4-1-2024

Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures

Iqbal H. Sarker
Edith Cowan University

Helge Janicke
Edith Cowan University

Mohamed A. Ferrag

Alsharif Abuadbba

10.1016/j.iot.2024.101110

Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbba, A. (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures. Internet of Things, 25, article 101110. https://doi.org/10.1016/j.iot.2024.101110

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Review article

Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures

Iqbal H. Sarker [a,b,*], Helge Janicke [a,b], Mohamed Amine Ferrag [c], Alsharif Abuadbba [d]

[a] *Centre for Securing Digital Futures, Edith Cowan University, Perth, 6027, WA, Australia*
[b] *Cyber Security Cooperative Research Centre, Perth, 6027, WA, Australia*
[c] *Technology Innovation Institute, Masdar City, Abu Dhabi, United Arab Emirates*
[d] *Data61, CSIRO, Sydney, 2122, NSW, Australia*

ARTICLE INFO

Keywords:
Cybersecurity
Rule-based Modeling
Explainable AI
Responsible AI
Machine learning
Security data analytics
Knowledge discovery
Data-driven decision-making
Automation
Intelligence
Transparency
Trustworthiness
Critical infrastructures

ABSTRACT

Critical infrastructure (CI) typically refers to the essential physical and virtual systems, assets, and services that are vital for the functioning and well-being of a society, economy, or nation. However, the rapid proliferation and dynamism of today's cyber threats in digital environments may disrupt CI functionalities, which would have a debilitating impact on public safety, economic stability, and national security. This has led to much interest in effective cybersecurity solutions regarding *automation* and *intelligent decision-making*, where AI-based modeling is potentially significant. In this paper, we take into account *"Rule-based AI"* rather than other black-box solutions since model *transparency*, i.e., human interpretation, explainability, and trustworthiness in decision-making, is an essential factor, particularly in cybersecurity application areas. This article provides an in-depth study on multi-aspect rule based AI modeling considering human interpretable decisions as well as security automation and intelligence for CI. We also provide a *taxonomy* of rule generation methods by taking into account not only knowledge-driven approaches based on human expertise but also data-driven approaches, i.e., extracting insights or useful knowledge from data, and their hybridization. This understanding can help security analysts and professionals comprehend how systems work, identify potential threats and anomalies, and make better decisions in various real-world application areas. We also cover how these techniques can address diverse cybersecurity concerns such as threat detection, mitigation, prediction, diagnosis for root cause findings, and so on in different *CI sectors*, such as energy, defence, transport, health, water, agriculture, etc. We conclude this paper with a list of identified *issues and opportunities* for future research, as well as their potential solution directions for how researchers and professionals might tackle future generation cybersecurity modeling in this emerging area of study.

1. Introduction

Critical infrastructure refers to the physical and virtual systems, services, and assets that are essential for the functioning of a society, economy, or organization. According to the Australian Cyber and Infrastructure Security Centre [1], Critical infrastructure is defined as: "those physical facilities, systems, assets, supply chains, information technologies, and communication networks which,

[*] Corresponding author at: Centre for Securing Digital Futures, Edith Cowan University, Perth, 6027, WA, Australia.
E-mail address: m.sarker@ecu.edu.au (I.H. Sarker).

https://doi.org/10.1016/j.iot.2024.101110
Received 10 September 2023; Received in revised form 29 January 2024; Accepted 2 February 2024
Available online 5 February 2024

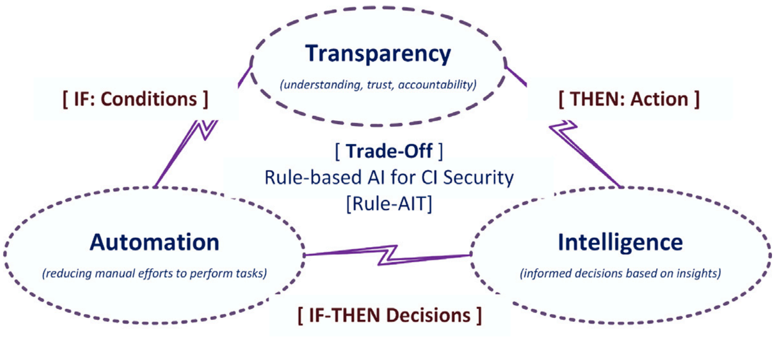
Transparency
(understanding, trust, accountability)
[IF: Conditions]
[THEN: Action]
[Trade-Off]
Rule-based AI for CI Security
[Rule-AIT]
Automation
(reducing manual efforts to perform tasks)
Intelligence
(informed decisions based on insights)
[IF-THEN Decisions]

Fig. 1. An illustration of the key aspects — Automation (A), Intelligence (I), and Transparency (T) of rule-based AI (RuleAIT) for CI Security Modeling, where IF-THEN decisions are taken into account for human understanding and decision explanation.

if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of Australia as a nation or its states or territories, or affect Australia's ability to conduct national defense and ensure national security". Thus, cybersecurity for critical infrastructure should be a nation's top concern because the disruption and destruction of these infrastructures would have a debilitating impact on public safety, economic stability, and national security. However, cyber security is a growing challenge in the digital age as cyber threats evolve and become more sophisticated. Thus, traditional security measures are often insufficient to defend against today's dynamic and persistent threats [2,3]. Therefore, it is crucial to take into account *automation* and *intelligence* in decision-making, as well as model *transparency* for human interpretation with explainability that can meet today's needs in this area of CI security.

Recent advances in artificial intelligence (AI) such as data science (DS) modeling and machine learning (ML) techniques, have drastically changed how we analyze data and use the extracted knowledge for automation and intelligent decision-making in various real-world application domains, including cybersecurity applications [4,5]. Although several black-box approaches like deep neural network learning, large language modeling have strong computing capabilities, human-understandable explanations, and trustworthiness are essential in deploying responsible AI-based models to solve CI security issues [6]. Thus, developing more *transparent* and *human interpretable* AI models, particularly for cyber analysts, could be more effective for cybersecurity solutions. To support this statement, in this paper, we explore rule-based AI modeling in the broad area of "cybersecurity and AI" where patterns, dependencies, or interpretable knowledge are discovered from data, which could be useful not only for model building but also resolving the black-box issues of traditional AI modeling in many application areas.

1.1. Why knowledge discovery and rule-based AI modeling?

In cybersecurity, knowledge discovery and rule mining-based AI modeling typically involves analyzing security data to uncover hidden patterns and relationships, helping to identify potential security threats that may not be covered by manual or traditional approaches. By extracting insights into patterns and anomalies that may not be apparent using manual solutions, previously unknown threats and vulnerabilities can be discovered. These models are also capable of adapting to new and emerging threats by continuously analyzing recent data and learning from patterns, which makes them more resilient to dynamic cybersecurity trends. With a better understanding of context and relationships within data, these models can reduce false positives and negatives, which eventually helps to build a more powerful model according to today's needs. Knowledge and rules discovered from relevant data can therefore play an important role in detecting, mitigating, and predicting the potential threats with outcome explanation. Cyber threats can also be diagnosed transparently by examining the dependencies and relationships between entities in rules derived from data. Thus, the discovered knowledge and rule-based AI modeling facilitates key features like automation, intelligence, and transparency according to today's need for cybersecurity modeling. These are defined below and can be represented by the acronym "RuleAIT", as shown in Fig. 1.

- *Automation* - the capability to perform tasks without manual intervention or reduce the need for human intervention through executing the generated rules.
- *Intelligence* - the capability of rule-based modeling for informed decision-making based on the discovered knowledge and automatic learning patterns and useful insights extracted from security data.
- *Transparency and Trust* - transparency typically refers to model visibility such as rule structure and understanding of how the model makes decisions through the generated rules. Today's cybersecurity relies heavily on this transparency to build trust, facilitate human oversight, and ensure accountability, which is the foundation of explainable and responsible AI development.

To make a decision in a certain situation, a rule is typically structured and generated as "$IF[`antecedent'] => THEN[`consequent']$" statement, where "antecedent" represents necessary security attributes, conditions or contextual situations, and "consequent" represents the corresponding action. Various techniques including machine learning and data science processes to discover this

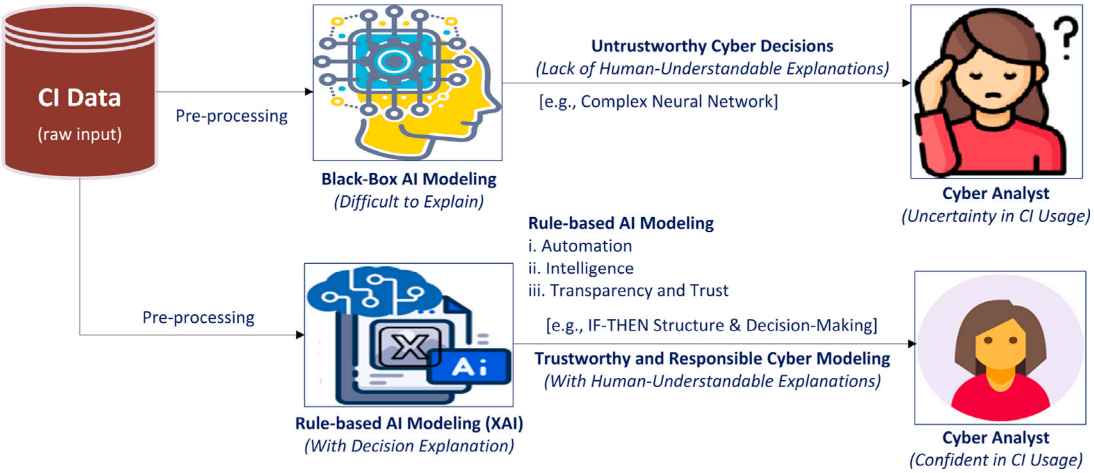
CI Data
(raw input)
Pre-processing
Black-Box AI Modeling
(Difficult to Explain)
Untrustworthy Cyber Decisions
(Lack of Human-Understandable Explanations)
[e.g., Complex Neural Network]
Cyber Analyst
(Uncertainty in CI Usage)
Rule-based AI Modeling
i. Automation
ii. Intelligence
iii. Transparency and Trust
Pre-processing
[e.g., IF-THEN Structure & Decision-Making]
Trustworthy and Responsible Cyber Modeling
(With Human-Understandable Explanations)
Rule-based AI Modeling (XAI)
(With Decision Explanation)
Cyber Analyst
(Confident in CI Usage)

Fig. 2. A motivational scenario highlighting Rule-based AI modeling vs Black-Box solutions from the perspective of a CI cyber analyst.

knowledge and relationships are discussed briefly in Fig. 3. Thus, it is much easier for human analysts to understand the logic behind a decision in a particular situation. This can help analysts and security professionals comprehend how the system functions, identify potential vulnerabilities and threats and ultimately make the best actionable decisions to address them in the CI environment successfully.

Another significant advantage of rule-based modeling is its flexibility in modeling such as rule addition, i.e., incorporating new knowledge, rule removal, i.e., deleting outdated rules, and rule updating, i.e., ensuring recent data patterns known as recency or data freshness to keep the knowledge up to date. Eventually, managing the whole system at the application level is easier and more transparent, which facilitates explaining the outcome. We also illustrate a motivating scenario highlighting the potential of RuleAIT from the perspective of a cyber analyst at the application level in Fig. 2. This paper aims to explore an in-depth study on multi-aspect rule-based AI modeling, where we take into account both the knowledge-driven approaches, i.e., based on human domain knowledge and expertise, and data-driven approaches, i.e., discovering useful knowledge or insights from data, as well as their hybridization for effective CI security solutions, discussed briefly in Section 4.

1.2. Related surveys and our contributions

Throughout the last few years, surveys focusing on CI security have typically been conducted emphasizing cybersecurity attacks, risks, and SCADA systems. For instance, Touhiduzzaman et al. [7] conducted a review of cybersecurity risk for CI. Stellios et al. [8] explore IoT-enabled attacks and mitigation in CI. Kayan et al. [9] explored ICPS security including IT and OT. A study on privacy-oriented attacks for CI has been conducted by Husnoo et al. [10]. Bhamare et al. [11] present a study on SCADA cyber security. These surveys provide important insights and valuable lessons for the academic and industrial realms, particularly in cyber attacks for CI. However, AI-based solutions, particularly knowledge discovery and rule-based AI modeling for CI security, are still under-addressed in this area. Recently, Koay et al. [12] presented a study on ML methods in ICS security. More related works are summarized in Table 2. However, an in-depth study and analysis of rule-based AI modeling with their transparency and explainable capabilities, taking into account "RuleAIT" is needed to comprehend its potential uses in cybersecurity modeling for CI.

To gain a deeper understanding of the cyber community and to explore the main focus of this article, we formulate the following five important questions:

(i) Are automation, intelligence, and transparent modeling necessary for next-generation cybersecurity solutions for critical infrastructure?
(ii) Which characteristics and structural advantages do rule-based AI modeling have that help to simplify the end product and are eventually beneficial to human users?
(iii) How to generate multi-aspect rules, such as knowledge-driven, data-driven, and their hybridization with the capability to address the wide range of threats?
(iv) Is the discovered knowledge and rule-based AI modeling applicable to resolve diverse cyber issues in different CI sectors like energy, water, health, agriculture, etc.? Also, how can rule-based AI methods lead to?
(v) What are the biggest challenges that knowledge discovery and rule-based methods face when addressing cyber issues, and how can scientists and researchers overcome those challenges in this particular CI area of study?

To establish the foundation for our contribution, we intend to explore these crucial topics from the perspective of knowledge discovery and rule-based AI modeling and their applicability in diverse real-world application areas of CI. To the best of our

Table 1
List of key acronyms.

Acronyms	Meaning
AI	Artificial Intelligence
XAI	Explainable Artificial Intelligence
AIT	Automation, Intelligence and Transparency
ML	Machine learning
DL	Deep learning
DNN	Deep Neural Network
KDD	Knowledge Discovery from Data
DDR	Data-Driven Rules
DDDM	Data-Driven Decision Making
NLP	Natural Language Processing
LLM	Large Language Model
CIA	Confidentiality, Integrity and Availability
CPS	Cyber–Physical Systems
CI	Critical Infrastructure
DDoS	Distributed Denial-of-service
DoS	Denial-of-service
IDS	Intrusion Detection System
IoT	Internet-of-Things
SIEM	Security Information and Event Management
SOC	Security Operation Centre
QoS	Quality-of-Services
IT	Information Technology
OT	Operational Technology
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controllers
DCS	Distributed Control System
IIoT	Industrial Internet of Things
ICPS	Industrial Cyber-Physical System
ICS	Industrial Control System

knowledge, this study represents the first attempt to present an in-depth analysis and discussion for CI security modeling by considering multi-aspect of rule-based AI, such as knowledge-driven, data-driven, and their hybridization for future enhancements of CI cyberspace.

