International Journal of Information Security (2026) 25:14
https://doi.org/10.1007/s10207-025-01188-9

REGULAR CONTRIBUTION

Proactive cybersecurity in industry 4.0: a survey of cybersecurity threat prediction approaches in manufacturing systems

Adel Alqudhaibi[1] · Majed Albarrak[1] · Abdulmosen Aloseel[2] · Amr Munshi[3] · Thamer Alsharif[1] · Sandeep Jagtap[1,4] · Konstantinos Salonitis[1]

Received: 13 August 2025 / Accepted: 6 December 2025
© The Author(s) 2025

Abstract

This review paper provides a literature review of predictive methods and cybersecurity frameworks essential to safeguard Industry 4.0 manufacturing systems against cyber threats. The review focuses on two key areas: the prediction method and the data used for this prediction. These areas are critical for anticipating cyber threats and implementing effective countermeasures. They underscore the need to combine predictive analytics, proactive threat management, and comprehensive frameworks to safeguard against evolving cyber threats. This review assesses the current state and capability of predictive cybersecurity methods within the manufacturing sector, focusing specifically on their effectiveness in predicting threats. The review also identifies gaps in the current research and suggests directions for future studies to further enhance cybersecurity measures in these vital sectors. The study discusses the main features of each method and highlights promising avenues for future research and applications. This literature review is based on a review of relevant publications from 2010 to February 2025. The analysis reveals significant gaps, particularly in the proactive identification and handling of proactively identifying and handling emerging threats. The review concludes with an analysis of the practical implications of implementing a predictive cybersecurity method and outlines future research directions, underscoring the necessity of adaptive, intelligent cybersecurity solutions to defend the manufacturing industry against cybercrime.

Keywords Industry 4.0 · Industrial Internet of Things (IIoT) · Cyberattack · Cyber threat · Security · Machine learning (ML)

1 Introduction

Industry 4.0 is a developing concept that focuses on integrating digitalisation technologies, connectivity, and automation across the business environment. It encompasses technologies such as the Internet of Things (IoT), blockchain technology, artificial intelligence (AI), cloud computing, big data, and advanced robotics. Businesses are adapting to rapid technological change by embracing new models that prioritize digital services and smart manufacturing [1]. This shift is leading to more flexible and responsive supply chains driven by data sharing between businesses and customers and the use of advanced analytics. However, as industries adopt new digital technologies, the attack surface expands, creating more opportunities for cyberattacks and emphasizing the need for strong security measures.

While digitalisation offers substantial benefits to the industrial sector, it also introduces new security challenges and vulnerabilities. In the era of Industry 4.0, maintaining robust cybersecurity is crucial for companies to stay competitive [2]. Industrial facilities are becoming more susceptible to cyberattacks, which can significantly disrupt operations and affect business models. According to Cisco's 2018 Annual

✉ Sandeep Jagtap
sandeep.jagtap@tlog.lth.se

Adel Alqudhaibi
adilq9@gmail.com

1 Sustainable Manufacturing Systems Centre, School of Aerospace Transport and Manufacturing (SATM), Cranfield University, Cranfield MK43 0AL, UK

2 Ministry of Defence, RCWA7182 Riyadh, Saudi Arabia

3 Department of Computer and Network Engineering, College of Computing, Umm Al-Qura University, 24382 Makkah, Saudi Arabia

4 Division of Engineering Logistics, Faculty of Engineering, Lund University, 22643 Lund, Sweden

Published online: 26 December 2025

Cybersecurity Report [3], 31% of organisations have experienced cyberattacks on their operational technology (OT), and 38% anticipate that these attacks will increasingly target OT, extending beyond traditional information technology (IT) systems. Despite the growing recognition of cybersecurity's importance, many organisations are not adequately prepared to address these threats. This lack of readiness is often due to the absence of standardised practices and a shortage of skilled professionals capable of implementing effective cybersecurity strategies [4]. Consequently, there is an increasing demand for predictive models to help organisations forecast and mitigate cyber threats within the industrial sector.

Previous studies [5, 6] have investigated the features and transformations of the globalised market in response to increased demand for individual and specialised products, shorter product lifecycles, and the need for greater adaptability and flexibility. To maintain competitiveness in the contemporary industrial landscape, integrating novel manufacturing processes that enhance operational capabilities and efficiency is imperative [7]. Automated mass production is becoming increasingly economically less viable. This study provides a comprehensive analysis of the industry 4.0 framework from a cybersecurity perspective, examining its challenges, components, issues, advancements, benefits, and significance in adoption. Furthermore, the study provides recommendations and solutions to address the cybersecurity challenges inherent in implementing Industry 4.0 technologies.

According to [8], numerous technological limitations associated with Industry 4.0 exert significant effects on various facets of the contemporary manufacturing industry. Thus, prior to implementing this technology, it is imperative to delineate a comprehensive plan involving all stakeholders in the value chain and to establish consensus on security-related matters and suitable architectural frameworks [9]. Additionally, several researchers have underscored the challenges inherent in implementing Industry 4.0 and suggested that its full adoption is likely to take a decade or more. Embracing this novel manufacturing methodology entails considering a multitude of factors and grappling with myriad obstacles and challenges across social, political, and economic dimensions, as well as technical, scientific, and economic barriers.

The proficiency and attributes of employees, such as their problem-solving skills, capacity to analyse failures, and adaptability to frequent changes, represent significant challenges for companies striving to implement this new strategy. Organisations need to assess specific Industry 4.0 technologies for complex tasks, such as collecting, processing, and visualising manufacturing process data [10]. To the best of the researchers' knowledge, few studies have been conducted in engineering and management education, particularly regarding the expectations placed on students and the shifts in the labour market [11]. The implementation of Industry 4.0 is expected to drive significant changes across multiple sectors beyond the industrial domain, fostering the development of new business models [12].

International organisations are increasingly prioritising strengthening their cybersecurity measures [13]. In 2017, the European Cyber Security Organisation (ECSO) compiled a document that gathered all relevant specifications and standards related to cybersecurity within the European Digital Single Market. This compilation provides a reference for companies to identify suitable schemes to address cybersecurity risks and threats. Furthermore, the International Electrotechnical Commission (IEC) issued a guide on information security and data privacy, which provided both implementation instructions and specific guidelines for IEC publications. These IEC guidelines are internationally recognised recommendations endorsed by national committees [14]. Given the rapid evolution of technology, cybersecurity is anticipated to become a core component of the strategic planning, design, and operational processes of companies adopting the Industry 4.0 framework.

The 2020 Global Risks Report of the World Economic Forum (WEF) identifies cyberattacks on critical infrastructure as one of the most significant threats facing the world. [15]. The WEF noted that 'attacks on critical infrastructure have become the new normal across sectors such as energy, healthcare, and transportation'. Practically all critical infrastructures operate in a digital environment. Meanwhile, the IT landscape has grown dramatically, increasing vulnerabilities. Threat opportunities have expanded because of global connectivity and the development of IoT, and smart cities have created additional vulnerabilities for threat actors. These threat actors have become more advanced and capable, including nation-states and organised digital crime. Manufacturing systems have become the favourite targets for cyber warfare in the digital sector [16].

The primary objective of this review is to provide a comprehensive analysis of the current state of cybersecurity threats in manufacturing systems. By understanding the specific vulnerabilities and threats faced by modern manufacturing systems, this paper explores the potential of predictive techniques to develop a robust cybersecurity framework. The emphasis is on the importance of proactive measures, particularly predictive tools, in protecting these manufacturing systems. The following are our focus points:

The first point begins by examining key manufacturing terminology and systems, establishing the context for understanding cybersecurity challenges in this domain. It explores related research on specific cybersecurity threats faced by manufacturing systems, such as industrial espionage and targeted malware attacks. The next point delves into the role of predictive techniques, including machine learning (ML), artificial intelligence (AI), and threat intelligence platforms,

in early threat detection and mitigation. Additionally, the development of a cybersecurity framework tailored to manufacturing is discussed, with an emphasis on integrating predictive techniques. Through real world case studies, this point provides a practical perspective on the effectiveness of these predictive measures. Finally, it addresses the challenges in implementing these measures and considers the future trajectory of predictive cybersecurity in manufacturing systems.

In the era of digital manufacturing, technologies integrate systems and processes across every aspect of production and establish a cohesive approach from design through manufacturing to the servicing of finished products. This review seeks to shed light on the evolving threat landscape, the potential of predictive techniques, and the path forward in ensuring the security of modern manufacturing systems. Following an introduction to Industry 4.0, this literature review provides a comprehensive analysis of the Industry 4.0 concept from a cybersecurity perspective. It explores the challenges, components, issues, progress, benefits, and relevance of Industry 4.0 adoption and offers suggestions and solutions for its cybersecurity challenges. The review also describes the research methodology employed and presents various perspectives on the challenges and limitations of Industry 4.0, as well as its benefits. Finally, it concludes by offering recommendations for future research.

