
- Although OT networks are relevant to IIoT components such as ICS/SCADA, it is complex to integrate it with information technologies from a security point of view. This is mainly due to the fact

that the IT network focuses mainly on the security of communication rather than securing the monitoring techniques.
- There is a need for a comprehensive evaluation of forensic solutions developed for IIoT and industry 4.0 processes.

Based on the research gaps, few opportunities for future research are identified. Technological advancements in IIoT can improve the incident response and allows rapid identification and mitigation of security attacks. Automating forensic processes can maximize the performance efficiency of forensic tools and minimize the dependency on manual efforts which leads to cost reduction. Exploring new revenue streams for organizations that develop forensic tools for securing industrial organizations can increase the deployment of DFIR tools for industrial environment. These opportunities can assist the researchers exploring the role of DFIR in securing IIoT and its system components.

Conclusion

This review paper focuses on the implementation of DFIR tools with an emphasis on the security of IIoT, ICS, CPS, and SCADA systems. The study reviews various security techniques for identifying different security threats and potential attacks on IIoT. The study highlights the need for digital forensics in IIoT and its system components. The stages involved in DFIR process and tools used in the malware analysis in SCADA/ICS are discussed in detail. Forensic solutions along with IDS can be used to provide robust security against various malicious attacks since it can handle the resource constrained nature and heterogeneity of IIoT systems. This review also outlines the techniques proposed in existing works and presents a thorough analysis on the implementation of different techniques for developing IDS in order to protect the system against the adversarial attacks. In addition, the study also discusses the methodologies developed for vulnerability analysis and risk assessment in SCADA/ICS systems. Finally, the study also discusses and addresses the challenges and research gaps associated with the implementation of DFIR based security approaches for IoT systems. The challenges and research gaps that are highlighted in this research can be considered as promising research directions for further research in IIoT security. In addition, the practical scenarios and use cases that validate the effectiveness of DFIR in securing IIoT from specific types of attacks can be discussed as a part of future work.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Pranita Binnar reports was provided by Veermata Jijabai Technological Institute. Pranita Binnar reports a relationship with Veermata Jijabai Technological Institute that includes: non-financial support.

CRediT authorship contribution statement

Pranita Binnar: Investigation.

Acknowledgement

We are thankful to the members of COE-CNDS lab, VJTI, Mumbai for providing the platform for conducting the research and for their continuous support during the entire research period. “This work is supported in part by Research Proposal Scheme grant from All India Council for Technical Education under ministry of HRD, Govt. of India, File number 8-Go/RFID/RPS/Policy 1/2017- 18".