Overall, our specific contributions are as follows:

- We review and compare the existing literature to determine the focus of our article on automation, intelligence, and transparent modeling from the perspective of CI security.
- We highlight and discuss the possible threats and anomalies in the context of critical infrastructure that are needed to mitigate.
- We present a taxonomy of multi-aspect rule-based AI methods that can contribute to cybersecurity modeling and discuss their computing capabilities and potentiality accordingly. We also highlight and explore diverse aspects of these methods in the context of cybersecurity.
- We explore real-world CI usage scopes of rule-based AI modeling in various application areas ranging from anomaly detection to mitigation and response. We also discuss how these methods can play a key role in solving diverse cyber issues in different CI sectors such as energy, water, transportation, agriculture, defense, etc.
- We identify and summarize several key challenges and research issues that need to be addressed for further enhancement in this emerging study area. We also provide possible research directions for next-generation cybersecurity modeling in the critical infrastructure environment.

1.3. Paper structure

The remainder of this article is structured as follows. Section 2 provides an overview of the related technology background, including critical infrastructure, cybersecurity, and rule-based AI, as well as existing literature and the scope of this paper. Section 3 highlights and discusses possible threats and anomalies of CI. An in-depth analysis of rule-based AI methods for cybersecurity modeling and their taxonomy has been presented in Section 4. Section 5 discusses various CI sectors and how these methods can contribute. Several research challenges and prospects highlighting potential solution directions have been outlined in Section 6. Section 7 summarizes some key points of our study, and finally, Section 8 concludes this paper. In addition, Table 1 listed the acronyms and their definitions used throughout this article.

Table 2
Previous survey comparison by taking into account ten key aspects relevant to this paper.

Aspects / Papers	RuleAIT Aspects	CI Threats and Risks	Human-Expert Rules	Data-Driven Rules	Ensemble Rules	Rule-based XAI in CI	Rule-based Taxonomy	Rule-based CI Usage	Challenges and Research Issues	Future Directions and Prospects	Remarks
Touhiduzzaman et al. [7], 2019	x	✓*	x	x	x	x	x	x	*	x	A review of cybersecurity risk for CI
Stellios et al. [8], 2018	x	✓*	x	x	x	x	x	x	✓	✓	Exploring IoT-enabled attacks and mitigation in CI
Kayan et al. [9], 2022	x	✓*	x	x	x	x	x	x	✓	✓	Exploring ICPS security including IT and OT
Husnoo et al. [10], 2021	x	✓*	x	x	x	x	x	x	✓	✓	Exploring privacy-oriented attacks for CI
Nazir et al. [13], 2017	x	✓*	x	*	x	x	x	*	✓	✓	A Study on SCADA cyber security
Bhamare et al. [11], 2020	x	*	x	✓	x	x	x	*	✓	✓	A study on SCADA cyber security
Das et al. [14], 2020	x	✓	x	x	x	x	x	x	✓	✓	A study on smart grid resilience
Wells et al. [15], 2022	x	✓	x	x	x	x	x	x	✓	✓	Review on CI resilience under compounding threats
Liu et al. [15], 2020	x	✓	x	x	x	x	x	x	✓	✓	Study on urban CI networks resilience
Ten et al. [16], 2010	x	✓	✓	x	x	x	x	*	✓	✓	Study on CI attack and defense modeling
Liu et al. [17], 2019	x	✓	x	x	x	x	x	x	*	✓	Study on IoT-based smart-world CI
Yadav et al. [18], 2021	x	✓	*	*	x	x	x	*	*	✓	Study on security of SCADA systems
Koay et al. [12], 2023	x	✓	*	✓	x	x	x	*	✓	✓	Study on ML methods in ICS security
Liu et al. [19], 2021	x	*	*	✓	x	✓	x	*	*	*	Study on rule-based IDS in smart grids
This paper (Sarker et al.)	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	An in-depth study on rule-based CI Security modeling focusing diverse cyber issues in CI, taxonomies, cyber usage scopes of different CI sectors, challenges, research directions from the perspective of RuleAIT (Automation-Intelligence-Transparency).

[Symbol Used: High Coverage (✓*), Mid Coverage (✓), Low Coverage (*) and No Coverage (x)].

2. State-of-the-art

In this section, we first explore the background that includes critical infrastructure (Section 2.1), cybersecurity in CI (Section 2.2), and rule-based AI-enhanced cybersecurity in CI (Section 2.3). We then review the related surveys within the scope of our study and discuss the key differences between our paper and the existing survey papers (Section 2.4) to identify the study gap in this area.

2.1. Critical infrastructure

The term "critical infrastructure" refers to the physical and virtual systems, networks, and assets essential for a society's and the economy's functioning. IT (Information Technology) and OT (Operational Technology) are crucial for CI. The term "IT" typically refers to the standard computing systems used for data processing, storage, and communication within organizations. Examples include servers, desktop computers, laptops, network devices, and software applications. On the other hand, the term "OT" typically refers to the hardware and software systems used for monitoring and controlling physical operations in various CI sectors, including energy, manufacturing, transportation, water, and so on. Some examples of OT systems include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Industrial Control Systems (ICS), Programmable Logic Controllers (PLCs), etc. [9,16]. These infrastructures provide vital services and support to ensure the smooth operation of various sectors and the well-being of a nation's population. Energy, Transportation, Communication, Water, Defence, etc., are examples under this area, discussed briefly in Section 5. These critical infrastructure sectors are interconnected and rely on each other to function correctly. However, CI is also vulnerable to disasters or threats, as it can have a direct impact on society [20,21]. They are critical because their disruption or destruction can severely affect public safety, national security, economic stability, and public health. While IT systems are responsible for data management and communication, OT systems control the physical processes that manage essential services. Thus, protecting and securing these infrastructures from physical and cyber threats is crucial for maintaining a nation's overall well-being and stability.

2.2. Cybersecurity and critical infrastructure

Cybersecurity typically involves a wide range of measures and technologies designed to protect digital assets, prevent cyber threats, and ensure data confidentiality, integrity, and availability [4,22]. In the real world digital space, cybercriminals have become more sophisticated, making it insufficient to defend the systems and react to real-time attacks. The evolution of computer crime towards the use of ICT and AI technologies can be defined below.

- *Computer crime* - generally refers to any illegal activity that involves the use of a computer or a computing device.
- *Cyber crime* - a more specific term that focuses on criminal activities conducted over the internet or other computer networks.
- *AI crime* - criminal activities that involve the use of AI. Cybercriminals can also use AI and machine learning to find new and innovative ways for malicious purposes, i.e., to automate attacks, evade detection by security systems, and similar others [23,24].

Thus, cybersecurity is crucial for protecting CI from cyber threats and ensuring its reliable and secure operation. As more CI systems become interconnected and digitized, they become potential targets for malicious actors seeking to disrupt or damage essential services. The consequences of successful cyberattacks on critical infrastructure can be significant, including financial losses, public safety risks, and national security implications, and thus essential to ensure the security of CI to protect against cyber threats, discussed briefly in Section 3.

2.3. Rule-based AI-enhanced cybersecurity in critical infrastructures

Rule-based AI-enhanced cybersecurity for critical infrastructure typically aims to protect this infrastructure from cyber threats according to the discovered knowledge from CI data and the rules generated and selected for execution. Thus, this approach may combine the advantages of traditional rule-based systems with AI capabilities, including data science and machine learning methods [5] to detect and respond to cyber threats more effectively. In addition, the rule-based models are updated to incorporate new knowledge and enhance their functionality based on feedback and evaluation outcomes. This can involve various strategies, including:

- *Rule Addition:* To capture recently discovered threats, novel attack patterns, or anomalies that have not been observed before, new rules can be introduced to the existing rule set. Based on the knowledge discovered from the updated information analysis, several new rules can be created.
- *Rule Updating:* Existing rules may need to be updated or refined based on feedback or changes in the cybersecurity landscape. This can involve adjusting rule conditions, weights, and thresholds or incorporating new features to enhance the accuracy and relevance of the rules.
- *Rule Removal:* In some cases, rules no longer practical or relevant may need to be removed from the rule set to prevent false positives or improve system efficiency. Regular evaluation and feedback help identify rules that are outdated or have become obsolete.

Thus, rule-based AI-enhanced cybersecurity is crucial not only in protecting CI environments from cyber threats through its adaptive capability but also in making the systems automated, intelligent, and transparent, as defined in Section 1. In this context, “Adaptive” can be defined as the characteristics of rule-based AI modeling in terms of incorporating new knowledge, outdated removal, and recency-based updating or data freshness in modeling, which helps to make the model up-to-date and more effective. In our context of the study, the term “transparency” typically refers to visibility and understanding of how the model makes decisions, e.g., IF-THEN structure of rules, which is easier to interpret. Thus this element of rule-based AI modeling helps to build trust, facilitate human oversight, and ensure accountability, which is the foundation of explainable and responsible AI development. Researchers often use the words “explainable”, “interpretable”, “trustable”, “reliable”, “accountable”, “responsible” or similar others interchangeably in different contexts of AI development, where rule-based transparent AI modeling could be the key. Various types of rule-based AI techniques for cybersecurity modeling within the context of our study are discussed in Section 4.

2.4. Related surveys, comparison, and study scope

A comparison of related surveys is presented in Table 2. For this, we first consider ten relevant key aspects, as shown in Table 2, to make the position of this paper. We then compare with previous surveys from the perspective of these key aspects to highlight the study scope and contributions of our article. Three main attributes are used in this survey, i.e., critical infrastructure, cybersecurity, and rule-based AI modeling. Thus we mainly use a combination of these search keywords “Cybersecurity”, “Critical Infrastructure”, “Artificial Intelligence”, “AI”, “Rule-based AI”, “Machine Learning”, “Knowledge Discovery”, “Data Science Modeling”, “Critical infrastructure Resilience” etc. while searching relevant papers. We consider scientific journals, conferences, and books peer-reviewed through several databases like Google Scholar, Science Direct, Springer Nature, Scopus, ACM, and IEEE Explore, published during the period of 2010 to 2023. We take into account the relevance of the research topic through the content of the abstract, introduction, discussion, and conclusion of the papers. Overall, we list 130 papers within the scope of our study 14 of which are survey papers comparing our paper listed in Table 2. Some surveys concentrate on CI threats and risks but have nothing to do with AI-enhanced cybersecurity [7,9,10]. For instance, Touhiduzzaman et al. [7] review of cybersecurity risk for CI. Kayan et al. [9] explore ICPS security, including IT and OT. Husnoo et al. [10] explore privacy-oriented attacks for CI. Similar to this, some surveys concentrate on SCADA security [11,13,18]. Some studies explore defense modeling [16], ML-based security [12] and resilience under threats [14,15,15]. More related works with their key objectives are summarized in Table 2 (see Refs. [17,19]). However, an extensive study on rule-based AI modeling in the context of cybersecurity and CI is still not explored, which motivates us to conduct this survey. Thus, our paper first focuses on various security issues in CI. We then present an in-depth review of different rule-based AI methods for cybersecurity modeling through a taxonomy with their explainable capabilities. This can assist analysts and security experts in figuring out how the system works, uncovering potential threats and anomalies, and finally deciding how best to deal with them. We also discuss the potentiality of rule-based AI methods in diverse cyber application areas in a CI environment. Eventually, we highlight the identified research issues with their potential solution directions for future cyber research and development in CI. Overall, we cover all the ten critical aspects, including RuleAIT (Rule-based AI taking into account Automation, Intelligence, and Transparency) shown in Table 2, which makes our survey unique compared with existing surveys in this emerging area of study.

2.5. Scope and target audience

Our paper focuses on bridging the gap between scientific research and the practical application of rule-based AI in the context of cybersecurity and critical infrastructure. We achieve this by compiling all of AI's advantages, drawbacks, and upcoming challenges across the broad cybersecurity sector in the CI environment into this single document. Similar to the ML study in [25], any reader interested in rule-based AI technologies and how they relate to cybersecurity and CI should be capable of comprehending our study. In addition, our rule-based AI methods and taxonomy presented in Section 4, might also be helpful for the audience of other application domains. We specifically address the following four groups of target readers:

- Top-level Decision-makers: Those who comprehend the state of the art to make decisions in the CI environment. This paper should make it easier to make wiser decisions concerning the use of rule-based AI and its integration into current systems to increase the efficiency of security operation centers.
- Scientists and Research scholars: Those interested in focusing on rule-based AI methods for cybersecurity modeling with innovative methods, enhancing current cyber systems in CI, or minimizing some drawbacks. These can be done through the research issues and prospects outlined, particularly in Section 6 in this paper.
- Industry Professionals and Practitioners: Who should know the potentiality of rule-based AI for cyber modeling towards automation, intelligence, and transparent modeling, i.e., trustworthiness in decision-making. This could be more effective in practice and commercial AI-based cyber solutions in a CI environment.
- knowledge Seeker: Who is seeking knowledge regarding the significance of rule-based AI, including knowledge-driven, data-driven, and their hybridization, mainly focused in Section 4, as well as their potentiality for real-world use cases discussed in this emerging area of study.

The key ideas from this paper use the input from all the reader groups indicated above and consider their perspectives. Experienced engineers or researchers, for instance, might be aware of the challenges of rule-based AI in real-world application scenarios. Still, they might not know how decision-makers react to such concerns. Security experts may be familiar with rule-based AI applications in CI. However, they would still benefit from being aware of the most important breakthroughs in this emerging area.

3. Threats to critical infrastructures

Critical infrastructures face a wide range of physical and cyber threats that can potentially disrupt essential services and compromise their security, resilience, and the well-being of society. Attackers can target both the information technology (IT) and operational technology (OT) systems to disrupt services, steal sensitive data, cause physical damage, or manipulate critical processes [26]. Thus, protecting both IT and OT networks is crucial for critical infrastructure security [7], which is a challenging task. While IT relates to information/data processing and management, OT focuses on monitoring and controlling physical phenomena via physical devices and processes [9], discussed below.