2 Research methodology

This paper conducts a narrative review to analyze and synthesize the current state of predictive cybersecurity methods in Industry 4.0 manufacturing systems. This methodological approach was chosen as it is ideal for identifying, classifying, and critically evaluating concepts and research gaps from a diverse and emerging body of literature. The review was executed using a structured four-stage process:

(i) Define Scope and Objectives: The review's scope was defined to focus on predictive cybersecurity methods and frameworks relevant to Industry 4.0 manufacturing. The primary objective was to map the current research, identify key methodologies, and pinpoint gaps in the literature.
(ii) Literature Search and Selection: A comprehensive literature search was conducted using two primary academic databases: Scopus and Google Scholar, covering publications up to March 2024. The search strategy employed a set of targeted keywords, including "Prediction Cybersecurity," "Prediction Manufacturing Systems," and "Cyber Attack Prediction."
(iii) Literature Analysis and Synthesis: The selected body of literature was analyzed to extract key information. Also, identifying the several types of predictive models, the data sources utilized, the application areas, and the challenges encountered. The findings were then synthesized to build the conceptual discussions presented in this paper.
(iv) Discussion and Conclusion: The final stage involved discussing the synthesized findings, critically evaluating the identified research gaps, and formulating the conclusions and recommendations for future research presented in this review. This structured approach ensures a comprehensive and reliable analysis of the most relevant studies in the field.

2.1 Paper organization

This paper is structured as follows: Sect. 2 presents the background, discussing the concept of Industry 4.0 and its inherent cybersecurity concerns, including vulnerabilities and risks. Section 3 addresses work on cybersecurity threat prediction approach. This section is further categorised, specifically focusing on predicting cyberattacks (Sect. 3.1). Within this subsection, various predictive models and their applications are meticulously organised and presented (3.1.1–3.1.8). Broader aspects are then examined, including major case studies and challenges (3.3) related to cybersecurity in Industry 4.0. Finally, Sect. 4 concludes with a comprehensive treatment of the topic. This paper presents a logical flow of information, moving from foundational concepts to its main aim, which aligns with practical considerations in the field of cybersecurity frameworks based on cybersecurity threat prediction approaches.

3 Background

This section provides essential background information to contextualize the subsequent discussion of cybersecurity within Industry 4.0 manufacturing environments. It begins by establishing fundamental definitions and concepts related to industry and Industry 4.0, highlighting the transformative impact of technological advancements. Furthermore, it addresses the evolving terminology in the cybersecurity field and outlines the key characteristics and challenges of securing modern manufacturing systems. This foundational understanding is critical for appreciating the need for proactive cybersecurity strategies and predictive threat models.

3.1 Industry 4.0 concept

Industry refers to any employer's trade, business, factory, or calling, as well as any worker's calling, service, employment, handicraft, or industrial occupation. According to management consulting firm McKinsey & Company, Industry 4.0

transitions have the potential to generate value comparable to 15–20% efficiency gains [17]. Modern economies feature many industry classifications, which are typically grouped into larger sectors. Typically, the largest sources of revenue are used as the classification method within individual organisations. Without industry classification systems, measuring economic activity, conducting a business data census, identifying competitors, assessing firms' performance, establishing market share, and developing sector indexes would be impossible. From the outset, classification has been an essential part of information sciences [18]. Even human growth is rooted in classification and categorisation.

Governments and governmental organisations are the primary developers and users of industry classification schemes (ICS). Examples include government-based systems as well as private frameworks such as the Bloomberg Industry Classification System and the FactSet Revere Business and Industry Classification System, which are widely utilised for categorising industries and businesses. Modern digitally enabled production processes have undergone significant transformation compared to the leading manufacturing practices of a decade ago. Innovations in data analytics, AI, big data, and ML, supported by contemporary technology vendors, have equipped manufacturers with numerous solutions to enhance their operational efficiency [17]. Although scaling digital initiatives across extensive factory networks remains a challenge, the drive for successful implementation is stronger than ever. Companies that lead in digital adoption are reaping substantial benefits across the manufacturing value chain. Digital transformation is revolutionising every facet of manufacturing and influencing processes, productivity, and workforce dynamics. Additionally, the effective use of technology not only facilitates data-driven decision-making but also creates opportunities for upskilling, fosters cross-functional collaboration, enhances talent acquisition and retention, and boosts workplace safety and employee satisfaction.

3.2 Industry 4.0 definitions and related terminologies

In less than a second, a Google Scholar search for 'manufacturing' generates 0.35 billion results, while 'definition of critical infrastructure' yields 6,230,000. As time passes and technology advances, the list of industries and sectors classified as essential manufacturing continues to grow. Over the last decade, reports of cybersecurity threats have increased, and attacks have become increasingly complex. Consequently, these attacks on manufacturing systems are becoming more sophisticated each year, necessitating high prioritisation and preventive measures. With these advancements in cybersecurity, new definitions and terminology have changed considerably [19]. This evolution in terminology has caused some issues, as the term 'cybersecurity' lacks the defining clarity of terms such as 'computer security'.

The existing definition landscape has been reviewed by experts and through literature from governmental and

Table 1 Definitions and Perspectives on Industry 4.0

No	Author	Industry 4.0 definition
1	Mohamed et al. (2018) [20]	'The term Industry 4.0 stands for the fourth industrial revolution and is best understood as a new level of organization and control over the entire value chain of the life cycle of products, it is geared towards increasingly individualized customer requirements.'
2	MacDougall (2014) [21]	'Industry 4.0 or Smart industry refers to the technological evolution from embedded systems to cyber-physical systems. It connects embedded system production technologies and smart production processes to pave the way to a new technological age which will radically transform industry and production value chains and business models.'
3	McKinsey Digital (2015) [22]	'Industry 4.0 seen as a digitization of the manufacturing sector, with embedded sensors in virtually all product components and manufacturing equipment, ubiquitous cyber physical systems, and analysis of all relevant data.'
4	Deloitte AG (2015) [23]	'The term Industry 4.0 refers to a further development stage in the organization and management of the entire value chain process involved in manufacturing industry.'
5	IBM (2020) [24]	'Industry 4.0, which is synonymous with smart manufacturing, is the realization of the digital transformation of the field, delivering real-time decision making, enhanced productivity, flexibility and agility to revolutionize the way companies manufacture, improve and distribute their products.'

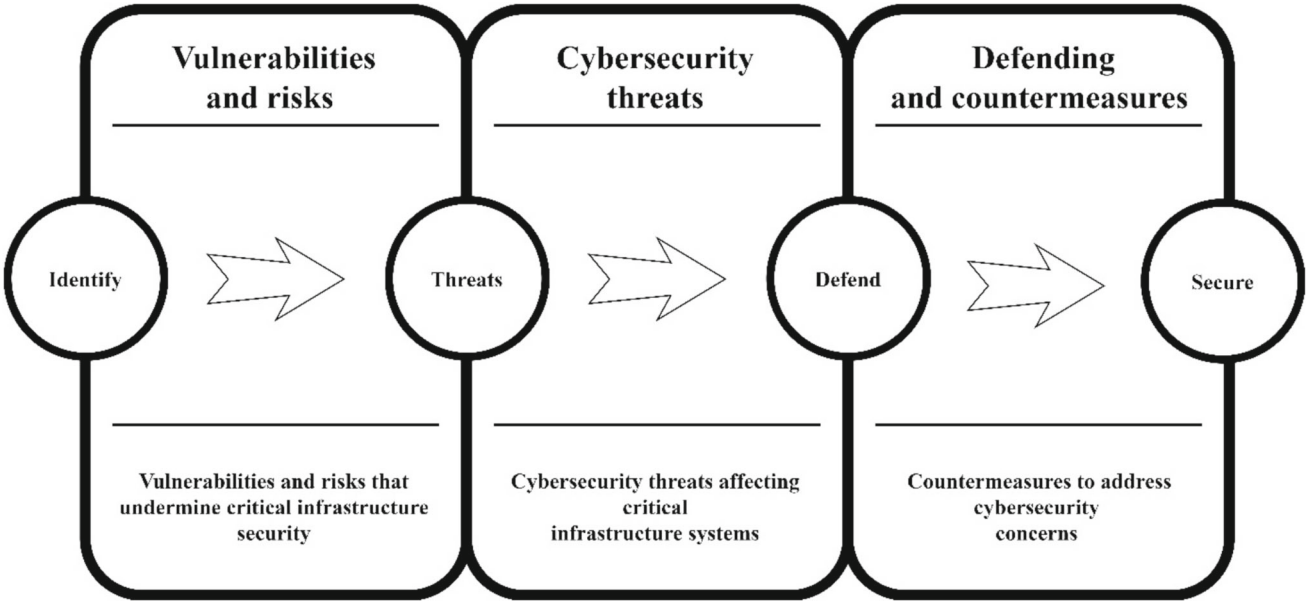


Fig. 1 Three Factors Discussed in Cybersecurity Characterisation

academic organisations to determine the most prevalent definitions. In 2011, the German government initially shaped the technology landscape and perception of Industry 4.0, which has since changed dramatically, creating various uncertainties. Table 1 provides an overview of various definitions and perspectives on Industry 4.0.