References

[1] L.L. Dhirani, T. Newe, Hybrid cloud SLAs for industry 4.0: bridging the gap, Annals of Emerging Technologies in Computing (AETiC), Print ISSN, 2020 2516-0281.
[2] H. Xu, W. Yu, X. Liu, D. Griffith, N. Golmie, On data integrity attacks against industrial Internet of Things, in: 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), IEEE, 2020, pp. 21–28.
[3] W. Glisson, G. Grispos, K.K. Choo, Cybersecurity investigations and digital forensics: mini-track overview, in: Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020.
[4] Y. Yu, R. Chen, H. Li, Y. Li, A. Tian, Toward data security in edge intelligent IIoT, IEEE Netw. 33 (5) (2019) 20–26.
[5] Y. Zhang, H. Huang, L.X. Yang, Y. Xiang, M. Li, Serious challenges and potential solutions for the industrial Internet of Things with edge intelligence, IEEE Netw. 33 (5) (2019) 41–45.
[6] J. Xiong, R. Ma, L. Chen, Y. Tian, Q. Li, X. Liu, Z. Yao, A personalized privacy protection framework for mobile crowdsensing in IIoT, IEEE Trans. Ind. Inf. 16 (6) (2019) 4231–4241.
[7] M. Amoretti, R. Pecori, Y. Protskaya, L. Veltri, F. Zanichelli, A scalable and secure publish/subscribe-based framework for industrial IoT, IEEE Trans. Ind. Inf. 17 (6) (2020) 3815–3825.
[8] J. Farkas, B. Varga, G. Miklós, J. Sachs, in: 5G-TSN Integration Meets Networking Requirements for Industrial Automation, Ericsson: Stockholm, Sweden, 2019, pp. 0014–0171.
[9] R. Prasad, V. Rohokale, Internet of Things (IoT) and machine to machine (M2M) communication, in: Cyber security: The lifeline of Information and Communication Technology, Springer, Cham, 2020, pp. 125–141.
[10] L.L. Dhirani, E. Armstrong, T. Newe, Industrial IoT, cyber threats, and standards landscape: evaluation and roadmap, Sensors 21 (11) (2021) 3901.
[11] J. Sengupta, S. Ruj, S.D. Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT, J. Netw. Comput. Appl. 149 (2020) 102481.
[12] D.G. Pivoto, L.F. de Almeida, R. da Rosa Righi, J.J. Rodrigues, A.B. Lugli, A.M. Alberti, Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: a literature review, J. Manuf. Syst. 58 (2021) 176–192.
[13] H. Xu, W. Yu, D. Griffith, N. Golmie, A survey on industrial Internet of Things: a cyber-physical systems perspective, Ieee access 6 (2018) 78238–78259.
[14] A. Jawad, J. Jaskolka, Analyzing the impact of cyberattacks on industrial control systems using timed automata, in: 2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS), IEEE, 2021, pp. 966–977.
[15] K. Coffey, L.A. Maglaras, R. Smith, H. Janicke, M.A. Ferrag, A. Derhab, A. Yousaf, Vulnerability assessment of cyber security for SCADA systems, in: Guide to Vulnerability Analysis for Computer Networks and Systems, Springer, Cham, 2018, pp. 59–80.
[16] F. Zhang, H.A.D.E. Kodituwakku, J.W. Hines, J. Coble, Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data, IEEE Trans. Ind. Inf. 15 (7) (2019) 4362–4369.
[17] M.R. Asghar, Q. Hu, S. Zeadally, Cybersecurity in industrial control systems: issues, technologies, and challenges, Comput. Netw. 165 (2019) 106946.
[18] J. Rak, D. Hutchison (Eds.), Guide to Disaster-Resilient Communication Networks, Springer Nature, 2020.
[19] B. Craggs, A. Rashid, C. Hankin, R. Antrobus, O. Şerban, N. Thapen, A reference architecture for IIoT and industrial control systems testbeds, in: Living in the Internet of Things (IoT 2019), IET, 2019, pp. 1–8.
[20] A. Moradbeikie, K. Jamshidi, A. Bohlooli, J. Garcia, X. Masip-Bruin, An IIoT based ICS to improve safety through fast and accurate hazard detection and differentiation, IEEE access 8 (2020) 206942–206957.
[21] T. Bakhshi, Forensic of Things: revisiting digital forensic investigations in Internet of Things, in: 2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST), IEEE, 2019, pp. 1–8.
[22] V.V.R.G. Saigopal, V. Raju, IIOT digital forensics and major security issues, in: 2020 International Conference on Computational Intelligence (ICCI), IEEE, 2020, pp. 233–236.
[23] Q. Li, Q. Tang, I. Chan, H. Wei, Y. Pu, H. Jiang, J. Zhou, Smart manufacturing standardization: architectures, reference models and standards framework, Comput. Ind. 101 (2018) 91–106.
[24] K. Tange, M. De Donno, X. Fafoutis, N. Dragoni, A systematic survey of industrial Internet of Things security: requirements and fog computing opportunities, IEEE Commun. Surv. Tutor. 22 (4) (2020) 2489–2520.
[25] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial internet of things: challenges, opportunities, and directions, IEEE Trans. Ind. Inf. 14 (11) (2018) 4724–4734.
[26] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, A. Urbieta, Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0, J. Manuf. Syst. 57 (2020) 367–378.
[27] O. Givehchi, K. Landsdorf, P. Simoens, A.W. Colombo, Interoperability for industrial cyber-physical systems: an approach for legacy systems, IEEE Trans. Ind. Inf. 13 (6) (2017) 3370–3378.
[28] L. Jänicke, Secure communication for Industrie 4.0, at-Automatisierungstechnik 67 (5) (2019) 364–371.
[29] S. Hilt, F. Maggi, C. Perine, L. Remorin, M. Rösler, R. Vosseler, Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats, Trend Micro, Shibuya City, Japan, White Paper, 2020.
[30] A. Cotrino, M.A. Sebastián, C. González-Gaya, Industry 4.0 Roadmap: implementation for small and medium-sized enterprises, Appl. Sci. 10 (23) (2020) 8566.
[31] N. Boltz, M. Walter, R. Heinrich, Context-based confidentiality analysis for industrial iot, in: 2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), IEEE, 2020, pp. 589–596.