3.1. IT threats examples

Attackers may penetrate IT systems to steal sensitive data, such as customer data, financial records, or intellectual property, resulting in legal penalties and reputational harm. For instance, a financial institution's IT systems being compromised could result in fraud or the loss of consumer information. DoS and DDoS attacks are common threats against IT systems, overwhelming networks and causing service unavailability, impacting critical services [27,28]. Ransomware is regarded as one of the biggest threats facing organizations today, regardless of the industry they operate in [29]. Ransomware attacks can lead to operational disruptions, financial losses, and compromised data integrity. To acquire unauthorized access to IT systems, attackers may utilize social engineering strategies like phishing emails to deceive employees into disclosing login information or downloading malware [30]. SQL injection and code injection attacks can exploit web application and database flaws to obtain unauthorized access or change data [31].

3.2. OT threats examples

As the world depends increasingly on networked systems, cyber-attacks on critical OT infrastructures are becoming significant. Unlike attacks on IT systems, cyber-attacks on OT systems can have direct physical consequences. Attackers who target OT systems intend to disrupt business operations, manipulate control systems, and potentially cause physical harm. For instance, compromising with a transportation system's control systems could result in accidents or disrupt traffic control. Critical services can be disrupted by direct attacks on control processes against OT systems, such as SCADA, ICS, PLCs, etc. [32]. For instance, a DoS attack on SCADA

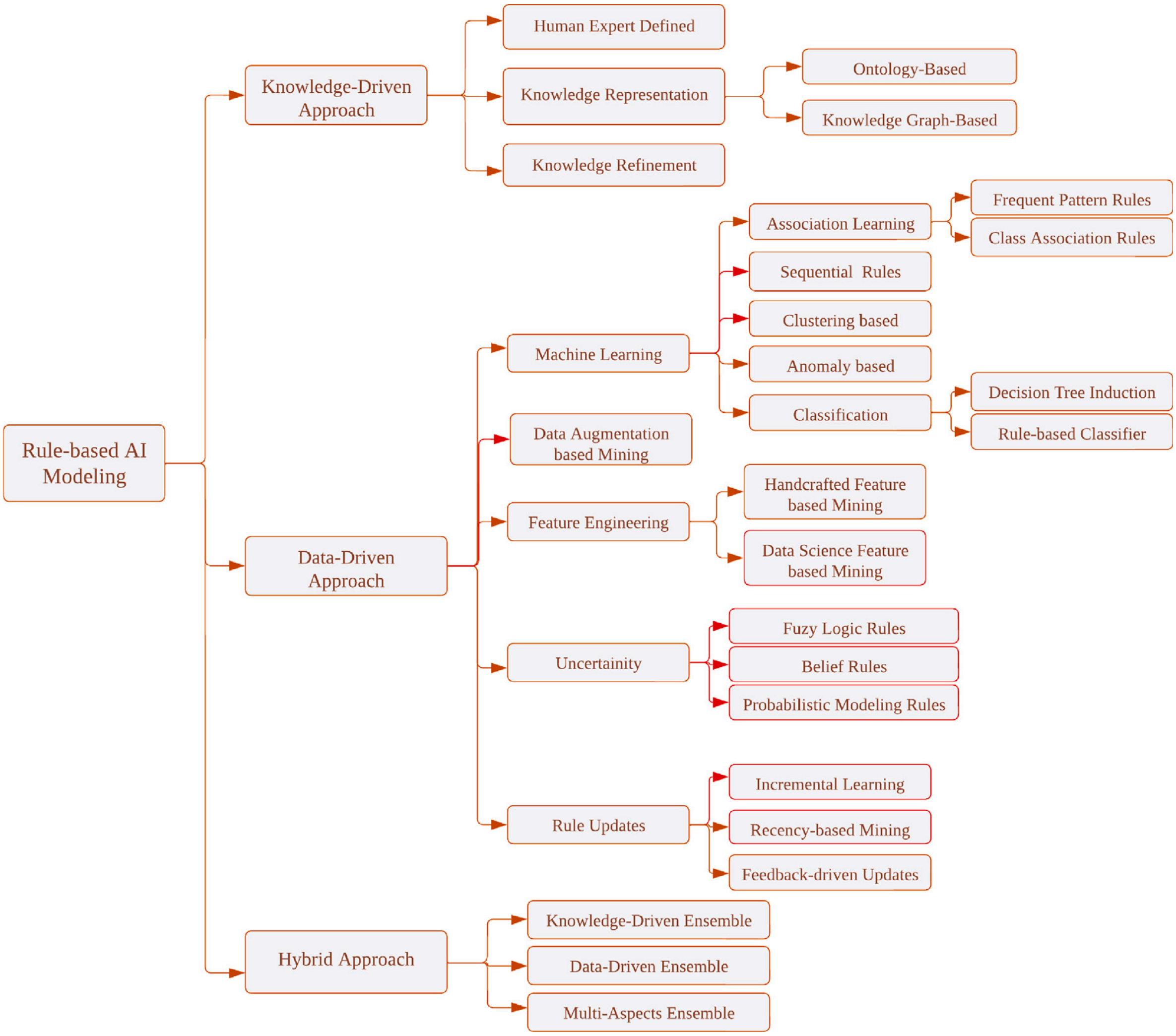

Fig. 3. A taxonomy of multi-aspects rule-based AI methods by taking into account both the knowledge-driven and data-driven approaches as well as their hybrid methods for the purpose of effective cybersecurity modeling according to today's diverse needs.

systems can have potentially disastrous consequences because of the fallout of the controlled process getting out of control [13,33]. Malware or malicious software poses a serious threat to a critical infrastructure scenario [34] as well as SCADA systems [35]. PLCs are also vulnerable to several attacks, including memory corruption and control-flow hijacking [36,37]. Spenneberg et al. [38] demonstrated ransomware worms could infect Internet-connected PLCs and be used as a backdoor to spread in a SCADA network. The sophistication of new malware attacking control systems, such as zero-day attacks, could be another possible disruption at the ICS component level [11]. Similarly, attackers attempted to exploit HMIs through typical Web attacks like SQL injection, CSRF (cross-site request forgery) and dictionary attacks [8]. Kayan et al. have also presented an attack taxonomy for ICPSs [9]. Maglaras et al. [39] highlighted different threats and attacks to CI, including the lifecycle of cybersecurity, such as prediction, protection, and detection, as well as incident notification and management, where rule-based modeling can play a crucial role.

4. Rule-based AI methods and taxonomy

In this section, we explore multi-aspect rule-based AI methods for cybersecurity modeling in CI and build a taxonomy accordingly, as shown in Fig. 3. To achieve this goal, we first divide the methods into three broad categories - (i) knowledge-driven approach, (ii) data-driven approach, and (iii) their hybridization approach, and discussed briefly in the following subsections. Some popular AI methods with their potential cybersecurity applications are also summarized in Table 3.

Table 3
Summary of various AI-based methods used in the context of cybersecurity applications in critical infrastructures.

Reference	Cyber applications	Methods used	Main contributions
Otoum et al. [40]	Intrusion detection system	Machine and Deep Learning, Feature selection	To recognize intrusive behavior in the collected traffic of critical infrastructure
Zeadally et al. [41]	Cybersecurity solutions	Machine and Deep learning	Harnessing AI capabilities to improve cybersecurity in Critical Infrastructures
Yu et al. [42]	Threat Detection	Deep learning, BERT	Exploring a DL-based proactive APT detection scheme in industrial IoT
Iwendi et al. [43]	Detecting cyber-attacks	Deep learning, LSTM	Exploring sustainable security for the IoT using AI architectures
Zhu et al. [44]	Cyberattack's impact assessment	Hierarchical knowledge	Impact assessment of cyberattacks for critical infrastructures
Wang et al. [45]	Cyber-attacks detection	Machine and Deep learning XGBoost, RF, Bagging, SVM, etc.	Exploring AI-based methods for cyber attack detection in industrial systems
Sheng et al. [46]	Intrusion detection	Correlating communication patterns, Modeling states of ICS devices	To detect intrusions from the SCADA network and assessing risk levels
Shin et al. [47]	cyber intelligence, surveillance, and reconnaissance	Incremental learning, Machine Learning	To propose method for cyber ISR in closed military network
Shin et al. [48]	cyber intelligence, surveillance, and reconnaissance	Feature Selection Method, Machine Learning	Towards efficient decision-making for cyber ISR through optimal features
Mcdonnell et al. [49]	Cyber threat recognition	Deep Learning, BERT	Towards a recommender system for malware recognition and classification to protect aviation and aerospace applications
Maleh et al. [50]	IoT intrusions detection	Feature selection Machine learning	Towards IoT intrusions detection in aerospace cyber–physical systems
Ferrag et al. [51]	Cybersecurity IDS	Feature extraction Machine learning	Towards machine learning-based solutions for intrusion detection for agriculture
Radanliev et al. [52]	Healthcare cybersecurity	Self-optimizing, self-adaptative AI	Towards designing a self-optimizing AutoAI capable of forecasting cyber risks in the health systems
Mohammad et al. [53]	Attack detection Systems	Machine Learning, Concept drift, PCA, k-NN	Towards ensuring cybersecurity of smart grid against data integrity attacks under concept drift
Bakalos et al. [54]	Protecting water infrastructure	Multimodal data fusion, deep learning, CNN	Monitoring critical systems to protect water infrastructure from cyber and physical threats
Kiss et al. [55]	Anomaly Detection Systems	Machine Learning, Clustering, K-means	Towards detecting cyber-attacks that cause anomalies in industrial control systems
Vavra et al. [56]	Anomaly Detection Systems	Machine Learning, ANN, OCSVM, Isolation Forest	Towards adaptive anomaly detection system in an industrial control environment
Elnour et al. [57]	Attack detection Systems	Machine Learning, Isolation Forest	Towards attack detection framework for industrial control systems

4.1. *Knowledge-driven approach*

When generating rules for cybersecurity modeling, a knowledge-driven approach typically uses multiple aspects, such as knowledge from experts, domain knowledge, and well-defined security principles. In other words, it focuses on integrating established best practices and human expertise into the rule-generating process. A rule-based AI model can incorporate this knowledge, which might be useful in many circumstances, particularly if human expertise or feedback is correlated with rules. In the following, we discuss how these rules can be formulated.

4.1.1. *Human expert defined*

Human experts can define rules based on their knowledge of cybersecurity best practices and common attack patterns. Known patterns or signatures of malware, viruses, or other malicious activities can be used to identify and block familiar threats. For instance, Narayanan et al. [58] use broad patterns or rules defined by security experts for the early detection of cybersecurity threats. It is, however, difficult to continually update and refine these security rules manually due to the dynamic nature and characteristics of today's threats and the lack of human knowledge to ensure optimal solutions in broad-scale scenarios.

4.1.2. Knowledge-representation

The use of formal knowledge representation techniques in cybersecurity modeling allows the capture and expression of domain-specific knowledge, which becomes the basis for generating rules for cybersecurity systems [59]. These methods typically focus on structuring and interpreting knowledge, thus facilitating rules aligned with domain expertise. These are:

- *Ontology-Based Rule Generation:* Cybersecurity ontologies can represent entities, threats, vulnerabilities, attack patterns, and defense mechanisms specific to a domain. For instance, Syed et al. [60] present Cybersecurity Vulnerability Ontology (CVO) to manage the vulnerabilities. Ontologies can also facilitate integrating data from various structured and unstructured sources [61]. Rules can be generated based on the relationships and constraints defined in the ontology, which may facilitate reasoning capabilities.
- *Knowledge-graph- Based Rule Generation:* In cybersecurity tasks, knowledge graphs could play a significant role in representing real-world knowledge more interconnectedly, making it simpler to navigate and comprehend the relationships between various pieces of information. For instance, Jia et al. [59] present an approach to construct a cybersecurity knowledge graph considering different entities like vulnerability, assets, and attacks, where the extracted rules are used to deduce new relationships and attribute values. By capturing the complex relationships and dependencies between cybersecurity elements in a graph format it enables a more flexible and comprehensive representation of knowledge and rule generation. The rules can then be used to classify, predict, or derive insights from new data. This powerful technique could be combining knowledge representation, graph theory, and machine learning [5].

4.1.3. Knowledge refinement

The process of refinement is ongoing and iterative. Rules are updated when new knowledge is continuously acquired, incorporated, and improved into the knowledge base. The expert-stakeholder feedback cycle ensures that the rules are still relevant, up-to-date, and effective in combating evolving cybersecurity threats.

Overall, ontologies and knowledge graphs can be valuable tools for rule-based cybersecurity modeling. However, scalability and manually maintaining these resources up to date is a challenging issue as the cyber threat landscape is constantly evolving. Thus, integrating with data science and machine learning-based methodologies [5] leveraging the strengths of each strategy to better threat identification and response could be a potential solution.

4.2. Data-driven approach

A data-driven approach typically produces rules based on analyzing and extracting patterns, insights, and knowledge from data [6]. This process uses the power of algorithms to automatically discover valuable rules from the data itself instead of manually creating rules based on expert knowledge or domain-specific ontologies. In the following, we discuss the potential approaches that can contribute to generating rules and corresponding cybersecurity solutions.

4.2.1. Machine learning

Machine learning techniques can automatically learn and extract patterns, correlations, and rules from data [5]. This method is particularly beneficial where manually crafting rules is challenging or time-consuming, especially when dealing with large-scale CI datasets. For example -

- *Association rule learning:* Association rule learning is a popular method for identifying significant relationships and dependencies between various events, activities, or features. Thus, in the context of cybersecurity, association analysis can help discover attack chains and correlation analysis [62]. For example, the Apriori algorithm [63] can analyze logs, network traffic, or system event data to identify recurring behavior patterns or actions that might indicate security breaches or anomalies. FP-Growth (Frequent Pattern-Growth), Eclat (Equivalence Class Transformation), RARM (Rule Association Rule Mining), etc., are some other techniques with the capability of generating rules from data. However, these may generate redundant rules leading to complex decision-making processes [5]. By leveraging the potential of association analysis, organizations can enhance their understanding of security threats and attack chains and discover the root cause of the incidents, which eventually helps with advanced security modeling.
- *Sequential rule learning:* Sequential rule mining in the context of cybersecurity is beneficial in identifying complicated attack scenarios that involve a series of events occurring over time. This method focuses more on comprehending the temporal order in which events occur to find hidden patterns that might not be observed through conventional association analysis. For instance, Husak et al. [64] presented a sequential rule mining approach to predict cyber situational awareness and personalized blacklisting. Kim et al. [65] used sequential rule mining in their attack graph-based predictive model to reflect the order of events.
- *Classification rule learning:* It is a form of supervised learning where the algorithm learns from labeled data to generate rules automatically. In the context of cybersecurity, Decision trees [66], random forests [67], and other rule-based classifiers [5] can be used to categorize data instances into different classes, particularly differentiating between legitimate and malicious behavior. For instance, Domb et al. [68] presented a random forest rule generation model consisting of multiple decision trees for anomaly detection. However, selecting the optimal number of trees could be crucial in terms of better decision accuracy [68]. Thus, security experts can create systems by considering an optimal set of rules that automatically categorize and detect security threats.