3.3 Industry 4.0 and manufacturing systems

Siemens Energy [25] asserts that prioritizing cybersecurity is essential for critical infrastructure, such as power generation, to fully realize the benefits of Industry 4.0. The compelling advantages of digitalization and Industry 4.0 outweigh the associated risks, making it impractical to avoid digitalization. Furthermore, a growing array of tools, technologies, and strategies are available to mitigate cybersecurity risks in operational technology (OT) environments, particularly those found in industrial and critical infrastructure facilities. Currently, most businesses must incorporate innovation into their manufacturing processes to sustain themselves in the face of change and provide more flawless production systems characterised by flexibility, agility, and proactivity [20].

3.4 Cybersecurity characterisation and risks

Once identified, manufacturing systems play a central role in cybersecurity challenges within Industry 4.0 contexts. This section explores cybersecurity challenges in Industry 4.0, focusing on risks to manufacturing systems. It emphasizes the importance of proactive security measures and introduces predictive models that can help mitigate these risks. Highlighting the potential consequences of security failures, such as production halts or data theft, underscores the critical role of cybersecurity in this rapidly evolving industrial landscape. This discussion provides a foundation for examining relevant research and potential solutions. This section discusses three key factors, as illustrated in Fig. 1.

- Vulnerabilities and risks that undermine critical infrastructure security
- Cybersecurity threats affecting critical infrastructure systems
- Threat motivations and cybersecurity countermeasures.

All these factors are linked to the concept of cybersecurity. Comparing the three elements above highlights the importance of the current economic and governmental situation in influencing an individual's tendency to commit cyberattacks. Cyberattacks tend to increase during periods of economic hardship or general dissatisfaction with the nation. Therefore, national economic and political stability may influence social views that motivate individual actions [26].

3.4.1 Vulnerabilities and risks in critical infrastructure

Critical infrastructure systems, which are vital for national security and economic stability, are vulnerable to cyberattacks due to outdated technology and increased interconnectedness [27]. Potential vulnerabilities include outdated software, inadequate network segmentation, and insufficient encryption. Attackers can exploit these weaknesses to disrupt

Table 2 Definitions of Cybersecurity and Cybersecurity Risk from Various Sources

Source	Definition of cybersecurity	Definition of cybersecurity risk	References
International Telecommunication Union (2022)	'The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and nonrepudiation; Confidentiality.'	'The probability that a threat will exploit vulnerability to breach the security of an asset.'	[38]
National Institute of Standards and Technology (2021)	'The process of protecting information by preventing, detecting, and responding to attacks.'	'A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.'	[39]
National Initiative for Cybersecurity Careers and Studies (2014)	'Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.'	'The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.'	[40]

operations or steal sensitive data. Securing critical infrastructure requires continuous risk assessments, system updates, and adherence to security best practices [28].

3.4.2 Cybersecurity threats to critical infrastructure

Critical infrastructure systems are increasingly exposed to a range of cyber threats, including malware, ransomware, and advanced persistent threats [29]. These threats can disrupt operations, cause physical damage, or compromise sensitive data. Addressing these threats necessitates a multilayered cybersecurity strategy encompassing threat detection, incident response, and regular security audits [30].

3.4.3 Threat motivations and countermeasures

Threat actors targeting critical infrastructure have diverse motivations, including financial gain, political goals, and corporate espionage [31]. Understanding these motivations

is crucial for developing effective countermeasures. Countermeasures include advanced threat detection systems, employee training, and a zero-trust security model. Regular system updates, vulnerability assessments, and collaboration with industry and government partners are also essential for safeguarding critical infrastructure [32].

3.5 Vulnerabilities and risks undermining manufacturing security

In the context of cybersecurity, vulnerability is a critical concept with varying definitions across different fields of study. According to [33], vulnerability can be broadly defined as the maximum rate of performance degradation caused by uncertain events, such as cyberattacks. This concept can be expressed in both quantitative and qualitative terms [34]. Wang et al. (2015) defined vulnerability specifically in cybersecurity as "the system's susceptibility to incidents that result in considerable reductions in serviceability" [35]. Furthermore, Mumby et al. (2014) provided both quantitative and qualitative definitions: Quantitative vulnerability involves determining a system's ability to stay above a key threshold when facing a cyberattack, while qualitative vulnerability refers to a system's adaptive capacity and sensitivity to such disturbances [36].

Classifying cybersecurity vulnerabilities involves considering various factors, such as remote access, software, local-area network configurations, and main memory vulnerabilities [2]. Vulnerabilities can also be identified by analysing security exploits [37]. To further understand the concept of security risk in cybersecurity, various definitions from articles and government agencies are presented in Table 2.

3.6 Cybersecurity challenges in the manufacturing sector

In a networked manufacturing environment, cybersecurity not only influences the IT infrastructure but also extends to the entire OT ecosystem, which interfaces directly with physical processes [41]. Cyberattacks on manufacturing systems can halt production, alter results, cause physical damage, or lead to worker accidents. Manufacturing systems, also known as cyber, smart, or digital manufacturing systems, integrate advanced technologies, such as the Industrial Internet of Things (IIoT), cloud computing, and ML, but are vulnerable to cyberattacks due to their designs and insecure communication protocols. The widespread use of IoT introduces additional cybersecurity challenges requiring new methodologies and technologies, such as blockchain, to ensure security and privacy [42].

Cyberattacks on smart manufacturing systems can originate from various external actors, such as nation-states, competitors, or hacktivists, with the intent to disrupt operations, steal intellectual property, or achieve financial gain [43]. Insider threats from employees or partners also pose significant risks by exploiting internal access to steal or disrupt data. To mitigate these risks, companies must provide all staff with regular cybersecurity training and awareness programmes covering security requirements, guidelines, and procedures. Overall, the integration of internet-based technologies in manufacturing offers advanced capabilities but also introduces new cybersecurity challenges that require robust measures to protect against external and internal threats [44].

Research indicates several challenges in the manufacturing cybersecurity arena, typically grouped into two categories: technology and people. An early study by [45] supports this by stating that robust cybersecurity best practices should be driven by an equally balanced equation of technology, people, and process.

According to 'cybersecurity workforce competencies', two of the top seven causes of major cybersecurity breaches are 'naive end-users and disgruntled employees' and 'users not keeping up with new tactics' [46]. An analysis of the 2015 and 2016 cyberattacks targeting the Ukrainian power grid, which compromised ICS, revealed noteworthy parallels with established attack patterns observed in enterprise IT systems [47]. This finding highlights the increasing convergence of vulnerabilities across traditionally distinct technological domains. These attacks were enabled by a successful spearphishing campaign targeting staff and system administrators, indicating that greater awareness and education among the manufacturing workforce could have prevented them [48].

Developing a robust security culture within an organisation that integrates both human and procedural elements is essential for effectively addressing many of the fundamental issues that lead to data breaches [49]. This approach ensures that employees are not only aware of security policies and practices but also actively engaged in implementing and upholding them. By creating a security-aware culture, businesses can greatly reduce the risk of cyber incidents and strengthen their defences against online threats. This approach encourages employees to naturally protect sensitive information, thereby improving overall security within the organisation [50]. An individual's cybersecurity behaviours are substantially shaped by a confluence of factors, including their domain-specific knowledge and skills; cognitive understanding of cybersecurity principles; accumulated experiences; and personal perceptions, attitudes, and beliefs regarding security threats and practices [51]. However, fostering this cultural change within a factory floor environment can be very challenging, as manufacturing employees are typically deeply immersed in day-to-day operations.