[32] C. Lupascu, A. Lupascu, I. Bica, DLT Based Authentication Framework for Industrial IoT Devices, Sensors 20 (9) (2020) 2621.

[33] A.Y.F. Alsahlani, A. Popa, Analysis of lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT, in: 2021 International Wireless Communications and Mobile Computing (IWCMC), IEEE, 2021, pp. 475–480.

[34] M. El-Hajj, A. Fadlallah, M. Chamoun, A. Serhrouchni, A survey of internet of things (IoT) authentication schemes, Sensors 19 (5) (2019) 1141.

[35] M. La Manna, P. Perazzo, M. Rasori, G Dini, Fabelous: an attribute-based scheme for industrial internet of things, in: 2019 IEEE International Conference on Smart Computing (SMARTCOMP), IEEE, 2019, pp. 33–38.

[36] N. Abosata, S. Al-Rubaye, G. Inalhan, C. Emmanouilidis, Internet of things for system integrity: a comprehensive survey on security, attacks and countermeasures for industrial applications, Sensors 21 (11) (2021) 3654.

[37] S. Plaga, N. Wiedermann, S.D. Anton, S. Tatschner, H. Schotten, T. Newe, Securing future decentralised industrial IoT infrastructures: challenges and free open source solutions, Future Generat. Comput. Syst. 93 (2019) 596–608.

[38] W. Li, P. Wang, Two-factor authentication in industrial Internet-of-Things: attacks, evaluation and new construction, Future Generat. Comput. Syst. 101 (2019) 694–708.

[39] E. Lara, L. Aguilar, M.A. Sanchez, J.A. García, Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial Internet of Things, Sensors 20 (2) (2020) 501.

[40] Y. Zhao, J. Yang, Y. Bao, H. Song, Trustworthy Authorization Method for Security in Industrial Internet of Things, 121, Ad Hoc Networks, 2021.

[41] M. Serror, S. Hack, M. Henze, M. Schuba, K. Wehrle, Challenges and opportunities in securing the industrial internet of things, IEEE Trans. Ind. Inf. 17 (5) (2020) 2985–2996.

[42] S. Forsström, I. Butun, M. Eldefrawy, U. Jennehag, M. Gidlund, Challenges of securing the industrial internet of things value chain, in: 2018 Workshop on Metrology for Industry 4.0 and IoT, IEEE, 2018, pp. 218–223.

[43] M. Lezzi, M. Lazoi, A. Corallo, Cybersecurity for Industry 4.0 in the current literature: a reference framework, Comput. Ind. 103 (2018) 97–110.

[44] L. Thames, D. Schaefer, in: Cybersecurity for Industry 4.0, Springer, Heidelberg, 2017, pp. 1–33.

[45] M. Javaid, A. Haleem, R.P. Singh, S. Rab, R. Suman, Upgrading the manufacturing sector via applications of industrial internet of things (IIoT), Sensor. Int. 2 (2021) 100129.

[46] R. Sethi, B. Bhushan, N. Sharma, R. Kumar, I. Kaushik, in: Applicability of Industrial IoT in Diversified sectors: evolution, Applications and Challenges, Multimedia technologies in the Internet of Things environment, 2021, pp. 45–67.

[47] V.V.R. Gudlur, V.A. Shanmugan, S. Perumal, R.M.S.R. Mohammed, Industrial internet of things (iiot) of forensic and vulnerabilities, Int. J. Recent Technol. Eng. (2020).

[48] N. Koroniotis, N. Moustafa, E. Sitnikova, A new network forensic framework based on deep learning for Internet of Things networks: a particle deep framework, Future Generat. Comput. Syst. 110 (2020) 91–106.