- *Clustering-Based Rule Learning:* In many cases, clustering can be used in detecting cyber threats as they can identify similarities [69,70]. Clustering has also the potential for representative feature selection [71]. Developing rules based on captured common characteristics in data, i.e., clustering, could be beneficial for identifying groups of related security events or behaviors. Distance, density, statistical, and hierarchical clustering are well-known approaches for cyber security applications [5,72]. Security experts can identify emerging threats, gain insight into common attack patterns, and aggregate similar occurrences for more effective analysis and response through cluster analysis. For instance, Kiss et al. [55] present a K-means clustering-based approach to detect and classify the potential cyber-attacks in industrial control systems. Thus rule mining based on clustering offers significant advantages in the detection of patterns and anomalies in cybersecurity data. However, to ensure the effectiveness of the approach, the selection of features, scalability issues, and interpretability of results are needed to be taken into account.
- *Anomaly-Based Rule Learning:* Anomaly is defined as highly unusual behaviors or differences from others; this is not a normal occurrence [73]. One traditional example of this would be spam detection, where a mail server has to determine if an incoming email is spam (unwanted email) or not. Similarly, an unusual pattern of computer network traffic may indicate unauthorized access [74]. Rules can be generated describing these deviations or anomalies. Statistical techniques, machine learning algorithms such as One-Class SVM, Isolation Forest, etc., or unsupervised learning strategies can be the foundation for anomaly detection [73]. Security systems can detect and respond proactively to unusual or suspicious activities, such as network intrusions, unauthorized access attempts, or compromises of system data, by learning the rules that define anomalies. For instance, Barbado et al. [75] present a OneClass SVM-based rule extraction method in unsupervised anomaly detection. An Isolation Forest-based ICS attack detection framework has been presented in [57].

Overall, traditional rule-based systems rely on rules defined manually, while machine learning [5] can enhance such systems by discovering knowledge and learning rules from data, making them more powerful for cybersecurity solutions. A machine learning-based solution typically provides the benefits of automatically discovering complex and hidden patterns, relationships, and dependencies within cybersecurity data, reducing the need for manual rule formulation. However, we need to take into account a transparent model rather than a black-box solution to build trust, facilitate human oversight, and ensure accountability.

4.2.2. Feature engineering

A key component of rule extraction is feature engineering, which can be divided into two broad categories: (i) handcrafted feature-based mining, and (ii) data science feature-based mining discussed below:

- *Handcrafted Feature-based Mining:* This process is manual and typically based on human expertise. Thus security analysts have direct control over feature selection as it leverages the skills and experience of cybersecurity professionals with in-depth knowledge of the threat landscape. Although handcrafted features are generally simple to understand and explain, manually constructing features for mining rules is time-consuming and may not scale effectively for large, dynamic data sets. In some circumstances, this could end up in potential bias or missed patterns, emphasizing the importance of data science-based features.
- *Data Science Feature-based Mining:* This is a dynamic process and can automatically learn essential features from raw data, which is particularly beneficial when dealing with large and diverse data sets. This typically involves selecting and creating pertinent features, transforming or discretization, as well as domain knowledge integration that dynamically captures the essential characteristics of the data as discussed below:

  – *Feature Selection:* Feature selection is crucial, particularly for high-dimensional data analysis [71], since irrelevant features in the data might reduce the model's accuracy and increase model complexity as well as training period [76]. This can be done based on domain knowledge or feature selection algorithms, e.g., recursive feature elimination, clustering, or using statistical methods, e.g., correlation analysis, feature importance [71,77]. For instance, Zhou et al. [78] presented correlation-based feature selection for building an efficient intrusion detection system. In certain situations, it may help an intrusion detection system increase detection rates while decreasing false positive rates [79].

  – *Feature Creation and Component Analysis:* In many real-world cases, the existing features might not be sufficient to generate effective rules. Thus, creating new features based on existing ones is necessary, which could enhance the representation of the data and model effectiveness. This can involve mathematical operations, e.g., aggregations, extracting domain-specific information, or some other data preprocessing techniques, including clustering methods, depending on the nature of the data. For instance, Cai et al. [71] present representative features using clustering methods. Coulter et al. [80] showed the increased detection rate with the new features in their traffic analysis study. Principal Component Analysis (PCA), which can minimize the dimension of the original dataset while preserving the most important information, may also play a crucial role in solving real-world problems [53,81]. For instance, Manimurugan et al. [82] extract features for anomaly detection based on PCA analysis.

  – *Discretization:* Another crucial data pre-processing method utilized in the broader field of data science is discretization, which primarily focuses on converting continuous attributes into discrete ones. Thus, it can simplify the rule mining process and make the generated rules more interpretable. Various methods, such as static, dynamic, supervised, unsupervised, splitting, merging, etc., can be used through the discretization process [83]. For example, unsupervised discretizers like EFB and EWB and supervised discretizers such as MDLP and ChiMerge are used by Tsai et al. [83] in their machine learning-based empirical study. Panda et al. [84] presented discretization-based solutions for secure machine learning against adversarial attacks.

- *Domain Knowledge Integration:* Incorporating domain knowledge into the feature engineering process can strengthen understanding the real-world scenario. For instance, Maxwell et al. [85] highlighted the importance of adequate feature engineering combining cybersecurity domain knowledge to prevent information loss. Domain experts can provide valuable guidance on relevant features, potential interactions, or transformations that align with the specific needs of feature engineering, which may lead to the rule mining task.

Overall, feature engineering provides benefits for improving model performance and interpretability by tailoring features to cybersecurity data characteristics. An effective feature engineering can contribute to generating applicable rules from raw security data, which eventually can improve the accuracy, interpretability, and generalizability of the ultimate rule-based models. In some real-world applications, a hybrid approach could be beneficial depending on human expertise and the nature of available data sets. However, it is important to take into account the challenges associated with resource intensity, overfitting, subjectivity, and data quality dependency when considering this strategy.

4.2.3. Uncertainty-based rule mining

This discusses how uncertainty measures or probabilistic information are included in rule-based modeling. Thus, we aim to measure the degree of uncertainty of various models discussed below.

- *Probabilistic Rule Mining:* Instead of generating deterministic rules, probabilistic rule mining techniques assign probabilities or confidence scores to rules to capture uncertainty. For example, Husak et al. [64] generated sequential rules to predict cyber situational awareness, using the confidence scores as probability values. These probabilities can represent the likelihood of a rule being accurate or the confidence level in its predictions. Bayesian network is a typical modeling strategy for probability inference [86]. For example, Zhang et al. [87] presented a multimodel-based incident prediction and risk assessment model for ICS, where an attack model, function model, and incident model are combined to form multilevel networks for probability inference. A probabilistic-based rule mining approach offers significant advantages for handling uncertainty and risk assessment in cybersecurity data. However, it is important to consider challenges related to complexity and data requirements when choosing and implementing probabilistic models.
- *Fuzzy Rule Mining:* Fuzzy logic extends traditional rule mining approaches by allowing rules to have degrees of membership or truth values and can be used for cybersecurity modeling. Various techniques like fuzzy decision trees [88] or fuzzy association rule mining [89,90] can be used for fuzzy rule-based cybersecurity modeling reflecting the uncertainty in the data. For instance, Alali et al. [91] presented a cyber security risk assessment model using a fuzzy logic inference system. Fuzzy rule mining is advantageous for handling uncertainty and presenting cybersecurity data in a linguistically flexible manner. However, it becomes complex to interpret and maintain fuzzy rule systems as more linguistic terms and rules are added. It is important to take into account the challenges in computational complexity of fuzzy systems, subjectivity in rule definition, as well as overfitting risks and interpretation before implementing this approach.
- *Belief Rule Base:* It leverages belief, evidence, or Dempster–Shafer theory to manage and reason with uncertain information. These rules are typically derived from expert knowledge, historical data, or a combination of both and can be used for cybersecurity analysis. Ul et al. [92] presented an anomaly detection model based on belief rules to handle uncertainty utilizing sensor data. He et al. [93] present a belief-rule-based method for fault diagnosis of wireless sensor networks. A belief-rule-based approach to ensure the trustworthiness of interpreted time-series decisions has been presented in [94]. A belief rule-based cybersecurity model provides advantages in handling uncertainty, flexible representation, and decision fusion. However, when dealing with many variables, rules, and evidence sources, belief rule-based models can become complex, making them difficult to interpret and manage. It is thus essential to carefully consider the complexity, the challenges of interpretation, and the potential risks of subjectivity and overfitting that may arise from the implementation of belief rule systems.

In summary, uncertainty-based cybersecurity models provide a realistic representation of uncertainties and enable adaptive decision-making. Cyber analysts can create rules incorporating the degrees of uncertainty, leading to more reliable security models depending on the nature of data and target solutions. However, implementation of these approaches needs to take into account challenges such as computational complexity, model complexity, subjectivity, and potential overfitting risks.

4.2.4. Data augmentation based techniques

Data augmentation could benefit cybersecurity, as its primary goal is to increase the volume, quality, and diversity of training data used for rule mining. Both data transformation and synthesis techniques [95] can enhance cybersecurity data, discussed below, which can eventually lead to better identification of security threats and anomalies, particularly when the available real-world data is limited or insufficient.

- *Data Transformation:* Data transformation can occur in both the input and feature space [95]. Feature space involves altering the features or attributes of the data, while input space refers to training samples. In cybersecurity, data transformation techniques apply a variety of operations to security-related data to enhance its quality, usefulness, and impact on security measures. For instance, incorporating new features based on existing ones that provide further information to distinguish between legitimate and malicious activity could eventually help to generate more effective rules. Sophisticated methods like convolutional neural networks could be useful for feature space transformation [95]. The input space can also be enhanced by sampling techniques to address data imbalance issues or by introducing simulated noise or anomalies to the input. For instance, the SMOTE sampling

technique has been used for phishing analysis [96] and fraud analysis [97]. Bagui et al. [98] used sampling techniques for network intrusion detection datasets. Although efficient transformation can produce a variety of insightful data that improves generalization in rule mining, unnecessary transformation may harm model performance.
- *Data Synthesis:* In certain scenarios, we can produce synthetic data that closely reflects to the regular data distribution using generative models. Various techniques, like generative adversarial networks, variational autoencoders, and data interpolation, as domain-specific methods, can be used. For instance, Li et al. [99] used GAN for data augmentation to detect anomalies effectively. A comprehensive survey of GAN cybersecurity intrusion detection usage has been presented in [100]. However, in the case of augmented data, overfitting can occur, specifically if patterns introduced by the augmentation techniques do not reflect real-world cybersecurity scenarios.

In summary, data-augmentation-based rule mining offers advantages in cybersecurity modeling in terms of improving robustness, generalization, and performance. Cybersecurity models can be trained to detect and effectively handle a variety of threats by creating synthetic attack scenarios and variations. Thus, data augmentation helps to capture a broader range of patterns and behaviors, resulting in more precise and effective rules for cybersecurity solutions. However, it is important to take into account the overfitting risks, representativeness of augmented data challenges, interpretability issues, and privacy concerns when utilizing augmented data.

4.2.5. Concept drift and rule updating techniques

The effectiveness of the current rules and models may be compromised by concept drift, i.e., to describe changes, which would increase the number of false positives and negatives and lower the detection accuracy. Rule updating techniques in cybersecurity modeling involve mechanisms to adapt and refine rule-based models based on new information, emerging threats, or system behavior changes. Here are some commonly used techniques for rule updating in cybersecurity modeling:

- *Incremental Learning:* Through incremental learning techniques, rule-based models can adapt to new data by adding it to the existing model rather than retraining it from scratch. This method enables efficient updates as it allows the relevant portions of the model to change. For instance, Kianmehr et al. [101] presented an incremental semi-rule-based learning model for cybersecurity in cyberinfrastructures. To keep the model up-to-date, incremental learning algorithms might modify rule weights, thresholds, or conditions in response to newly acquired information. Thus, in a dynamic and ever-changing cybersecurity environment, incremental learning enables the model to adapt to new and emerging threats over time.
- *Data freshness and recency-based mining:* The concept of freshness and recency-based rule mining in cybersecurity involves prioritizing the most recent data when creating and updating cybersecurity rules. This method takes time-stamped data into account and creates rules that consider the temporal dynamics of cyber threats. For instance, Sarker et al. [102] presented a recency-based rule mining technique to highlight the significance of recent patterns in user behavioral rules. It may incorporate approaches like sliding windows, time-based segmentation, or decay functions to add weight or value to recent data points during the rule-mining process. Whenever the model is updated or generated based on fresh data, new insights are generated, ensuring its effectiveness and relevance as the context of cybersecurity rapidly changes. However, it is important to balance the benefits and challenges such as the risk of overfitting, loss of historical context, and increased sensitivity to noisy data.
- *Feedback-Driven Updates:* The rule-based models are improved through feedback-driven updates that consider user input, performance feedback from the system, and feedback from domain experts. This input can point out misclassifications, false positives, or areas where the model needs to be improved. Based on the feedback, rule weights, thresholds, or conditions can be modified to mitigate issues, improve accuracy, or assign some rules priority over others. For instance, the expert can remove some rules that might not make sense in practice or add some interesting rules to the existing rule set [101].

In summary, rule updating in cybersecurity modeling offers advantages in adaptability and real-time threat response. The implementation of rules ensures that rule-based systems remain relevant and effective by keeping them current and adapting to changing circumstances. However, effective rule updating in cybersecurity requires careful consideration of potential challenges, such as overfitting, increased noise sensitivity, complexity, and resource requirements.

4.3. Hybrid approach

To generate robust and flexible rules for threat detection and cybersecurity analysis, hybrid strategies for rule generation in cybersecurity modeling incorporate many methodologies, such as data-driven approaches, knowledge-driven methods, and expert knowledge. These are:

4.3.1. Knowledge-driven ensemble

This typically combines multiple sources of knowledge and expertise to produce an extensive collection of rules for threat detection and cybersecurity solutions. Ontologies and knowledge graphs, for instance, can be used to enhance the rule generation process and increase the model's capacity to identify complex and dynamic cyber threats [59]. The ontology defines concepts, relationships, and properties, while the knowledge graph captures complicated interactions between numerous entities. This ensemble method seeks to improve the rule generation process and provide more accurate and understandable models by leveraging the benefits of multiple knowledge-driven techniques such as formalized knowledge representations and human expertise.