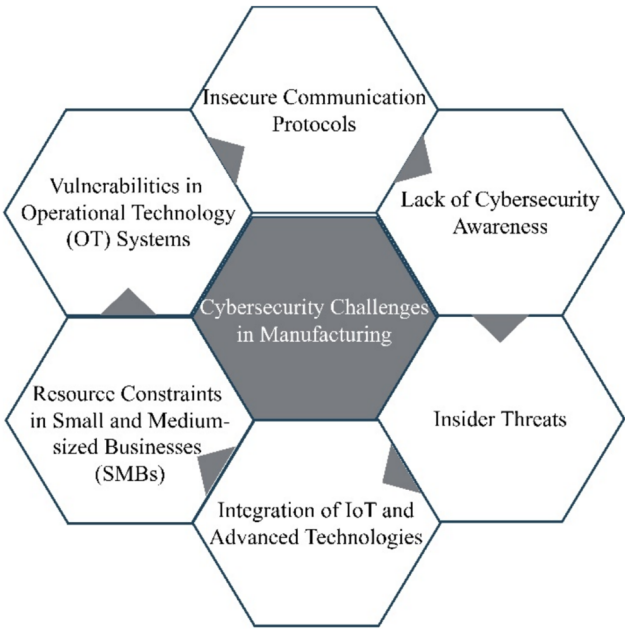


Fig. 2 Cybersecurity Challenges in Manufacturing

Academic research emphasises the pivotal role of individuals in maintaining strong cybersecurity measures. [52] argue that enhancing an organisation's cybersecurity requires management to identify critical assets, understand relevant threats, and develop effective strategies while actively engaging and educating employees. However, this educational effort must extend beyond mere information delivery; it should be focused, practical, and attainable to be truly effective. Figure 2 illustrates the cybersecurity challenges in manufacturing by highlighting six key areas of concern.

As with factory floor staff, manufacturing leadership is often so engaged in daily operations that cybersecurity considerations are frequently overlooked. This oversight can negatively impact resource and finance allocation, making it harder to justify improvements. [53] argues that leadership should support the business case for adopting cybersecurity measures by using the same justification used for deploying and connecting systems initially, as the impact of a successful cyberattack may be as severe as losing operational capability.

The literature highlights a challenge stemming from cultural differences between IT and manufacturing functions: IT primarily focuses on maintaining confidentiality, while manufacturing emphasizes ensuring availability [54]. This issue has been exacerbated by the traditional split between IT and OT systems, but it needs to be resolved in the modern manufacturing landscape. Therefore, IT and manufacturing personnel must collaborate to improve cybersecurity together [55].

A critical factor that connects the technological and human aspects of complex manufacturing environments is the role of small and medium-sized businesses (SMBs) that supply, maintain, and upgrade factory machinery and equipment [56]. As connectivity increases, machinery becomes a prime target for cybercriminals. Unlike larger enterprises, SMBs often face significant challenges in implementing robust cybersecurity measures due to limited awareness, expertise, and resources [57]. This issue has been extensively discussed in academic research, industry analyses, and government guidelines [19]. According to a report by [3], these resource and financial constraints mean that SMBs will continue to struggle with cybersecurity in the long term, creating a substantial vulnerability within the broader cybersecurity strategies of large organisations.

4 Related work in the field of cybersecurity predictive models

This section reviews relevant research and advancements in predictive cybersecurity models and focuses on their application across various domains, including industrial control systems, e-government services, and general IT infrastructure. The models discussed range from traditional data mining techniques to advanced ML and deep learning approaches, and their ability to effectively predict and prevent cyber threats is emphasized. To the best of our knowledge, a comprehensive survey of prediction methods in cybersecurity for manufacturing systems has not yet been conducted, despite several recent surveys focusing on specific tasks and use cases. In 2013, Wei and Jiang [58] investigated network security situation prediction by comparing neural networks, time series analysis, and support vector machines (SVMs), primarily to emphasise the limitations of these methods. Yang et al. [59] formalised the concept of attack projection in 2014 and categorised the literature into three distinct areas: prediction based on attack plans, estimation of attackers' capabilities and intentions, and learning attack patterns and behaviour. In 2015, Leau and Manickam [60] classified network security situation-forecasting techniques into three groups based on their theoretical foundations: ML, Markov models, and Grey theory. In 2016, Gheyas and Abdallah [61] conducted a survey on insider threat detection and prediction and highlighted that predictive approaches have not been extensively explored in recent years. Ramaki and Atani [62] reviewed early warning systems utilising predictive analytics but did not provide an in-depth analysis. West [63] proposed a prediction model framework that integrates statistical methods, ML algorithms, and network analysis techniques. This framework is specifically designed to predict cyberattacks in precision agriculture by analysing network traffic and identifying potential threats based on historical data and learned patterns. Abdlhamed et al. [64] provided a taxonomy of intrusion prediction methods and categorised them into

three groups: hidden Markov models, Bayesian networks, and genetic algorithms. They also identified enhancements to intrusion detection, including artificial neural networks, data mining, and algorithmic methodologies. The same authors later published a survey categorising prediction methodologies into alert correlation, action sequences, statistical and probabilistic methods, and feature extraction, and categorising prediction systems into hidden Markov models, Bayesian networks, neural networks, genetic algorithms, algorithmic methods, and data mining [65]. Recently, Ahmed and Zaman [66] surveyed attack intention recognition methods and identified four categories: dynamic Bayesian networks, graphical models, path analysis, and causal networks, with causal networks being the most effective.

4.1 Predictive models and approaches

Predicting cyberattacks using current technology is challenging due to the numerous potential breach points, unpredictable motivations of attackers, and increasing reliance on connectivity and cloud storage. As businesses continually adopt new technologies, each one introduces its own vulnerabilities, significantly elevating the risks associated with various devices [67]. To understand the cybersecurity predictive models utilized in several studies, a review and summary of these models is provided below.

4.1.1 Predictive analysis of ransomware attacks using context-aware AI in IoT systems

The model uses context-aware AI that incorporates a context ontology to extract information features, such as connection requests and software updates [68]. ML algorithms are also used to predict and detect ransomware penetration attempts in IoT systems early. While the model optimizes prediction efficiency, reducing processing time by 60%, it has notable limitations. The reliance on specific context features limits flexibility, making it less applicable to the diversity of IoT setups. Additionally, the model's focus on Windows-based IoT systems may overlook other platforms prevalent in IoT environments. The requirement for continual updates to context profiles adds to resource demands, reducing practicality. These limitations emphasize the need for adaptable ML models that can address ransomware threats across diverse IoT systems more effectively, offering a broader, less resource-intensive approach to managing evolving threats.

While the approach has strengths in optimizing computational efficiency and providing early detection, it has notable limitations. The heavy reliance on predefined context profiles reduces adaptability to novel or evolving ransomware threats. The framework's focus on a limited set of attack vectors and specific IoT device types restricts its generalizability to broader, heterogeneous IoT environments. Additionally, the methodology appears to emphasize Windows-based IoT systems, which limits applicability to other platforms and technologies prevalent in IoT ecosystems. The lack of scalability and real-time adaptability further diminishes its effectiveness against sophisticated, multi-faceted attacks.

These constraints highlight the need for more versatile, dynamic solutions, such as advanced machine learning models that can handle diverse data and rapidly evolving threats without relying on static context definitions. Such models could enhance prediction accuracy and applicability across a wider range of IoT systems and cyberattack scenarios.

4.1.2 Predicting consequences of cyber-attacks

ML and natural language processing techniques are used to predict the consequences of cyberattacks [69]. Various ML models employing word vectors obtained using Term Frequency-Inverse Document Frequency (tf-idf) and Document to Vector (Doc2Vec) models are compared. However, there are significant limitations. The model's accuracy is relatively low, achieving only about 60%, which may be insufficient for critical applications. The research is limited by a small, imbalanced dataset that risks reducing the model's reliability and generalizability. Additionally, reliance on manually created clusters introduces subjectivity, potentially affecting consistency across different attack types. These limitations emphasize the need for more adaptive and comprehensive machine learning approaches that can manage large, diverse datasets, achieve higher accuracy, and reduce manual intervention, making ML models preferable for more precise, scalable cyberattacks.

While the study provides a valuable dataset and demonstrates the feasibility of predicting the consequences of cyberattacks, it has significant limitations. The 60% accuracy is relatively low for practical applications, suggesting limited reliability. The dataset, although unique, is small and imbalanced, reducing the generalizability and robustness of the predictive models. Additionally, the focus on clustering and categorizing attacks rather than directly predicting consequences limits its practical impact. The reliance on traditional word embedding methods such as tf-idf and Doc2Vec may not fully capture the complexity of cyberattacks, and the study does not explore advanced NLP techniques such as transformers or deep learning models that could enhance prediction accuracy.

4.1.3 Cybersecurity: a statistical predictive model for the expected path length

This model predicts the expected path length in cyberattacks [70]. It utilises vulnerability data and host-centric attack graphs to estimate the number of steps an attacker would need to take to compromise security. The model assists

security administrators in gaining a deeper understanding of system vulnerabilities and prioritising protective measures. Additionally, the research introduces a vulnerability ranking system, which facilitates effective decision-making to mitigate risks. The benefits of this model include its structured approach to analysing attack paths and ranking vulnerabilities, which help administrators prioritize defences. However, its limitations are significant. The model relies heavily on predefined vulnerabilities and paths, making it less adaptable to real-time or evolving threats. It also assumes static conditions within the network, overlooking the dynamic nature of cyber environments where vulnerabilities and threat landscapes change rapidly. Moreover, it requires extensive data on vulnerabilities, which may not always be feasible or up to date, limiting its practical application. These limitations highlight the need for more adaptable, scalable machine learning models that can incorporate real-time data, account for evolving attack strategies, and dynamically predict attack paths under different conditions, offering a more robust alternative to statistical methods.