[49] V. Mothukuri, P. Khare, R.M. Parizi, S. Pouriyeh, A. Dehghantanha, G. Srivastava, Federated-learning-based anomaly detection for IoT security attacks, IEEE IoT J. 9 (4) (2021) 2545–2554.

[50] G.D.L.T. Parra, P. Rad, K.K.R. Choo, Implementation of deep packet inspection in smart grids and industrial Internet of Things: challenges and opportunities, J. Netw. Comput. Appl. 135 (2019) 32–46.

[51] H. Al-Aqrabi, R. Hill, Evaluating multi-layer security resistance to adversarial hacking attacks on industrial internet of things devices, in: Digital Forensic Investigation of Internet of Things (IoT) Devices, Springer International Publishing, Cham, 2020, pp. 187–203.

[52] A. Poletykin, Cyber security risk assessment method for SCADA of industrial control systems, in: 2018 International russian automation conference (RusAutoCon), IEEE, 2018, pp. 1–5.

[53] P. Eden, A. Blyth, K. Jones, H. Soulsby, P. Burnap, Y. Cherdantseva, K. Stoddart, SCADA system forensic analysis within IIoT, in: Cybersecurity for Industry 4.0, Springer, Cham, 2017, pp. 73–101.

[54] A. Sajid, H. Abbas, K. Saleem, Cloud-assisted IoT-based SCADA systems security: a review of the state of the art and future challenges, IEEE Access 4 (2016) 1375–1384.

[55] R.A. Awad, S. Beztchi, J.M. Smith, B. Lyles, S. Prowell, Tools, techniques, and methodologies: a survey of digital forensics for scada systems, in: Proceedings of the 4th Annual Industrial Control System Security Workshop, 2018, pp. 1–8.

[56] I. Ahmed, S. Obermeier, S. Sudhakaran, V. Roussev, Programmable logic controller forensics, IEEE Secur Priv 15 (6) (2017) 18–24.

[57] M. Elhoseny, A.E. Hassanien, M. Elhoseny, A.E. Hassanien, in: Using Wireless Sensor to Acquire Live Data on a SCADA system, Towards Monitoring File Integrity, Dynamic Wireless Sensor Networks: New Directions for Smart Technologies, 2019, pp. 171–191.

[58] P. Eden, A. Blyth, P. Burnap, Y. Cherdantseva, K. Jones, H. Soulsby, K. Stoddart, A cyber forensic taxonomy for scada systems in critical infrastructure, in: Critical Information Infrastructures Security: 10th International Conference, CRITIS 2015, Springer International Publishing, Berlin, Germany, 2016, pp. 27–39. October 5-7, 2015, Revised Selected Papers 10.

[59] P. Eden, A. Blyth, P. Burnap, Y. Cherdantseva, K. Jones, H. Soulsby, A forensic taxonomy of SCADA systems and approach to incident response, in: 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015), 3, 2015, pp. 42–51.

[60] G.D. Pamnani, P. Saxena, Incident handling in SCADA & OT environments, Water Energy Int. 66 (3) (2023) 28–35.

[61] R. Udd, M. Asplund, S. Nadjm-Tehrani, M. Kazemtabrizi, M. Ekstedt, Exploiting bro for intrusion detection in a SCADA system, in: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, 2016, pp. 44–51.

[62] R. Schlegel, A. Hristova, S. Obermeier, A framework for incident response in industrial control systems, in: 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE), 4, IEEE, 2015, pp. 178–185.

[63] J. Stirland, K. Jones, H. Janicke, T. Wu, Developing cyber forensics for SCADA industrial control systems, in: Proceedings of the International Conference on Information Security and Cyber Forensics, Kuala Terengganu, Malaysia, Universiti Sultan Zainal Abidin, 2014.

[64] P. Binnar, A. Dalvi, S. Bhirud, F. Kazi, Cyber forensic case study of waste water treatment plant, in: 2021 IEEE Bombay Section Signature Conference (IBSSC), IEEE, 2021, pp. 1–5.

[65] M. Khadpe, P. Binnar, F. Kazi, Malware injection in operational technology networks, in: 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2020, pp. 1–6.