4.3.2. Data-driven ensemble

Combining various data-driven methodologies to provide a comprehensive and robust collection of rules for threat detection and cybersecurity analysis is the basis of a data-driven ensemble for rule generation in cybersecurity modeling. For instance, Kianmehr

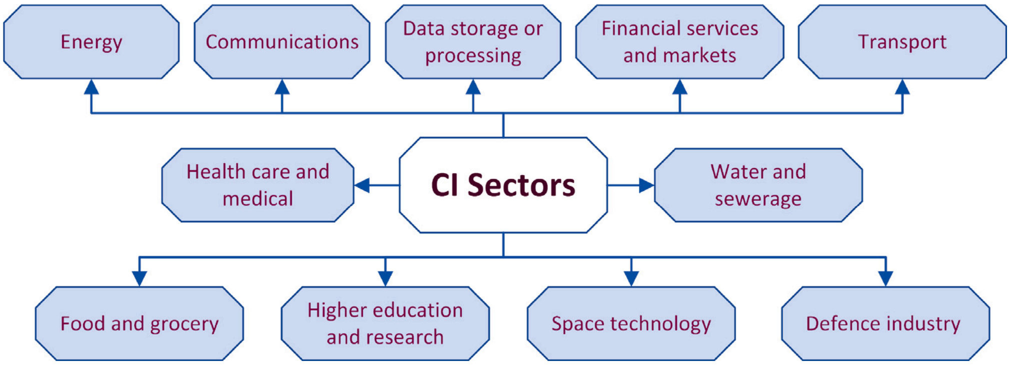

Fig. 4. Major CI sectors according to Australian Government Critical Infrastructure Centre [1].

et al. [101] used feature selection and incremental approach to build an effective rule-based model. To identify patterns, correlations, and anomalies in cybersecurity data, the data-driven ensemble approach typically uses the advantages of multiple machine learning and data mining techniques. Different methods such as voting, weighted combination, stacking, or rule prioritization could be useful to combine the rules produced by multiple data-driven strategies discussed earlier.

4.3.3. Multi-aspects ensemble

This involves integrating the strength of data-driven methodologies with domain-specific knowledge to construct a resilient and adaptable collection of rules for threat identification and cybersecurity analysis. For instance, Jia et al. [59] built a knowledge graph using a machine learning technique to extract entities to obtain a cybersecurity knowledge base. Similarly, a data-driven technique like deep learning is used to extract the relationship between entities for creating cybersecurity knowledge graphs [103,104]. Thus, the combination of both data-driven insights and structured domain knowledge ensures a more extensive coverage of cybersecurity concepts and interactions.

Overall, hybrid rule-based modeling in cybersecurity offers advantages in adaptability, accuracy, and the use of expert knowledge. However, it is important to consider trade-offs, increased complexity, and integration challenges when designing, and implementing such models.

4.4. Performance analysis and discussion

As discussed earlier, different methods can potentially build a rule-based model in the context of cybersecurity, depending on the problem's nature and data characteristics. In Table 4, we summarize the performance of various methods to solve diverse cybersecurity issues. Although accuracy on unseen test cases is one of the popular metrics, different other metrics such as detection rate, false positive rate, false negative rate, error calculation, etc. [105], can be used to evaluate the effectiveness of a model.

According to the performance comparison of different rule-based models as shown in Table 4, it may differ depending on data preprocessing, intended solution, and other relevant factors. For instance, Sindhu et al. [106] have shown that the detection rate varies depending on the selected features while doing their experimental analysis on the KDD Cup dataset. Sarker et al. [107] have demonstrated that accuracy can vary depending on the features selected and the kind of categorization, such as binary or multi-class problems. In certain scenarios, one approach can be utilized as a foundation for another method; thus, the ultimate outcome depends on the integration of multiple methods. Furthermore, Sarker et al. [102] emphasized in their study that, in addition to accuracy, rule redundancy, number of rules, and even rule type, such as general or more specific, are crucial factors when model complexity and decision-making are taken into account. Barbado [75] et al. highlighted several factors such as rule completeness, the impact of the number of rules and length, etc. in their rule-based model. Based on our study we can conclude that several key factors such as: (i) model accuracy — a general measure of a model's overall correctness; (ii) rule completeness or representativeness — how well the rules capture all relevant patterns; (iii) model complexity — to reduce the number of rules it contains and the length of each rule; (iv) non-redundancy — do not contain unnecessary or overlapping information; and (v) rule generalization — broadly applicable rules in addition to specific conditional rules are needed to take into account. These factors may differ depending on the problem, the ultimate solution viewpoint, data characteristics, and the available resources. Thus, to build a successful rule-based cybersecurity model, domain knowledge, human expertise, AI, and data science knowledge need to be integrated.

5. Real-world usage scopes

This section discusses the potential usage scopes of rule-based cybersecurity modeling in various real-world CI sectors. Towards this, we first summarize major sectors of critical infrastructure (CI) in Fig. 4, defined by Australian Government CI Centre [1]. These are as follows:

Table 4
Performance of various rule-based methods used in the context of cybersecurity applications.

Methods used	Objective	Dataset used	Performance	Reference
Decision tree classification	Intrusion detection	KDD Cup 99	Classification rate = 98.38% Error rate = 1.62%	Sindhu et al. [106]

Decision tree classification	Detecting multi-attacks	NSL-KDD,
		UNSW-NB15
			Accuracy = 99%,
			Accuracy = 81%
				Sarker et al. [107]

Random forest classification	Detecting multi-attacks	NSL-KDD,
		UNSW-NB15
			Accuracy = 99%,
			Accuracy = 83%
				Sarker et al. [107]

Association rule mining	Cyber intrusion detection	KDD'99	Precision = 0.934,
			Recall = 0.842,
			F-Score = 0.897
				Lou et al. [108]

Fuzzy association rule mining	Cyber intrusion detection	DARPA98	Detection rate = 98.7%, Positive false rate = 0.53%, Negative false rate = 3.75%	Mabu et al. [89]
Sequential pattern mining	Intrusion detection of power system	Testbed simulation log data	Detection rate = 73.43%	Pan et al. [109]
Data-clustering based approach	Detecting anomalies in industrial control systems	Simulated data	RMS error = 0.108	Kiss et al. [55]
Anomaly detection based approach	Application to OneClass SVM for detecting anomalies	Public and real data	P@1 rule; Precision min = 1.0, Recall min = 0.0	Barbado et al. [75]
Feature selection based voting approach	To build an efficient intrusion detection system	CIC-IDS2017	Accuracy = 99.89%, Attack Detection Rate = 99.9%, False Alarm Rate = 0.12%	Zhou et al. [78]
Belief rule based approach	Detecting anomalies from Custom sensor data	Sensor data	Area under curve = 0.979, Confidence interval = 0.967–0.991	Ul et al. [92]

Knowledge graph based approach	To detect and predict dynamic types of attacks	Information security website, Enterprise's self-built information response center	Precision = 0.739,
			Recall = 0.735,
			F1 Score = 0.737
				Jia et al. [59]

5.1. Energy

Employing AI techniques in the context of the energy sector is popular, mainly to protect power plants, electrical grids, and other energy infrastructure against cyber threats. For instance, Yu et al. [42] present a deep-learning-based proactive advanced persistent threats (APTs) detection scheme in IIoT, using labeled data from a private power grid. Yang et al. [110] present a deep-learning-based intrusion detection system for SCADA networks using the traffic data collected from two SCADA cyber-security test beds for energy-delivery systems. Khaw et al. [111] present a deep learning-based cyberattack detection system for transmission protective relays. A comprehensive review-based study on machine learning methods and solutions for cybersecurity in smart grids has been presented in [112]. In addition to these AI models, Das et al. [36] present a rule-based model that could be beneficial for detecting anomalies. Similarly, an ML-based firewall with appropriate preventive rules for power grid security has been presented by Haghighi et al. [113]. Rule-based AI modeling can also be used to monitor user activity and access patterns to identify insider threats or other suspicious activities, preventing unauthorized access or data theft in this CI sector. Overall, organizations can enhance their ability to detect and mitigate cybersecurity threats with explainability analysis by implementing rule mining based transparent AI modeling.

5.2. Communications

Communication is another sector of CI, and several researchers are exploring AI modeling for cyber solutions in this area. For instance, Zeadally et al. [41] explore AI's potential to improve cybersecurity solutions by considering various communication networks in critical infrastructure. Simola et al. [114] develop cybersecurity considering IT/ICT and OT/ICS networks and threats by using a testbed in an industrial environment. Pinto et al. [115] explore various network intrusion detection systems based on machine learning techniques to protect critical infrastructure. Otoum et al. [40] explore AI-based intrusion detection solutions, considering both machine learning and deep-learning-based IDS for critical infrastructure monitoring WSNs. Rule-based AI modeling can assist in protecting communications networks and thwart attacks on critical communications infrastructure according to the extracted rules from data. According to the rule structure, these models can detect malicious activity, network intrusions, etc., and can take appropriate action to protect communication services.

5.3. Financial services and markets

Financial service is another crucial area of critical infrastructure where cybersecurity solutions must improve. Kotsias et al. [116] discuss how commercial organizations can adopt and integrate cyber-threat intelligence to routinely defend their information systems and resources from increasingly advanced cyber-attacks. Al et al. [117] explore how AI-powered technology can enhance cybersecurity in the banking industry in Qatar. Using rule-based AI models, financial institutions and payment systems can improve their cybersecurity based on human interpretable rules of action. These models can identify fraudulent activity, prevent unauthorized access to financial systems, reduce the risk of data breaches, and identify financial crime by tracking transactions, network traffic, and user behavior.

5.4. Water and sewerage

Smart water systems are now crucial to any modern city's infrastructure. Cyber threats can affect these infrastructure systems responsible for controlling water supply and wastewater treatment. Bello et al. [118] highlight cybersecurity challenges in Australian water infrastructure management. Bakalos et al. [54] present an attack detection framework for critical water infrastructure protection based on multimodal data fusion and adaptive deep learning (CNN model). Sobien et al. [119] explore AI for cybersecurity in water systems, highlighting several water supply testbeds, secure water treatment, and distribution datasets. Multi-aspects rule-based AI modeling could be highly beneficial in securing these systems by detecting potential breaches, ensuring water quality integrity, and preventing unauthorized access to crucial infrastructure components. For instance, Das et al. [36] extract rules to design an anomaly detection system using the sensor measurements of a water treatment system. Machine learning and data mining-based techniques are used to generate invariant rules for anomaly detection in ICS [120].

5.5. Health care and medical

The health sector is a vital part of a country. Thus, cybersecurity becomes crucial to ensure the accessibility of crucial medical services, avoid potentially catastrophic disruptions, and protect patient privacy. Radanliev et al. [52] explore advancing the cybersecurity of the healthcare system with self-optimizing and self-adaptative AI that can use edge health devices with real-time data. He et al. [121] present AI-based directory discovery attack and prevention of the medical systems. As the health sector needs to handle enormous volumes of sensitive patient data, such as personal information and medical records, this becomes a prime target for data breaches. Thus, AI models consisting of a set of valuable and relevant rules can detect and respond to online threats according to rule structure and unauthorized access attempts protecting patient privacy.

5.6. Food and grocery

This industry is becoming more networked and dependent on digital technologies, making it more vulnerable to cyber-attacks. Alim et al. [122] describe a SCADA system testbed for cybersecurity research in critical infrastructure in the food and agricultural sector. Ferrag et al. [51] present machine learning-based solutions for cyber security intrusion detection for agriculture. Sontowski et al. [123] highlight various cyber issues on smart farming infrastructure. The authors demonstrate a Denial of Service (DoS) attack that can hinder the functionality of a smart farm by disrupting deployed on-field sensors. Similarly, a holistic study on security and privacy in a smart farming ecosystem highlighting challenges and opportunities has been presented by Gupta et al. [124]. As this sector increasingly depends on digital technologies with a complicated supply chain with several stakeholders, it becomes vulnerable to cyber threats from suppliers, vendors, and partners. Thus, a feasible solution could be implementing strong security standards based on rules for all supply chain partners.

5.7. Transport

The transportation industry is another vital component of a country's critical infrastructure for the smooth operation of societies and economics. However, Internet of Things (IoT) devices and connected vehicles in the transportation industry may be vulnerable to compromises, posing a risk to public safety and even causing accidents. For instance, cyberattacks on traffic control systems may alter traffic patterns, causing congestion and possible safety risks. Lehto et al. [125] discuss the cybersecurity issues for critical transportation sectors, including aviation, maritime and automotive. Argyropoulos et al. [126] highlight the role of AI/ML techniques in identifying and mitigating cybersecurity and privacy threats in different aspects of the next-generation mobility ecosystem. A rule-based proactive approach can assist in protecting the transportation industry's critical infrastructure from escalating cyber threats. For example, extracting a set of sophisticated rules and setting up intrusion detection systems accordingly can be used to detect and block suspicious activities in real-time. ML techniques can extract rules through anomaly detection and behavioral analysis.

5.8. Defence industry

Cyberattacks in defence systems might have catastrophic consequences, ranging from disrupting military operations to compromising national security. Thus, defense needs to incorporate cyber resiliency into every phase of the capability lifecycle and relevant policy development [127], where AI can contribute. For instance, Shin et al. [47] present a method to efficiently operate cyber ISR (intelligence, surveillance, and reconnaissance) in a closed military network using machine learning, especially incremental learning methods. Shin et al. [48] also consider the cyber ISR process focusing on efficient decision-making based on feature selection methods. Similarly, a robust and operational cyber military strategy for cyberspace superiority in cyber warfare has been presented by Eom et al. [128]. Extracting a set of security rules and corresponding AI models could play a crucial role in defending the critical defense industry. For example, implementing email filtering rules can assist in blocking known phishing domains and prevent malicious attachments from reaching users, which could be a potential solution for phishing attacks.

5.9. Others

Rule-based modeling can also contribute to other CI sectors like space technology, data storage and processing, education and research, or other additional systems and cyber application areas, particularly, where model transparency, explainability and trustworthiness are important. Garcia et al. [129] explore how AI and machine learning techniques can increase aviation security, aid decision-making scenarios, find patterns to determine risk and detect faulty components in the systems. Maleh et al. [50] explore different machine-learning techniques for IoT intrusion detection in aerospace cyber–physical systems. Mcdonnell et al. [49] present a deep learning-based CyberBERT solution to protect aviation and aerospace applications from prospective third-party applications and malware. Vavra et al. [56] focuses on cybersecurity research for industrial control systems widely used in critical information infrastructure. Their approach presents an adaptive anomaly detection system based on machine learning algorithms in an industrial control environment, considering the dataset consists of recorded ICS communication under cyber-attacks. Cybercriminals may seek unauthorized access to crucial data stored in databases or processing systems, causing data breaches and disclosing private information. Similarly, data manipulation or tampering could produce inaccurate outcomes or decisions. Access control rules that enforce robust authentication processes and role-based access defining who has access to particular data and under what conditions could be a potential solution.