4.1.4 Predicting cyber attacks on industrial systems using the Kalman filter

The Kalman filter is employed to predict cyberattacks in industrial systems, focusing on statistical prediction of attack patterns based on system-state estimates [71]. The filter's strengths are its minimal need for historical data, reduced storage requirements, and adaptability to real-time data, which are valuable for early anomaly detection in dynamic industrial contexts. However, this approach has several significant limitations. It relies heavily on an accurate a priori model, which is often unfeasible in complex or rapidly evolving industrial systems, leading to inaccuracies. Furthermore, while effective for linear processes, the Kalman filter's efficiency diminishes when handling the complex, non-linear, and multidimensional attack patterns common in modern cyber-physical environments. The study also lacks a comparison with advanced machine learning techniques and uses evaluation metrics (MSE, MAE) that do not address real-world implications such as detection delay or false positives. Overall, this method is promising for straightforward applications but highlights the need for more advanced, adaptive models.

4.1.5 Cognitive models in cybersecurity: learning from expert analysts and predicting attacker behavior

This study investigates cognitive models for predicting attacker and defender behaviours in cybersecurity [72]. Symbolic deep learning enhances threat detection by 25% and offers decision support to non-expert defenders. Model-tracing predicts attacker preferences with 40–70% accuracy, mitigating attack risks. On the defense side, SDL is used to model expert analysts' behavior in Intrusion Detection Systems (IDS) to assist non-expert users. This method helps reduce missed threats by 25%, enhancing the detection accuracy for novice analysts. On the attacker side, model tracing with dynamic parameter fitting is used to predict and exploit individual attacker preferences, achieving 40–70% prediction accuracy across various attackers. This technique demonstrates significant potential in personalizing defense strategies by anticipating attacker moves.

Despite these advantages, several limitations affect the broader application of cognitive modeling. SDL requires labeled expert data, which is often sparse in cybersecurity contexts, reducing model generalizability. Moreover, SDL models lack transparency in decision-making, limiting user trust and practical adoption. For real-time applications, the model's reliance on behavioral data updates introduces complexity and challenges in balancing model adaptability without compromising prior-learned data. The model-tracing approach also faces challenges: attackers who recognize predictive agents may adopt random or adversarial strategies, thereby reducing the model's accuracy. Overall, while cognitive models provide insights and customization, these constraints highlight the need for more robust, adaptable solutions that address these data and transparency issues, making machine learning methods more promising for scalability and practical application in cybersecurity.

4.1.6 Predicting the behavior of attackers and the consequences of attacks against cyber-physical systems

Fuzzy logic and attack tree analysis are used to predict attackers' behaviour and the consequences of their actions on cyber-physical systems [73]. This research focuses on predicting attackers' behavior and the consequences of attacks on cyber-physical systems (CPS) using a fuzzy TOPSIS-based method and dynamic modeling. This approach effectively evaluates attack scenarios, estimates their probabilities, and assesses their physical consequences, including time-to-shutdown (TTSD) and system vulnerabilities. By combining fuzzy logic with attack tree modeling, the study provides a systematic way to address uncertainties in attackers' decision-making processes, offering a structured approach to assess and quantify security risks in CPS environments.

However, the study has several notable limitations. The reliance on predefined attack trees reduces the model's adaptability to evolving or unforeseen attack patterns, limiting its applicability in dynamic, real-world CPS scenarios. The fuzzy TOPSIS method, while computationally efficient,

lacks robustness when dealing with complex multidimensional data, which is often encountered in modern cyberattacks. Additionally, the focus on static metrics like TTSD does not adequately address real-time response capabilities, which are critical for mitigating ongoing threats. The proposed approach also heavily depends on expert input for parameterization, introducing subjectivity and potential bias into the model. Furthermore, the absence of advanced machine learning techniques in the analysis restricts the framework's ability to leverage large datasets for predictive accuracy and scalability.

In summary, while the research provides valuable insights into CPS security evaluation, its reliance on static models, predefined attack structures, and expert-dependent parameterization underscores the need for more adaptive, scalable machine learning approaches to address the evolving complexities of CPS security threats effectively.

4.1.7 A novel architecture for predictive cybersecurity using non-homogeneous Markov models

This study proposes a novel architecture for predictive cybersecurity using non-homogeneous Markov models [74]. This approach focuses on assessing and predicting the security state of enterprise networks by modelling attack graphs with time-dependent variables, such as vulnerability age and discovery rates. By incorporating exploitability and impact metrics, the model provides insights into the evolving risk of attacks, enabling organisations to prioritise vulnerabilities and make informed decisions. The study emphasises the importance of addressing dynamic security attributes and conducting granular analysis to understand how threats may change over time.

While the methodology is innovative, several limitations hinder its practical application. The reliance on predefined attack graphs and vulnerability metrics reduces flexibility, making the model less effective in dynamic or rapidly evolving environments. The dependency on CVSS scores, which are often static and subjective, undermines the accuracy of predictions in real-world scenarios. Moreover, the architecture lacks integration with advanced machine learning techniques that could enhance adaptability and scalability. The model's focus on theoretical metrics, such as expected path length and probabilistic paths, does not adequately address real-time attack detection and response, which are critical for proactive cybersecurity. Additionally, the absence of real-world case studies or comparisons with other predictive techniques limits its validation and generalizability.

In conclusion, while the proposed framework provides a comprehensive, structured approach to understanding cybersecurity risks, its reliance on static data and theoretical metrics underscores the need for more robust, adaptive solutions. Integrating machine learning could significantly improve its effectiveness in addressing modern cybersecurity challenges.

4.1.8 Predicting the discovery pattern of publicly known exploited vulnerabilities

The research introduces a predictive approach for discovering publicly known exploited software vulnerabilities by leveraging vulnerability discovery models (VDMs) and a neural network model (NNM) [75]. The study compares two scenarios: one using all reported vulnerabilities and another focusing only on exploited vulnerabilities. The results highlight that using all vulnerabilities (Scenario S1) improves prediction accuracy in most cases, with NNM outperforming VDMs due to its ability to handle nonlinear patterns. This method offers practical insights into predicting vulnerabilities and optimizing resource allocation for cybersecurity.

However, the study has significant limitations. Reliance on publicly reported vulnerabilities overlooks potential exploits that are not disclosed or available only in non-public forums, such as the dark web, thereby limiting the dataset's comprehensiveness. The dependency on historical data makes the approach less adaptive to emerging and zero-day vulnerabilities. While NNM shows superior performance, its "black-box" nature limits interpretability, making it challenging for cybersecurity experts to validate its predictions. Moreover, the methodology aggregates vulnerabilities across software versions, potentially diluting specificity and creating generalizations that may not apply to distinct versions. The study also fails to explore advanced machine learning architectures, such as recurrent neural networks (RNNs), which could better capture temporal dependencies and improve prediction accuracy.

In summary, while the research provides a structured framework for predicting exploited vulnerabilities, its reliance on limited, aggregated datasets, its lack of adaptability to new threats, and its insufficient exploration of advanced models underscore the need for more robust, transparent, and scalable predictive approaches. These advancements could enhance the method's relevance and applicability in the rapidly evolving cybersecurity landscape.

4.1.9 Cybersecurity attack prediction: a deep learning approach

This study explores the use of deep learning techniques to predict potential cyberattacks [76]. It emphasizes that existing detection models struggle to handle the increasing volume and variety of cyberattacks, underscoring the need for predictive models to enable proactive security. The authors propose several deep learning-based models, including long short-term memory (LSTM), recurrent neural network, and

Table 3 Limitations and Challenges Faced by Predictive Models

Reference and year	Study purpose	High accuracy	High efficiency	High cost	Implement advanced countermeasures
[77], 2022	Propose an adaptive deep learning algorithm for Internet of Things cybersecurity prediction in industrial manufacturing applications	✓	✓	✓	✓
[78], 2020	Review the application of digital twin technology for cybersecurity incident prediction	✗	✓	✓	✓
[79], 2007	Predict potential attack paths and their likely impact on a manufacturing system	✗	✗	✓	✓
[80], 2017	Adapt to technological advancements	✗	✓	✓	✓
[81], 2022	Evaluate cyber situational awareness in predicting cyberattacks for independent power producers	✗	✓	✓	✓
[82], 2021	Integrate machine learning techniques with expert knowledge to achieve more accurate cyberattack predictions in manufacturing	✓	✓	✗	✓
[83], 2021	Develop a privacy-preserving federated learning model for defect prediction in smart manufacturing processes	✓	✓	✗	✗
[84], 2021	Predict risks in the digital transformation of manufacturing supply chains using principal component analysis and backpropagation artificial neural networks	✓	✓	✗	✓
[85], 2017	Predict which machines are at risk of malware infection based on binary file appearance logs	✓	✓	✗	✗

MLP, designed to predict the type of attack before it occurs. These models were tested on a dataset from a capture-the-flag (CTF) competition. Among the models, LSTM achieved the highest performance, with an F-measure exceeding 93%, highlighting its suitability for handling time-series data. The paper concludes with suggestions for future improvements, including testing the models with real-world traffic and enhancing their ability to predict zero-day attacks. The study effectively demonstrates the potential of deep learning to predict and prevent cybersecurity incidents. Tables 2, 3 presents the limitations and challenges faced by predictive models.