[66] N. Dutta, K. Tanchak, K. Delvadia, Modern methods for analyzing malware targeting control systems, Recent Dev. Ind. Control Syst. Resilience (2020) 135–150.

[67] M. Gaiceanu, M. Stanculescu, P.C. Andrei, V. Solcanu, T. Gaiceanu, H. Andrei, Intrusion detection on ics and scada networks, in: Recent Developments on Industrial Control Systems Resilience, Springer, Cham, 2020, pp. 197–262.

[68] A. Humayed, J. Lin, F. Li, B. Luo, Cyber-physical systems security—a survey, IEEE Internet of Things Journal 4 (6) (2017) 1802–1831.

[69] Y. Ashibani, Q.H. Mahmoud, Cyber physical systems security: analysis, challenges and solutions, Computers & Security 68 (2017) 81–97.

[70] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, C. Maple, Cyber resilience and incident response in smart cities: a systematic literature review, Smart Cities 3 (3) (2020) 894–927.

[71] National Institute of Standards and Technology NIST, in: Computer Security Incident Handling Guide, NIST, Gaithersburg, MD, USA, 2004, p. 148. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Available online.

[72] M.R. Belgaum, Z. Alansari, R. Jain, J. Alshaer, A framework for evaluation of cyber security challenges in smart cities, in: Smart Cities Symposium 2018, IET, 2018, pp. 1–6.

[73] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique, E. Bartocci, A roadmap toward the resilient internet of things for cyber-physical systems, IEEE Access 7 (2019) 13260–13283.

[74] N. Moustafa, E. Adi, B. Turnbull, J. Hu, A new threat intelligence scheme for safeguarding industry 4.0 systems, IEEE Access 6 (2018) 32910–32924.

[75] Y. Wang, G. Yan, A new model approach of electrical cyber physical systems considering cyber security, IEEJ Trans. Electric. Electron. Eng. 14 (2) (2019) 201–213.

[76] F. Li, Y. Shi, A. Shinde, J. Ye, W. Song, Enhanced cyber-physical security in internet of things through energy auditing, IEEE IoT J. 6 (3) (2019) 5224–5231.

[77] L. Vegh, Cyber-physical systems security through multi-factor authentication and data analytics, in: 2018 IEEE International Conference on Industrial Technology (ICIT), IEEE, 2018, pp. 1369–1374.

[78] E. Anthi, S. Ahmad, O. Rana, G. Theodorakopoulos, P. Burnap, EclipseIoT: a secure and adaptive hub for the Internet of Things, Comput. Secur. 78 (2018) 477–490.

[79] K. Tsiknas, D. Taketzis, K. Demertzis, C. Skianis, Cyber threats to industrial IoT: a survey on attacks and countermeasures, IoT 2 (1) (2021) 163–186.

[80] X.C. Yin, Z.G. Liu, L. Nkenyereye, B. Ndibanje, Toward an applied cyber security solution in IoT-based smart grids: an intrusion detection system approach, Sensors 19 (22) (2019) 4952.

[81] M. Altaha, J.M. Lee, M. Aslam, S. Hong, An autoencoder-based network intrusion detection system for the SCADA system, J. Commun. 16 (6) (2021) 210–216.

[82] H. Yao, P. Gao, P. Zhang, J. Wang, C. Jiang, L. Lu, Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection, IEEE Netw. 33 (5) (2019) 75–81.

[83] S.M. Kasongo, An advanced intrusion detection system for IIoT based on GA and tree based algorithms, IEEE Access 9 (2021) 113199–113212.

[84] L. Zhang, S. Jiang, X. Shen, B.B. Gupta, Z. Tian, PWG-IDS: An Intrusion Detection Model for Solving Class Imbalance in IIoT Networks Using Generative Adversarial Networks, arXiv preprint, 2021 *arXiv:2110.03445*.

[85] S. Tharewal, M.W. Ashfaque, S.S. Banu, P. Uma, S.M. Hassen, M. Shabaz, Intrusion detection system for industrial Internet of Things based on deep reinforcement learning, Wirel. Commun. Mobile Comput. (2022) 2022.

[86] A. Rajapkar, P. Binnar, F. Kazi, Design of intrusion prevention system for ot networks using deep neural networks, in: 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2020, pp. 1–6.