6. Challenges and future prospects with potential research directions

Numerous research challenges and opportunities exist in rule-based AI modeling for critical infrastructure cybersecurity. Based on our studies, we have identified these and present the potential solution directions in this section. These are as follows:

i *Innovative Rule Generation Method:* Critical infrastructure systems often involve many connected components and dependencies, making them complicated. It is quite challenging to find the most appropriate methods that adequately capture the intricate interactions and relationships between these components. Existing rule mining methods discussed briefly in Section 4 might not be appropriate in particular circumstances, which motivated innovative rule generation techniques to be developed. For instance, proposing novel algorithms, or improving existing methods or even integrating data-driven machine intelligence with human expertise could be a feasible solution. Thus, research is needed to explore and develop innovative methods for managing rule complexity for CI security, which could be a promising direction in this emerging study area.

ii *Adaptive and Dynamic Rule-based Modeling:* Rule-based AI models often respond to predefined rules at the application level. Critical infrastructure, however, functions in dynamic environments with evolving threats and circumstances. Thus, static and predetermined rules may no longer be sufficient to adequately protect critical systems as the threat landscape continues to change. To protect critical infrastructure and ensure the continuity of essential services, it is crucial to have the ability to adapt and modify rule sets depending on new data dynamically. Therefore, research should focus on developing adaptive rule-learning techniques that can learn from new data and dynamically adjust rule sets to combat new and emerging cyber threats.

iii *Anomaly Detection and Rule Learning:* Methods for detecting anomalies, especially unsupervised machine learning algorithms, can potentially analyze suspicious or unusual behavioral activities in critical infrastructures. Specific rules can be created to address possible security issues when behavior deviates from regular patterns. These algorithms can create a baseline of expected behavior from historical data, allowing them to identify anomalies dynamically. Therefore, one of the key areas of future research will be the creation of methods to effectively detect anomalies in user activity, system behavior, and network traffic in the CI environment and generate security rules accordingly.

iv *Integration with Other AI Techniques:* Rule-based AI models are typically effective at capturing well-known patterns and established regulations. Combining rule-based models with other AI approaches like machine learning, NLP and semantic technologies [4] can improve system efficacy considering their computational capabilities. For instance, NLP can assist in comprehending and extracting contextual information from unstructured data sources like text, which can contribute in recognizing the intent and impact of possible threats. Even rule based AI combining with LLM modeling can contribute to explain the model decisions according to their dependencies and correlation. This integration provides a robust defense system for critical infrastructure, from threat detection to automated response. Therefore, how to effectively combine these AI techniques with rule-based modeling could be another research direction towards a trustable and responsible defense mechanism for critical infrastructure.

v *Human Factors and Applicability:* It is essential to keep human operators, particularly cybersecurity analysts, in mind, as they play a central role in interpreting and acting upon the insights provided by data-driven intelligent models [130]. To detect threats and make decisions, cybersecurity analysts must comprehend the rationale behind the rules that the model triggers. A motivational scenario has also been shown in Fig. 2. Human analysts can trust an AI model and make more informed decisions when it is transparently explained. For instance, analysts can quickly understand complex patterns and anomalies with visual representations. The ultimate goal is to establish an integrated relationship between humans and technology, where AI models support analysts' decision-making rather than taking control of it. Research is required to make rule-based AI systems more understandable and practical for cybersecurity analysts to promote greater human–machine collaboration.

vi *Conflict Resolution and Optimization:* In complex systems, rule conflicts can be a significant issue, especially in the context of CI security. It is crucial to resolve conflicts and optimize rule execution as the number of rules increases and overlaps may happen. Thus, to investigate methods for consolidating and simplifying decision-making rules is important [102]. This might include rule optimization by eliminating duplicate or redundant rules, merging similar rules, and streamlining the decision-making process to minimize conflicts. In addition, specific rules might have higher priority than others; thus, creating a hierarchy might assist in resolving conflicts more effectively. Research is needed to develop rule prioritization, conflict resolution, and optimization methodologies to provide efficient and productive rule-based AI modeling for CI security.

vii *Adversarial Attacks and Robust Defense Modeling:* Malicious actors can intentionally manipulate inputs to exploit vulnerabilities or bypass the rules, potentially leading to significant disruptions or breaches. Developing a robust defense model, including anomaly detection tools, rule validation mechanisms, and model strengthening strategies integrating ensemble methods, feature engineering, or data augmentation, could be beneficial to increase the system's resistance to adversarial attacks. For instance, developing anomaly detection technologies that identify unusual input patterns could indicate suspicious attacks and thus generate alerts for further investigation. Moreover, employing data augmentation techniques that increase the diversity of the training data could support building a robust model and eventually improve the model's ability to handle variations introduced by adversaries. Therefore, focusing on robust cyber solutions accordingly could be one of the top priorities of research in the context of CI security.

viii *Context-Aware Modeling:* Rules might have variable applicability and relevance under particular circumstances, and thus, prioritization of contextual rules provides effective resource allocation and response. When generating and applying security rules, context awareness typically considers the specific operational context, system state, and other external factors. Therefore, developing algorithms to produce context-aware rules dynamically could be another potential research direction, where the eventual model can better adapt to dynamic environments according to the current situation. Research needs to focus on combining data from numerous sources, such as sensor data, logs, network traffic, and external threat intelligence in the context of CI to produce security rules and corresponding context-aware modeling.

ix *Privacy and Data Protection:* Critical infrastructure systems might have to deal with sensitive and private data. To prevent unauthorized access to sensitive data, privacy-preserving techniques such as data anonymization or secure computing can contribute [10]. For instance, data anonymization techniques like differential privacy can be used to preserve individual identities and sensitive information while preserving the utility of the data for modeling. Exploring federated learning in rule-based AI modeling could be another potential direction, as it allows multiple entities to build a model collaboratively. Therefore, maintaining the reliability and confidentiality of the infrastructure requires a strong focus on developing innovative methods of privacy-preserving modeling.

x *Designing Rule-based Security Framework:* Establishing a solid foundation that supports automation, intelligence, and trustworthy decisions is the most important challenge for developing a rule-based cybersecurity system. For instance, incorporating intelligence into the model enables it to effectively analyze and interpret data, discover meaningful patterns, and identify and respond to potential threats. Extracting a set of valuable rules employing suitable techniques discussed briefly in Section 4 could be the basis of this intelligence, as the system's behavior and how it reacts to different threats and events are controlled by rules. Therefore, designing a practical rule-based framework for security modeling and experimental evaluation with CI data could be a potential direction by considering transparency, rule interpretation, and control over the system's behavior.

Our study has identified several challenges and promising research directions for protecting critical infrastructure. First, additional study is required on the properties of CI data, such as involved features, data characteristics and distribution patterns, and associated contexts. Second, CI data needs to be used to evaluate the scalability and efficacy of current rule-based analytics approaches. Thirdly, it is necessary to design innovative methods and algorithms to address the underlying issues. Fourth, a wide range of empirical assessments, considering diverse factors as summarized in Section 4 are required to measure the overall effectiveness of the model. Fifth, further work is needed to deploy the ultimate rule-based security models in a way that will assist in necessary automation, intelligence, and trustworthiness in the pertinent application domains. Overall, the issues highlighted above and the possible solution directions discussed could aid the community of critical infrastructure in realizing the full potential of rule-based modeling in the broad area of AI and cybersecurity.

7. Discussion

The paper provides an in-depth discussion of knowledge discovery and rule-based AI modeling in tackling cybersecurity issues within critical infrastructure. In particular, we answered the questions formulated in Section 1 throughout the paper. The most important observations and findings from the study are highlighted in this section, which might benefit the CI community and decision-makers.

Our study finds that rule-based AI modeling holds much promise for enhancing CI security solutions, mainly when considering automation, intelligence, and transparency, i.e., trustworthiness in decision-making. Rule-based models can efficiently recognize and respond to various cyber threats, such as network intrusions, malware attacks, unauthorized access attempts, and so on, by utilizing a set of relevant rules. While rule-based solutions predefined by human expertise could be beneficial in some cases in various sectors mentioned above, it is worth noting that cybersecurity is an ever-evolving field, and relying solely on such rule-based approaches may not be sufficient. Thus, we need to take into account more powerful rules combined with AI techniques like data science process, machine learning, anomaly detection, and behavior analysis to create a robust and adaptive cybersecurity system for critical infrastructure. These rules are adaptable and scalable across various critical infrastructure systems such as energy, water, defence, communication, and so on discussed briefly in Section 5 since rules are developed by considering data-driven insights and human expert knowledge in the domain.

One of the primary benefits of rule-based AI models is their capability to provide transparent and explicit decisions through their IF-THEN rule structure. Thus, it becomes human-interpreted compared to other sophisticated AI techniques, as shown in Fig. 2. The key reason is rules are typically generated based on known attack signatures, abnormal behavior patterns, other relevant indicators, or even hidden patterns extracted from data. When specific threats or behavior patterns are detected, a set of rules defining relevant conditions and actions are taken. This could include blocking malicious IP addresses, restricting affected systems, or alerting security professionals. This interpretability enables cybersecurity professionals to understand and verify the rationale for the model's behaviors, promoting trust and facilitating cooperation between human operators and AI systems. Adding, deleting, and updating rules to reflect new knowledge is a key benefit of rule-based modeling, making it simpler to manage the entire system at the application level [102].

Rule-based AI models also offer the ability for quick responses. These models can identify anomalies by continually observing network traffic and system behavior. They can then prompt rapid responses like blocking suspicious activity or producing alerts for further investigation. In critical infrastructure, where even minor security breaches can have serious repercussions, real-time responsiveness and human understanding are of the utmost significance. Thus, rule-based modeling can assist accordingly rather than other black box modeling in the broad AI area. The reason is that it provides transparency, human interpretation, and control over the system's behavior according to the rule structure. In the following, we summarize the potentiality and key usages of knowledge discovery and rule-based AI modeling for the broader audience in the context of cybersecurity.

- *Explainable detection, classification and prioritization:* Using vast datasets of historical attack patterns, rule mining algorithms identify recurring sequences of events and patterns that indicate potential security threats. By discovering hidden relationships and dependencies in data, such knowledge or rule-based modeling can formulate rules that can detect and classify emerging threats more accurately. According to these rules, threats are prioritized based on their severity and potential impact on an organization's digital assets. An automated or efficient threat detection or prioritization system typically relies on this discovered knowledge. Thus integrating interpretable rules into detection systems provides cybersecurity professionals with insights into the decision-making process, enabling better threat analysis.
- *Explainable mitigation and response:* With the mitigation rules derived from rule mining-based modeling, cybersecurity professionals can better understand the logic behind mitigation recommendations, allowing them to make more informed decisions. The discovered knowledge can also be used in response modeling. While mitigation aims to prevent or reduce the impact of cybersecurity threats beforehand, response deals with addressing and managing incidents that have already occurred. Thus both mitigation and response strategy with actionalble rules allow for a clear understanding of why each action is being taken and promoting a more adaptive and accountable cybersecurity model.
- *Explainable prediction:* With the knowledge or rules derived from data, cybersecurity professionals can predict emerging threats and identify them, providing a clear understanding of what influences predictions. This increases the trustworthiness of predictive models, facilitating informed decisions when addressing vulnerabilities and strengthening digital defenses.
- *Explainable diagnosis or root cause findings:* Cyber threats can be diagnosed transparently by examining the dependencies and relationships between entities in rules derived from data. A detailed understanding of the factors and indicators that contribute to the detection of anomalies or malicious activities is provided by derived rules or patterns, enabling cybersecurity professionals to diagnose anomalies and malicious activities more accurately.
- *Empowering cyber teams and strengthening the overall resilience:* Through the transparent and interpretable rules generated by the model, humans can better understand the underlying factors responsible for potential threats, allowing them to make more informed and effective decisions. Furthermore, the model is able to suggest mitigation actions based on the extracted rules, enabling cybersecurity teams to respond quickly and appropriately to emerging threats. By collaborating between this knowledge or rule mining and human expertise, organizations can enhance their resilience against evolving cyber risks through more efficient and adaptive cybersecurity practices.

Although rule-based AI modeling has lots of potential, this paper also identified specific issues that need to be considered for further research and investigation. A well-designed rule-based framework considering the relevant issues identified in Section 6, is important to get its full potential at the application level. A well-balanced relationship between data-driven technology and human expert knowledge could be beneficial for this. Overall, we can say that further research on identified areas and development and collaboration between cybersecurity professionals, AI experts, and CI communities is necessary for next-generation cybersecurity in a critical infrastructure environment.

8. Conclusion

In this article, we have provided an in-depth study on multi-aspect rule-based AI modeling on a broad scale towards critical infrastructure security. We also provided a taxonomy of rule-generation methods by taking into account both the knowledge-driven and data-driven approaches as well as their hybridization. We covered the potentiality of these approaches and how these techniques can address diverse cybersecurity concerns such as threat detection, mitigation, prediction, diagnosis for root cause findings, and so on. We also highlighted the power of rule-based AI modeling in terms of automation, intelligence, and transparent modeling through discovering knowledge, patterns and relationships from data. Our study on CI security can help security analysts and professionals comprehend how rule-based modeling can be applicable in addressing cybersecurity concerns in different CI sectors, such as energy, defence, finance, health, etc. We also identified and discussed the issues and potential solution directions for future research and development. Overall, our study on knowledge discovery and rule-based AI modeling opens a promising path for next-generation CI security modeling and can be used as a reference guide for CI researchers, professionals, and policy makers.

CRediT authorship contribution statement

Iqbal H. Sarker: Writing – review & editing, Writing – original draft, Methodology, Formal analysis, Conceptualization. **Helge Janicke:** Writing – review & editing, advising. **Mohamed Amine Ferrag:** Writing – review & editing. **Alsharif Abuadbba:** Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgment

The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Program.

References

[1] Cyber and infrastructure security centre, department of home affairs, 2023, Australian Government https://www.homeaffairs.gov.au/. (Accessed: 20 July 2023).