While the study highlights the advantages of LSTM and temporal data integration, it has notable limitations. The dataset used (CTF'17) is controlled, limiting the models' applicability to real-world scenarios with diverse, unpredictable attack patterns. Reliance on structured input features such as IP addresses and attack types of limits adaptability to zero-day attacks or unconventional methods not reflected in the dataset. Furthermore, the models depend heavily on labeled data, which is often scarce in cybersecurity contexts. The evaluation metrics, focused on F-measure, fail to account for critical operational factors such as false positives and detection latency, which are pivotal in real-world deployments. Additionally, the computational overhead of deep learning models, particularly LSTM, raises concerns about scalability in resource-constrained environments.

In summary, while the research advances the field of attack prediction through temporal deep learning techniques, its reliance on controlled datasets, structured inputs, and high computational demands highlights the need for more adaptable, scalable, and real-world-validated solutions to address the dynamic nature of modern cyber threats.

These limitations underscore the need for larger, more diverse datasets and the integration of cutting-edge AI techniques to improve the precision and applicability of such models. While the research is a step toward bridging technical and non-technical communication in cybersecurity, its limited predictive accuracy and scope highlight significant areas for improvement in future work.

4.2 Major case studies of cyber incidents in manufacturing systems

In 2023, Clorox experienced a suspected ransomware attack that significantly disrupted its operations. The attack affected many automated systems, resulting in substantial operational downtime and a 20% decline in sales [86]. Financially, this incident cost Clorox $356 million, with an additional $25 million spent on post-breach system security. This case underscores the critical financial and operational impacts ransomware can have on manufacturing companies.

Norsk Hydro, a global aluminium manufacturer, was attacked by the LockerGoga ransomware in 2019, forcing the shutdown of multiple plants [87]. The attack disrupted IT systems across various countries, including Norway, Qatar, and Brazil, resulting in estimated losses of $70 million. Deciding not to pay the ransom, Norsk Hydro had to rely on cybersecurity experts to dismantle the ransomware and recover its systems, illustrating the extensive recovery efforts required after such attacks.

In 2017, Mondelez International fell victim to the NotPetya malware, which destroyed 1700 servers and 24,000 laptops and disrupted global production [88]. This attack led to $100 million in losses and resulted in the theft of numerous user credentials, severely impacting the company's ability to fulfil customer orders. This case highlights the broad and damaging effects of malware on large manufacturing entities.

JBS, a major meat producer, was hit by a ransomware attack by the REvil group in 2021, which halted operations at plants in the US, Canada, and Australia [89]. The company decided to pay an $11 million ransom to restore its systems, underscoring the vulnerability of critical food supply chains to cyber threats. This incident shows the severe operational disruptions that can occur in the food manufacturing sector due to ransomware attacks.

Brunswick Corporation, a boating manufacturer, experienced a cyberattack in June 2023 that disrupted operations for 9 days, resulting in an $85 million loss [90]. The attack significantly affected the company's financial projections and caused major operational delays. This case emphasises the critical need for manufacturing companies to secure their systems to avoid significant financial and operational disruptions.

In 2016, FACC AG, an Austrian aerospace component manufacturer, was targeted by a whaling campaign where attackers impersonated the chief executive officer (CEO) to trick the accounting department into transferring $55.8 million [91]. The attack led to the firing of the CEO and the chief financial officer (CFO), and to additional losses from subsequent legal actions and recovery efforts. This incident highlights the potential for significant financial and managerial repercussions from sophisticated phishing attacks within the manufacturing sector. These case studies illustrate the critical need for robust cybersecurity measures in manufacturing systems to protect against increasingly sophisticated cyber threats.

4.3 Challenges of developing a predictive model from the related studies

Predicting cyberattacks in manufacturing systems presents several challenges, including the limited availability of attack data, the rapidly evolving nature of attack techniques, the unique characteristics of industrial control systems, and the need to balance prediction accuracy with actionable insights [92]. Future research is expected to focus on developing more sophisticated ML models capable of adapting to new attack patterns, incorporating threat intelligence and external data sources to enhance prediction capabilities, and designing user-friendly interfaces that present prediction results in a meaningful way to assist security analysts in making informed decisions.

The impact of challenges in the field of developing a predictive model has been reflected negatively on the security countermeasures, as shown in the mentioned incidents (Sect. 3.2). The following table summarises the correlation between the challenges and the listed incidents. Table 4 summaries of the correlation between the challenges and the listed incidents.

5 Assessment and evaluation of prediction models and paper contributions

This section presents a comprehensive evaluation of the prediction models and approaches developed in this study. SubSect. 4.1 presents a performance analysis of the models using standard evaluation metrics, comparing their accuracy, efficiency, and reliability with baseline methods. SubSect. 4.2 offers a critical discussion of the results and outlines the work's key contributions, emphasizing its novelty, practical impact, and potential to advance future research in the field.

5.1 Evaluation of the effectiveness of the prediction models and approaches

A comprehensive analysis of the advantages and disadvantages of each model is essential for understanding the cybersecurity predictive models employed in the research. Regarding the advantages and disadvantages of the model in 'Predictive Analysis of Ransomware Attacks Using Context-Aware AI in IoT Systems', on the bright side, a context-aware AI powered by context ontology for extracting information features, such as connection requests and software updates, provides an effective way to detect ransomware

Table 4 Cybersecurity Incidents in Manufacturing Systems: Challenges, Impacts, and Security Breaches

Incident	Related Challenges & Impact	Breaches And Security Principles
Clorox Ransomware Attack (2023) [86]	Significant operational downtime due to automated system failures, leading to financial losses and delays in securing systems	Integrity, availability: disruption of automated systems and operational processes
Norsk Hydro LockerGoga (2019) [87]	Disruption across multiple plants and countries, requiring extensive recovery efforts	Confidentiality, availability: information technology system shutdown across countries, reliance on external recovery expertise
Mondelez NotPetya Attack (2017) [88]	Destruction of servers and laptops, impacting production, leading to theft of credentials, and disrupting the ability to fulfil customer orders	Confidentiality, integrity: destruction of infrastructure and data breaches, affecting global operations
JBS Ransomware (2021) [89]	Shutdown of plants in multiple countries and ransom payment to recover systems, illustrating the vulnerability of the food supply chain	Availability, integrity: Operational disruptions, ransom payment to recover critical systems
Brunswick Corporation (2023) [90]	Nine days of operational disruption leading to significant financial losses and delays in production	Availability, integrity: prolonged downtime with considerable financial implications
FACC AG Whaling Attack (2016) [91]	Chief executive officer impersonation leading to a massive financial transfer, firing of key executives, and legal battles	Confidentiality, integrity: social engineering attack, leading to major financial and managerial repercussions

infiltration attempts in a far more accurate and timely manner. Furthermore, ML-based instrumentation enables early prediction, which is critical for reducing the impact of ransomware attacks on IoT systems. However, high computational resources and large training datasets might be required to build an efficient model. The integration of context-aware AI into existing IoT systems may also bring many challenges during implementation.

The 'Predicting Consequences of Cyber-Attacks' model [69] is guided by ML and natural language processing, which provides a robust framework for prediction related to the consequences of cyberattacks. The upside of the model is that it provides a way to improve prediction accuracy by comparing different ML models, including those using tf-idf and Doc2Vec. Nevertheless, it heavily depends on how good and complete the training data are. Moreover, it may not do justice to the nuanced context of cyberattack scenarios, as it is based on word vectors, leading to lower accuracy in complex scenarios. Figure 3 summarizes the predictive methods in cybersecurity discussed in this section.

In 'Predicting Cyber Attacks on Industrial Systems Using the Kalman Filter', the Kalman filter provides a mathematically robust technique to perform system state-based prediction of cyberattacks. Hence, it is well-suited to dynamic industrial environments. This model allows for anomaly detection well in advance and quick response times. The downside is that, with non-linear attack patterns or when the system model is poorly defined, the Kalman filter's performance may degrade. It is also not as good at predicting new or sophisticated attack vectors that differ considerably from historical patterns.

The model of 'Predicting Cyber Threats Using ML for Improving Cyber Supply Chain Security' is oriented to security and has enhanced proactive threat identification measures [92]. The former can be achieved using ML algorithms to predict cyber threats in the cyber supply chain. It helps stakeholders make informed decisions and manage risk by leveraging past data and trends. However, its reliance on historical data can make it hard to predict new threats that may not look and act like other known threats. Furthermore, the dynamic and interrelated features of supply chains may introduce complexities that are highly challenging for ML algorithms to capture precisely.

Finally, the 'Predicting the Behavior of Attackers and the Consequences of Attacks Against Cyber-Physical Systems' model uses fuzzy logic and attack tree analysis to obtain a detailed assessment of attacker behaviour and possible consequences with regard to cyber-physical systems. The approach allows for understanding attack paths and for creating appropriate countermeasures. However, further subjectivity may be introduced into the prediction process through the application of fuzzy logic, thereby influencing the model's reliability. In addition, attack tree analysis becomes increasingly complex and difficult to handle as the number of possible attack paths increases. Table 5 and Fig. 4 summarize the predictive models identified in the reviewed literature.

Crucially, this review provides a more comprehensive analysis of existing research gaps. It identifies the limited

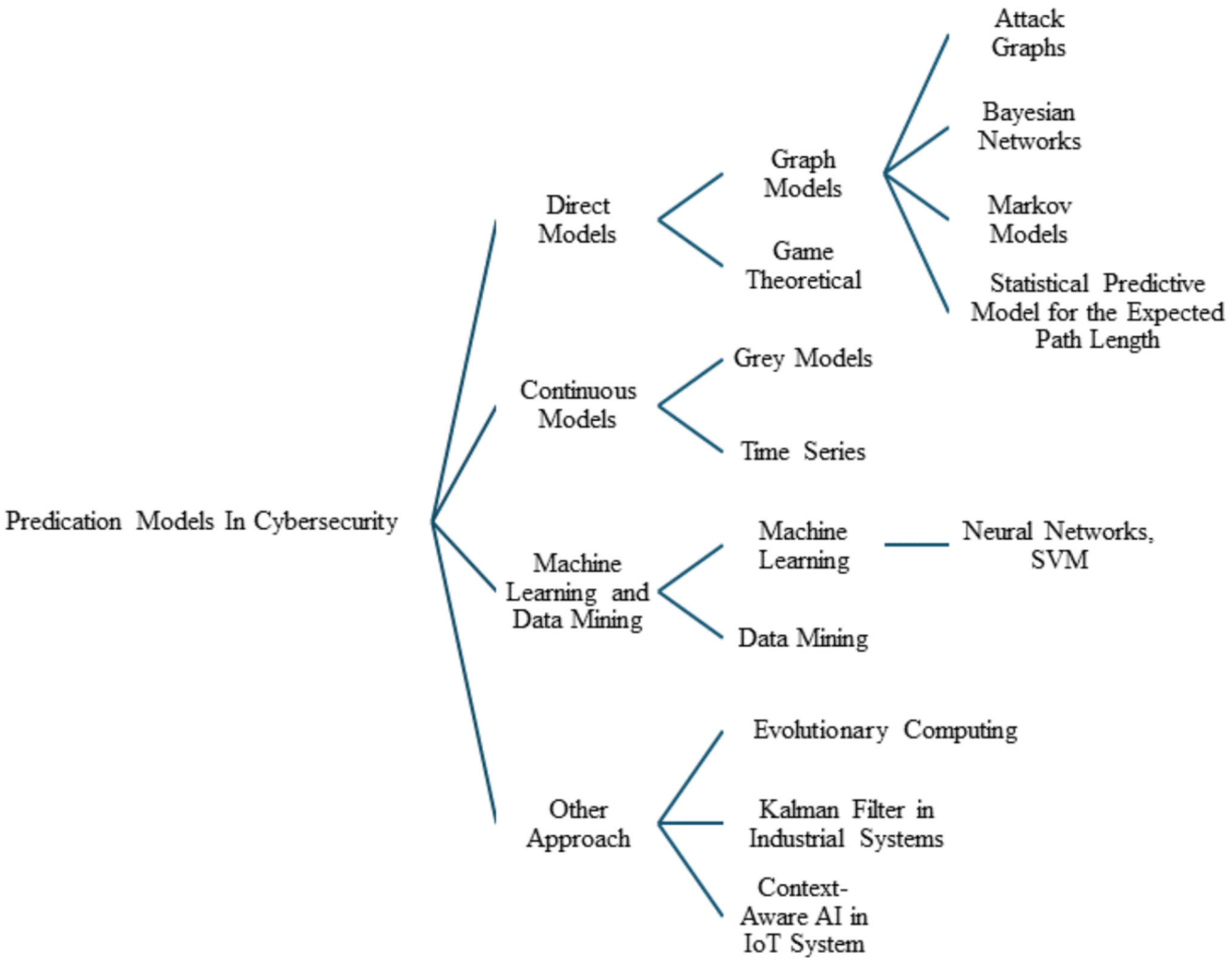


Fig. 3 Predictive methods in cybersecurity

exploration of explainable AI (XAI) in cybersecurity for manufacturing, hindering trust and adoption by non-experts. The need for more robust evaluation methodologies, specifically tailored to the dynamic and real-time nature of industrial systems, is also highlighted. Moreover, the paper emphasizes the lack of comprehensive frameworks that seamlessly integrate these advanced predictive models into existing industrial cybersecurity architectures. Future research directions are proposed, advocating for the development of more interpretable AI models, the creation of standardized evaluation benchmarks for industrial cybersecurity prediction, and the design of practical, integrated frameworks for proactive threat mitigation in Industry 4.0 manufacturing. Therefore, developing a predictive cybersecurity model for the manufacturing industry is necessary. Several papers have been published to help bridge this gap [102–108].

5.2 Paper contributions

This review paper makes several key contributions to the understanding of cybersecurity in Industry 4.0 manufacturing. It provides a structured, in-depth synthesis of the diverse predictive methods used to enhance cybersecurity in these systems, enabling researchers and practitioners to understand the current state of the art in threat prediction. The paper also critically examines the types of data used by different predictive approaches, highlighting the importance of data quality, relevance, and availability for effective threat prediction and identifying potential gaps in data utilization. Furthermore, through a systematic review, the paper identifies significant research gaps, particularly concerning the practical implementation of predictive models and the need for robust validation techniques, and proposes concrete directions for future research. By emphasizing the importance of predictive approaches, this review contributes to the development of more proactive cybersecurity strategies,

Table 5 Predictive Models Across Various Industries: Applications and References

No	Implementation field	Predictive models	References
1	Healthcare	Neural networks for phishing and trojan content detection in Internet of Things systems	[93]
2	Finance	K-means, influenced association classifier, J48 prediction tree for predicting cybercrimes in the banking sector	[94]
3	Robotics and automation	Fuzzy logic, neural networks, and genetic algorithms for autonomous decision-making and robot control	[95]
4	Business and marketing	Artificial intelligence-driven anomaly detection models, machine learning for intrusion detection, deep learning for malware classification	[96]
5	Manufacturing and supply chain	Machine learning (logistic regression, support vector machine, random forest, decision tree) for predicting cyber threats in supply chain systems	[97]
6	Energy	Deep belief network for predicting cyberattacks on smart grids	[98]
7	Government	Epidemiological modelling of cyber threats, using susceptible, exposed, infectious, recovered (SEIR) and herd immunity to enhance cybersecurity in digital governance	[99]
8	Food	Machine learning models (K-nearest neighbour, decision tree), deep learning models (convolutional neural network-long short-term memory) for detecting cyberattacks on industry classification schemes	[100]
9	Information and communication	Data mining-based framework using the J48 decision tree algorithm for cyberattack prediction	[101]

underscoring the shift from reactive to anticipatory security measures, which is crucial for mitigating evolving cyber threats in Industry 4.0. Finally, the paper serves as a valuable, consolidated resource for both researchers and industry practitioners, offering a comprehensive overview of relevant literature and facilitating a deeper understanding of the challenges and opportunities in this field.

6 Conclusion

This study explored the prediction of cyber threats in cybersecurity frameworks, which are attributed to the absence of robust, objective security measures and the consequent neglect of cyber threat anticipation during the initial stages of system development. While each predictive model offers unique advantages in enhancing cybersecurity measures across different domains, they also present specific challenges and limitations. Addressing these drawbacks is essential for maximising the effectiveness of these models in real-world applications. A comprehensive literature review of cybersecurity predictive models and frameworks identified a significant gap in predicting cyber threats. This study suggests that integrating AI and ML techniques offers a viable approach to addressing this challenge.