[2] M. Malatji, A.L. Marnewick, S. Von Solms, Cybersecurity capabilities for critical infrastructure resilience, Inf. Comput. Secur. 30 (2) (2022) 255–279.

[3] R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: Managing a strategic balance between prevention and response, Inf. Manag. 51 (1) (2014) 138–151.

[4] I.H. Sarker, Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview, Secur. Priv. (2023) e295.

[5] I.H. Sarker, Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects, Ann. Data Sci. (2022) 1–26.

[6] I.H. Sarker, AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability, Springer, 2024.

[7] M. Touhiduzzaman, S.N.G. Gourisetti, C. Eppinger, A. Somani, A review of cybersecurity risk and consequences for critical infrastructure, 2019 Resil. Week (RWS) 1 (2019) 7–13.

[8] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, J. Lopez, A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3453–3495.

[9] H. Kayan, M. Nunes, O. Rana, P. Burnap, C. Perera, Cybersecurity of industrial cyber-physical systems: a review, ACM Comput. Surv. 54 (11s) (2022) 1–35.

[10] M.A. Husnoo, A. Anwar, R.K. Chakrabortty, R. Doss, M.J. Ryan, Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey, IEEE Access 9 (2021) 153276–153304.

[11] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin, Cybersecurity for industrial control systems: A survey, Comput. Secur. 89 (2020) 101677.

[12] A.M. Koay, R.K.L. Ko, H. Hettema, K. Radke, Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges, J. Intell. Inf. Syst. 60 (2) (2023) 377–405.

[13] S. Nazir, S. Patel, D. Patel, Assessing and augmenting SCADA cyber security: A survey of techniques, Comput. Secur. 70 (2017) 436–454.

[14] L. Das, S. Munikoti, B. Natarajan, B. Srinivasan, Measuring smart grid resilience: Methods, challenges and opportunities, Renew. Sustain. Energy Rev. 130 (2020) 109918.

[15] E.M. Wells, M. Boden, I. Tseytlin, I. Linkov, Modeling critical infrastructure resilience under compounding threats: a systematic literature review, Prog. Disaster Sci. (2022) 100244.

[16] C.-W. Ten, G. Manimaran, C.-C. Liu, Cybersecurity for critical infrastructures: Attack and defense modeling, IEEE Trans. Syst. Man Cybern. A 40 (4) (2010) 853–865.

[17] X. Liu, C. Qian, W.G. Hatcher, H. Xu, W. Liao, W. Yu, Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities, IEEE Access 7 (2019) 79523–79544.

[18] G. Yadav, K. Paul, Architecture and security of SCADA systems: A review, Int. J. Crit. Infrastruct. Prot. 34 (2021) 100433.

[19] Q. Liu, V. Hagenmeyer, H.B. Keller, A review of rule learning-based intrusion detection systems and their prospects in smart grids, IEEE Access 9 (2021) 57542–57564.

[20] G. Ampratwum, V.W. Tam, R. Osei-Kyei, Critical analysis of risks factors in using public-private partnership in building critical infrastructure resilience: a systematic review, Constr. Innov. 23 (2) (2023) 360–382.

[21] Y. Yang, H. Tatano, Q. Huang, H. Liu, G. Yoshizawa, K. Wang, Evaluating the societal impact of disaster-driven infrastructure disruptions: A water analysis perspective, Int. J. Disaster Risk Reduct. 52 (2021) 101988.

[22] Y. Li, Q. Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Rep. 7 (2021) 8176–8186.

[23] N. Kaloudi, J. Li, The ai-based cyber threat landscape: A survey, ACM Comput. Surv. 53 (1) (2020) 1–34.

[24] E. Bout, V. Loscri, A. Gallais, How machine learning changes the nature of cyberattacks on IoT networks: A survey, IEEE Commun. Surv. Tutor. 24 (1) (2021) 248–279.
[25] G. Apruzzese, P. Laskov, E. Montes de Oca, W. Mallouli, L. Brdalo Rapa, A.V. Grammatopoulos, F. Di Franco, The role of machine learning in cybersecurity, Dig. Threats Res. Pract. 4 (1) (2023) 1–38.
[26] G.M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger, J. Benjamin, Industrial and critical infrastructure security: Technical analysis of real-life security incidents, IEEE Access 9 (2021) 165295–165325.
[27] B. Sousa, M. Arieiro, V. Pereira, J. Correia, N. Lourenço, T. Cruz, Elegant: Security of critical infrastructures with digital twins, IEEE Access 9 (2021) 107574–107588.
[28] B. Hussain, Q. Du, B. Sun, Z. Han, Deep learning-based DDoS-attack detection for cyber–physical system over 5G network, IEEE Trans. Ind. Inform. 17 (2) (2020) 860–870.
[29] G. Potamos, S. Theodoulou, E. Stavrou, S. Stavrou, Building maritime cybersecurity capacity against ransomware attacks, in: Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022, 20–21 June Wales, Springer, 2023, pp. 87–101.
[30] N. Chowdhury, V. Gkioulos, Cyber security training for critical infrastructure protection: A literature review, Comp. Sci. Rev. 40 (2021) 100361.
[31] D. Resul, M.Z. Gündüz, Analysis of cyber-attacks in IoT-based critical infrastructures, Int. J. Inform. Secur. Sci. 8 (4) (2020) 122–133.
[32] M. Lehto, Cyber-attacks against critical infrastructure, in: Cyber Security: Critical Infrastructure Protection, Springer, 2022, pp. 3–42.
[33] J.P. Disso, K. Jones, S. Bailey, A plausible solution to SCADA security honeypot systems, in: 2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications, IEEE, 2013, pp. 443–448.
[34] E. Ciancamerla, M. Minichino, S. Palmieri, Modeling cyber attacks on a critical infrastructure scenario, in: IISA 2013, IEEE, 2013, pp. 1–6.
[35] I.N. Fovino, A. Carcano, M. Masera, A. Trombetta, An experimental investigation of malware attacks on SCADA systems, Int. J. Crit. Infrastruct. Prot. 2 (4) (2009) 139–145.
[36] T.K. Das, S. Adepu, J. Zhou, Anomaly detection in industrial control systems using logical analysis of data, Comput. Secur. 96 (2020) 101935.
[37] A. Abbasi, T. Holz, E. Zambon, S. Etalle, ECFI: Asynchronous control flow integrity for programmable logic controllers, in: Proceedings of the 33rd Annual Computer Security Applications Conference, 2017, pp. 437–448.
[38] R. Spenneberg, M. Brüggemann, H. Schwartke, Plc-blaster: A worm living solely in the plc, Black Hat Asia 16 (2016) 1–16.
[39] L. Maglaras, M. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, S. Rallis, Threats, countermeasures and attribution of cyber attacks on critical infrastructures, EAI Endorsed Trans. Secur. Saf. 5 (16) (2018).
[40] S. Otoum, B. Kantarci, H. Mouftah, A comparative study of AI-based intrusion detection techniques in critical infrastructures, ACM Trans. Internet Technol. (TOIT) 21 (4) (2021) 1–22.
[41] S. Zeadally, E. Adi, Z. Baig, I.A. Khan, Harnessing artificial intelligence capabilities to improve cybersecurity, IEEE Access 8 (2020) 23817–23837.
[42] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A.K. Bashir, F.A. Khan, Securing critical infrastructures: deep-learning-based threat detection in IIoT, IEEE Commun. Mag. 59 (10) (2021) 76–82.
[43] C. Iwendi, S.U. Rehman, A.R. Javed, S. Khan, G. Srivastava, Sustainable security for the internet of things using artificial intelligence architectures, ACM Trans. Internet Technol. (TOIT) 21 (3) (2021) 1–22.
[44] Q. Zhu, Y. Qin, C. Zhou, L. Fei, Hierarchical flow model-based impact assessment of cyberattacks for critical infrastructures, IEEE Syst. J. 13 (4) (2019) 3944–3955.
[45] W. Wang, F. Harrou, B. Bouyeddou, S.-M. Senouci, Y. Sun, Cyber-attacks detection in industrial systems using artificial intelligence-driven methods, Int. J. Crit. Infrastruct. Prot. 38 (2022) 100542.
[46] C. Sheng, Y. Yao, Q. Fu, W. Yang, A cyber-physical model for SCADA system and its intrusion detection, Comput. Netw. 185 (2021) 107677.
[47] G. Shin, H. Yooun, D. Shin, D. Shin, Incremental learning method for cyber intelligence, surveillance, and reconnaissance in closed military network using converged IT techniques, Soft Comput. 22 (2018) 6835–6844.
[48] G. Shin, H. Yooun, D. Shin, D. Shin, Hybrid feature selection method based on a Naïve Bayes algorithm that enhances the learning speed while maintaining a similar error rate in cyber ISR, KSII Trans. Internet Inform. Syst. 12 (12) (2018).
[49] S. McDonnell, O. Nada, M.R. Abid, E. Amjadian, Cyberbert: a deep dynamic-state session-based recommender system for cyber threat recognition, in: 2021 IEEE Aerospace Conference (50100), IEEE, 2021, pp. 1–12.
[50] Y. Maleh, Machine learning techniques for IoT intrusions detection in aerospace cyber-physical systems, Mach. Learn. Data Mining Aerosp. Technol. (2020) 205–232.
[51] M.A. Ferrag, L. Shu, O. Friha, X. Yang, Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions, IEEE/CAA J. Autom. Sin. 9 (3) (2021) 407–436.
[52] P. Radanliev, D. De Roure, Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptative artificial intelligence (part 2), Health Technol. 12 (5) (2022) 923–929.
[53] M. Mohammadpourfard, Y. Weng, M. Pechenizkiy, M. Tajdinian, B. Mohammadi-Ivatloo, Ensuring cybersecurity of smart grid against data integrity attacks under concept drift, Int. J. Electr. Power Energy Syst. 119 (2020) 105947.
[54] N. Bakalos, A. Voulodimos, N. Doulamis, A. Doulamis, A. Ostfeld, E. Salomons, J. Caubet, V. Jimenez, P. Li, Protecting water infrastructure from cyber and physical threats: Using multimodal data fusion and adaptive deep learning to monitor critical systems, IEEE Signal Process. Mag. 36 (2) (2019) 36–48.
[55] I. Kiss, B. Genge, P. Haller, G. Sebestyén, Data clustering-based anomaly detection in industrial control systems, in: 2014 IEEE 10th International Conference on Intelligent Computer Communication and Processing, ICCP, IEEE, 2014, pp. 275–281.
[56] J. Vávra, M. Hromada, L. Lukáš, J. Dworzecki, Adaptive anomaly detection system based on machine learning algorithms in an industrial control environment, Int. J. Crit. Infrastruct. Prot. 34 (2021) 100446.
[57] M. Elnour, N. Meskin, K. Khan, R. Jain, A dual-isolation-forests-based attack detection framework for industrial control systems, IEEE Access 8 (2020) 36639–36651.
[58] S.N. Narayanan, A. Ganesan, K. Joshi, T. Oates, A. Joshi, T. Finin, Early detection of cybersecurity threats using collaborative cognition, in: 2018 IEEE 4th International Conference on Collaboration and Internet Computing, CIC, IEEE, 2018, pp. 354–363.
[59] Y. Jia, Y. Qi, H. Shang, R. Jiang, A. Li, A practical approach to constructing a knowledge graph for cybersecurity, Engineering 4 (1) (2018) 53–60.
[60] R. Syed, Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system, Inf. Manag. 57 (6) (2020) 103334.
[61] M. Iannacone, S. Bohn, G. Nakamura, J. Gerth, K. Huffer, R. Bridges, E. Ferragut, J. Goodall, Developing an ontology for cyber security knowledge graphs, in: Proceedings of the 10th Annual Cyber and Information Security Research Conference, 2015, pp. 1–4.
[62] Y. Qi, Z. Gu, A. Li, X. Zhang, M. Shafiq, Y. Mei, K. Lin, Cybersecurity knowledge graph enabled attack chain detection for cyber-physical systems, Comput. Electr. Eng. 108 (2023) 108660.
[63] R. Agrawal, R. Srikant, et al., Fast algorithms for mining association rules, in: Proc. 20th Int. Conf. Very Large Data Bases, Vol. 1215, VLDB, Santiago, Chile, 1994, pp. 487–499.
[64] M. Husák, T. Bajtoš, J. Kašpar, E. Bou-Harb, P. Čeleda, Predictive cyber situational awareness and personalized blacklisting: a sequential rule mining approach, ACM Trans. Manag. Inform. Syst. (TMIS) 11 (4) (2020) 1–16.
[65] Y.-H. Kim, W.H. Park, A study on cyber threat prediction based on intrusion detection event for APT attack detection, Multimedia Tools Appl. 71 (2014) 685–698.

[66] J.R. Quinlan, C4. 5: Programs for Machine Learning, Elsevier, 2014.
[67] L. Breiman, Random forests, Mach. Learn. 45 (2001) 5–32.
[68] M. Domb, E. Bonchek-Dokow, G. Leshem, Lightweight adaptive random-forest for IoT rule generation and execution, J. Inform. Secur. Appl. 34 (2017) 218–224.
[69] L. Ignaczak, G. Goldschmidt, C.A.D. Costa, R.D.R. Righi, Text mining in cybersecurity: A systematic literature review, ACM Comput. Surv. 54 (7) (2021) 1–36.
[70] N. Milosevic, A. Dehghantanha, K.-K.R. Choo, Machine learning aided Android malware classification, Comput. Electr. Eng. 61 (2017) 266–274.
[71] J. Cai, J. Luo, S. Wang, S. Yang, Feature selection in machine learning: A new perspective, Neurocomputing 300 (2018) 70–79.
[72] M. Landauer, F. Skopik, M. Wurzenberger, A. Rauber, System log clustering approaches for cyber security applications: A survey, Comput. Secur. 92 (2020) 101739.
[73] V. Yepmo, G. Smits, O. Pivert, Anomaly explanation: A review, Data Knowl. Eng. 137 (2022) 101946.
[74] F.T. Liu, K.M. Ting, Z.-H. Zhou, Isolation-based anomaly detection, ACM Trans. Knowl. Discov. Data (TKDD) 6 (1) (2012) 1–39.
[75] A. Barbado, Ó. Corcho, R. Benjamins, Rule extraction in unsupervised anomaly detection for model explainability: Application to OneClass SVM, Expert Syst. Appl. 189 (2022) 116100.
[76] H. Alazzam, A. Sharieh, K.E. Sabri, A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer, Expert Syst. Appl. 148 (2020) 113249.
[77] G. Chandrashekar, F. Sahin, A survey on feature selection methods, Comput. Electr. Eng. 40 (1) (2014) 16–28.
[78] Y. Zhou, G. Cheng, S. Jiang, M. Dai, Building an efficient intrusion detection system based on feature selection and ensemble classifier, Comput. Netw. 174 (2020) 107247.
[79] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, H. Karimipour, Cyber intrusion detection by combined feature selection algorithm, J. Inform. Secur. Appl. 44 (2019) 80–88.
[80] R. Coulter, Q.-L. Han, L. Pan, J. Zhang, Y. Xiang, Data-driven cyber security in perspective—Intelligent traffic analysis, IEEE Trans. Cybern. 50 (7) (2019) 3081–3093.
[81] I.H. Sarker, H. Alqahtani, F. Alsolami, A.I. Khan, Y.B. Abushark, M.K. Siddiqui, Context pre-modeling: an empirical analysis for classification based user-centric context-aware predictive modeling, J. Big Data 7 (1) (2020) 1–23.
[82] S. Manimurugan, IoT-Fog-Cloud model for anomaly detection using improved Naïve Bayes and principal component analysis, J. Ambient Intell. Humaniz. Comput. (2021) 1–10.
[83] C.-F. Tsai, Y.-C. Chen, The optimal combination of feature selection and data discretization: An empirical study, Inform. Sci. 505 (2019) 282–293.
[84] P. Panda, I. Chakraborty, K. Roy, Discretization based solutions for secure machine learning against adversarial attacks, IEEE Access 7 (2019) 70157–70168.
[85] P. Maxwell, E. Alhajjar, N.D. Bastian, Intelligent feature engineering for cybersecurity, in: 2019 IEEE International Conference on Big Data, Big Data, IEEE, 2019, pp. 5005–5011.
[86] Y. Qin, Y. Peng, K. Huang, C. Zhou, Y.-C. Tian, Association analysis-based cybersecurity risk assessment for industrial control systems, IEEE Syst. J. 15 (1) (2020) 1423–1432.
[87] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, S. Huang, Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems, IEEE Trans. Syst. Man Cybern. 46 (10) (2015) 1429–1444.
[88] P.P. Chan, J. Zheng, H. Liu, E.C. Tsang, D.S. Yeung, Robustness analysis of classical and fuzzy decision trees under adversarial evasion attack, Appl. Soft Comput. 107 (2021) 107311.
[89] S. Mabu, C. Chen, N. Lu, K. Shimada, K. Hirasawa, An intrusion-detection model based on fuzzy class-association-rule mining using genetic network programming, IEEE Trans. Syst. Man Cybern. C 41 (1) (2010) 130–139.
[90] M. Masdari, H. Khezri, A survey and taxonomy of the fuzzy signature-based intrusion detection systems, Appl. Soft Comput. 92 (2020) 106301.
[91] M. Alali, A. Almogren, M.M. Hassan, I.A. Rassan, M.Z.A. Bhuiyan, Improving risk assessment model of cyber security using fuzzy logic inference system, Comput. Secur. 74 (2018) 323–339.
[92] R. Ul Islam, M.S. Hossain, K. Andersson, A novel anomaly detection algorithm for sensor data under uncertainty, Soft Comput. 22 (5) (2018) 1623–1639.
[93] W. He, P.-L. Qiao, Z.-J. Zhou, G.-Y. Hu, Z.-C. Feng, H. Wei, A new belief-rule-based method for fault diagnosis of wireless sensor network, IEEE Access 6 (2018) 9404–9419.
[94] S.F. Nimmy, O.K. Hussain, R.K. Chakrabortty, F.K. Hussain, M. Saberi, An optimized Belief-Rule-Based (BRB) approach to ensure the trustworthiness of interpreted time-series decisions, Knowl.-Based Syst. 271 (2023) 110552.
[95] A. Mumuni, F. Mumuni, Data augmentation: A comprehensive survey of modern approaches, Array (2022) 100258.
[96] M. Ahsan, R. Gomes, A. Denton, Smote implementation on phishing data to enhance cybersecurity, in: 2018 IEEE International Conference on Electro/Information Technology, EIT, IEEE, 2018, pp. 0531–0536.
[97] E. Ileberi, Y. Sun, Z. Wang, Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost, IEEE Access 9 (2021) 165286–165294.
[98] S. Bagui, K. Li, Resampling imbalanced data for network intrusion detection datasets, J. Big Data 8 (1) (2021) 1–41.
[99] Y. Li, Z. Shi, C. Liu, W. Tian, Z. Kong, C.B. Williams, Augmented time regularized generative adversarial network (atr-gan) for data augmentation in online process anomaly detection, IEEE Trans. Autom. Sci. Eng. 19 (4) (2021) 3338–3355.
[100] A. Dunmore, J. Jang-Jaccard, F. Sabrina, J. Kwak, A comprehensive survey of generative adversarial networks (GANs) in cybersecurity intrusion detection, IEEE Access (2023).
[101] K. Kianmehr, An incremental semi rule-based learning model for cybersecurity in cyberinfrastructures, in: 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems, CYBER, IEEE, 2012, pp. 123–128.
[102] I. Sarker, A. Colman, J. Han, P. Watters, et al., Context-Aware Machine Learning and Mobile Data Analytics: Automated Rule-Based Services with Intelligent Decision-Making, Springer, 2021.
[103] A. Pingle, A. Piplai, S. Mittal, A. Joshi, J. Holt, R. Zak, Relext: Relation extraction using deep learning approaches for cybersecurity knowledge graph improvement, in: Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2019, pp. 879–886.
[104] A. Piplai, S. Mittal, A. Joshi, T. Finin, J. Holt, R. Zak, Creating cybersecurity knowledge graphs from malware after action reports, IEEE Access 8 (2020) 211691–211703.
[105] J. Han, J. Pei, H. Tong, Data Mining: Concepts and Techniques, Morgan kaufmann, 2022.
[106] S.S.S. Sindhu, S. Geetha, A. Kannan, Decision tree based light weight intrusion detection using a wrapper approach, Expert Syst. Appl. 39 (1) (2012) 129–141.
[107] I.H. Sarker, CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks, Internet Things 14 (2021) 100393.
[108] P. Lou, G. Lu, X. Jiang, Z. Xiao, J. Hu, J. Yan, Cyber intrusion detection through association rule mining on multi-source logs, Appl. Intell. 51 (2021) 4043–4057.
[109] S. Pan, T. Morris, U. Adhikari, Developing a hybrid intrusion detection system using data mining for power systems, IEEE Trans. Smart Grid 6 (6) (2015) 3104–3113.

[110] H. Yang, L. Cheng, M.C. Chuah, Deep-learning-based network intrusion detection for SCADA systems, in: 2019 IEEE Conference on Communications and Network Security, CNS, IEEE, 2019, pp. 1–7.

[111] Y.M. Khaw, A.A. Jahromi, M.F. Arani, S. Sanner, D. Kundur, M. Kassouf, A deep learning-based cyberattack detection system for transmission protective relays, IEEE Trans. Smart Grid 12 (3) (2020) 2554–2565.

[112] T. Berghout, M. Benbouzid, S. Muyeen, Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects, Int. J. Crit. Infrastruct. Prot. (2022) 100547.

[113] M.S. Haghighi, F. Farivar, A. Jolfaei, A machine learning-based approach to build zero false-positive IPSs for industrial IoT and CPS with a case study on power grids security, IEEE Trans. Ind. Appl. (2020).

[114] J. Simola, R. Savola, T. Frantti, A. Takala, R. Lehkonen, Developing cybersecurity in an industrial environment by using a testbed environment, in: European Conference on Cyber Warfare and Security, Vol. 22, No. 1, 2023, pp. 429–438.

[115] A. Pinto, L.-C. Herrera, Y. Donoso, J.A. Gutierrez, Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure, Sensors 23 (5) (2023) 2415.

[116] J. Kotsias, A. Ahmad, R. Scheepers, Adopting and integrating cyber-threat intelligence in a commercial organisation, Eur. J. Inf. Syst. 32 (1) (2023) 35–51.

[117] K. AL-Dosari, N. Fetais, M. Kucukvar, Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges, Cybern. Syst. (2022) 1–29.

[118] A. Bello, S. Jahan, F. Farid, F. Ahamed, A systemic review of the cybersecurity challenges in Australian water infrastructure management, Water 15 (1) (2022) 168.

[119] D. Sobien, M.O. Yardimci, M.B. Nguyen, W.-Y. Mao, V. Fordham, A. Rahman, S. Duncan, F.A. Batarseh, AI for cyberbiosecurity in water systems—A survey, in: Cyberbiosecurity, Springer, 2023, pp. 217–263.

[120] C. Feng, V.R. Palleti, A. Mathur, D. Chana, A systematic framework to generate invariants for anomaly detection in industrial control systems, in: NDSS, 2019, pp. 1–15.

[121] Y. He, C. Luo, J. Zheng, K. Wang, H. Zhang, AI based directory discovery attack and prevention of the medical systems, in: 2022 Computing in Cardiology, Vol. 498, (CinC), IEEE, 2022, pp. 1–4.

[122] M.E. Alim, S.R. Wright, T.H. Morris, A laboratory-scale canal SCADA system testbed for cybersecurity research, in: 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA, IEEE, 2021, pp. 348–354.

[123] S. Sontowski, M. Gupta, S.S.L. Chukkapalli, M. Abdelsalam, S. Mittal, A. Joshi, R. Sandhu, Cyber attacks on smart farming infrastructure, in: 2020 IEEE 6th International Conference on Collaboration and Internet Computing, CIC, IEEE, 2020, pp. 135–143.

[124] M. Gupta, M. Abdelsalam, S. Khorsandroo, S. Mittal, Security and privacy in smart farming: Challenges and opportunities, IEEE Access 8 (2020) 34564–34584.

[125] M. Lehto, Cyber security in aviation, maritime and automotive, Comput. Big Data Transp. Dig. Innov. Surf. Air Transp. Syst. (2020) 19–32.

[126] N. Argyropoulos, P.S. Khodashenas, O. Mavropoulos, E. Karapistoli, A. Lytos, P.A. Karypidis, K.-P. Hofmann, Addressing cybersecurity in the next generation mobility ecosystem with CARAMEL, Transp. Res. Procedia 52 (2021) 307–314.

[127] S. Fowler, C. Sweetman, S. Ravindran, K.F. Joiner, E. Sitnikova, Developing cyber-security policies that penetrate Australian defence acquisitions, Aust. Def. Force J. (202) (2017) 17–26.

[128] J.-H. Eom, N.-U. Kim, S.-H. Kim, T.-M. Chung, Cyber military strategy for cyberspace superiority in cyber warfare, in: Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, Cybersec, IEEE, 2012, pp. 295–299.

[129] A.B. Garcia, R.F. Babiceanu, R. Seker, Artificial intelligence and machine learning approaches for aviation cybersecurity: An overview, in: 2021 Integrated Communications Navigation and Surveillance Conference, ICNS, IEEE, 2021, pp. 1–8.

[130] I.H. Sarker, H. Janicke, L. Maglaras, S. Camtepe, Data-driven intelligence can revolutionize today's cybersecurity world: A position paper, in: Communications in Computer and Information Science, Springer Nature, Switzerland, 2023.

Iqbal H. Sarker received his Ph.D. in Computer Science from Swinburne University of Technology, Melbourne, Australia in 2018. Now he is working as a Research Fellow of the Cyber Security Cooperative Research Centre (CRC) in association with the Centre for Securing Digital Futures, Edith Cowan University (ECU), Australia. His research interests include Cybersecurity, AI/XAI and Machine Learning, Data Science and Behavioral Analytics, Digital Twin, IoT and Smart City Applications, and Critical Infrastructure Security. He has published 100+ journal and conference papers in various reputed venues published by Elsevier, Springer Nature, IEEE, ACM, Oxford University Press, etc. Moreover, he is a lead author of the books "Context-Aware Machine Learning and Mobile Data Analytics", and "AI-driven Cybersecurity and Threat Intelligence", published by Springer Nature, Switzerland. He has also been listed in the world's top 2% of most-cited scientists, published by Elsevier & Stanford University, USA. In addition to research work and publications, Dr. Sarker is also involved in a number of research engagement and leadership roles such as Journal editorial, international conference program committee (PC), student supervision, visiting scholar and national/international collaboration. He is a member of IEEE, ACM and Australian Information Security Association.

Helge Janicke is a Professor of Cybersecurity at Edith Cowan University (ECU), Australia. He is the Director of ECU's Security Research Institute and the Research Director for Australia's Cyber Security Cooperative Research Centre. He optained his PhD in 2007 from De Montfort University, UK, where he established DMU's Cyber Technology Institute and its Airbus Centre of Excellence for SCADA cybersecurity and digital forensics research, as well as heading up DMU's School of Computer Science. His research interests are Cybersecurity in Critical Infrastructure, Human Factors of Cybersecurity, Cybersecurity of Emerging Technologies, Digital Twins and Industrial IoT.

Mohamed Amine Ferrag earned his Bachelor's, Master's, Ph.D., and Habilitation degrees in Computer Science from Badji Mokhtar-Annaba University in Annaba, Algeria, completing his studies in 2008, 2010, 2014, and 2019, respectively. He served as an Associate Professor in the Department of Computer Science at Guelma University, Algeria, from 2014 until 2022. Dr. Ferrag's research is primarily focused on a spectrum of topics within the cyber security domain, including wireless network security, network coding security, applied cryptography, blockchain technology, generative AI, software security, and the application of AI in cyber security. His scholarly output includes over 140 papers published in international journals and conference proceedings. Dr. Ferrag has spearheaded numerous projects in research and development, fostering collaborative ties with academic institutions in the UK, Australia, USA, Canada, and China. He has consistently been named on Stanford University's list of the world's top 2% of scientists four times from 2020 through 2023. Dr. Ferrag also contributes to the academic community as an associate editor for prestigious journals, such as the IEEE Internet of Things Journal and ICT Express (Elsevier). In addition to his research and editorial roles, Dr. Ferrag is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

Alsharif Abuadbba is a Distributed Systems Security Team Leader at CSIRO's Data61. He has a PhD in computer security from RMIT University, Australia. He also has several years of experience working as a senior research engineer with Californian-based technology companies. He has contributed to a few US IP-filled Patents in cybersecurity. He also has 45+ publications and submissions in high-quality venues such as IEEE S&P, NDSS, ACM ASIACCS, ACSAC, IEEE TDSC, and IEEE TIFS. He is also a regular reviewer at many of those venues. His specialist interests include AI and cybersecurity, System security and privacy.