A range of cybersecurity countermeasures for Industry 4.0 environments has been established. While various approaches to predicting cyberattacks exist, such as 'Predicting Cyber Attacks on Industrial Systems Using the Kalman Filter', 'Predicting the Behavior of Attackers and the Consequences of Attacks Against Cyber-Physical Systems', 'Predicting Cybersecurity Vulnerabilities', and 'Predictive Analysis of Ransomware Attacks Using Context-Aware AI in IoT Systems', a critical need to develop a new predictive model that is proactive and capable of preventing cyberattacks remains. Moreover, the analysed papers do not address

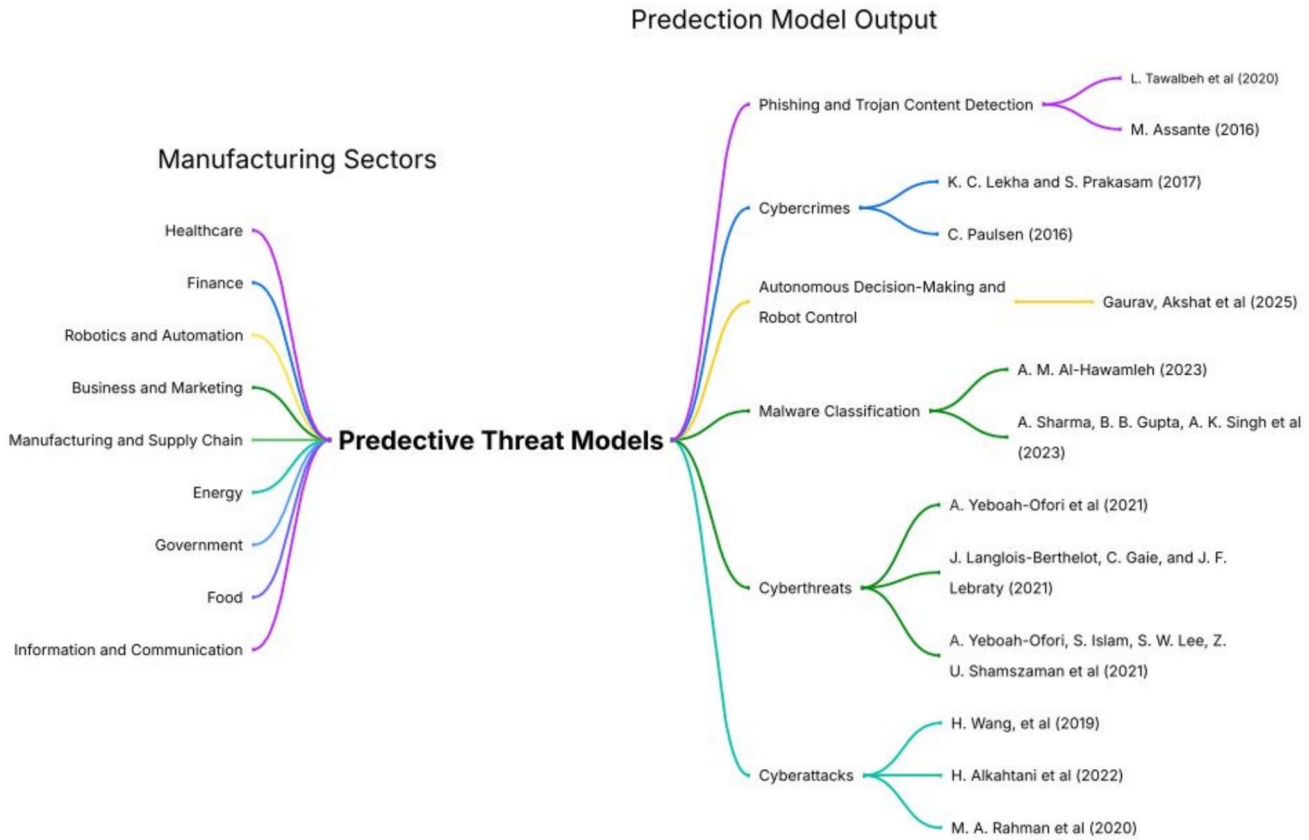


Fig. 4 Taxonomy of predictive models

cybersecurity from a purely management perspective but rather focus on the IT aspect. Adopting a management perspective can help a company effectively implement new organisational practices and change management initiatives, ultimately leading to robust cybersecurity. In conclusion, while each cybersecurity predictive model offers distinct advantages, such as improved detection accuracy and early prediction, they also face notable challenges, including substantial computational requirements, reliance on extensive training datasets, and integration complexities. A thorough analysis of these models indicates that their effectiveness depends largely on the quality of the data, the complexity of the systems they are designed to protect, and the availability of resources for their implementation.

Acknowledgements The author would like to express sincere gratitude to Cranfield University for providing the academic environment and resources that made this research possible. Special thanks are extended to Dr. Sandeep Jagtap and Dr. Konstantinos Salonitis, for their guidance, constructive feedback, and continuous encouragement throughout this study. Appreciation is also extended to the participants and organizations that contributed valuable insights to support the research.

Author contributions Adel Alqudhaibi: Conceptualization, Methodology, Investigation, Writing – Original Draft, Data Curation, and Visualization. Abdulmosen Aloseel: Formal Analysis, Review & Editing, and Supervision. Amr Munshi: Resources, Validation, and Review & Editing. Thamer Alsharif: Literature Review and Data Analysis. Sandeep Jagtap: Supervision, Project Administration, Review & Editing. Konstantinos Salonitis: Supervision, Methodology Refinement, and Final Approval of the Manuscript. All authors have read and agreed to the published version of the manuscript.

Funding Open access funding provided by Lund University. This research received no external funding.

Data availability Not applicable.

Declarations

Conflict of interest The authors declare that they have no competing interests.

Ethical and consent to participate Not applicable.

Consent to publish Not applicable.

Institutional review board Not applicable.

Informed consent Not applicable.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes

were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Culot, G., Fattori, F., Podrecca, M., Sartor, M.: Addressing industry 4.0 cybersecurity challenges. IEEE Eng. Manag. Rev. **47**(3), 79–86 (2019). https://doi.org/10.1109/EMR.2019.2927559
2. Lezzi, M., Lazoi, Ma., Corallo, A.: Cybersecurity for industry 4.0 in the current literature: a reference framework. Comput. Ind. **103**, 97–110 (2018). https://doi.org/10.1016/j.compind.2018.09.004
3. Ii, P. and A:. Cisco, Cisco. Annual cybersecurity report, (2018) https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.
4. Bauer, H., Scherf, G., Tann, V., Klinkhammer, L.: How CEOs can tackle the challenge of cybersecurity in the age of the internet of things (2017) (accessed 2 September 2024), [online] Available: https://www.mckinsey.de/~/media/McKinsey/Featured%20Insights/Internet%20of%20Things/Our%20Insights/Six%20ways%20CEOs%20can%20promote%20cybersecurity%20in%20the%20IoT%20age/How-CEOs-can-tackle-the-challenge-of-cybersecurity-in-the-age-of-the-Internet-of-Things.pdf.
5. Höse, K., Amaral, A., Götze, U., et al.: Manufacturing flexibility through industry 4.0 technological concepts—impact and assessment. Glob. J. Flex. Syst. Manag. **24**, 271–289 (2023). https://doi.org/10.1007/s40171-023-00339-y
6. Freitag, B., Häfner, L., Pfeuffer, V., et al.: Evaluating investments in flexible on-demand production capacity: a real options approach. Bus. Res. **13**, 133–161 (2020). https://doi.org/10.1007/s40685-019-00105-w
7. Raoufi, K., Sutherland, J.W., Zhao, F., et al.: Current state and emerging trends in advanced manufacturing: smart systems. Int. J. Adv. Manuf. Technol. (2024). https://doi.org/10.1007/s00170-024-14279-z
8. Pereira, A.C., Romero, F.: A review of the meanings and the implications of the Industry 4.0 concept. Procedia Manuf. **13**, 1206–1214 (2017). https://doi.org/10.1016/j.promfg.2017.09.032
9. Toussaint, M., Krima, S., Panetto, H.: Industry 4.0 data security: a cybersecurity frameworks review. J. Ind. Inf. Integr. **39**, 100604 (2024). https://doi.org/10.1016/j.jii.2024.100604
10. Unger, H., Börner, F., Müller, E.: Context related information provision in Industry 4.0 environments. Procedia Manuf. **11**, 796–805 (2017). https://doi.org/10.1016/j.promfg.2017.07.181
11. Motyl, B., Baronio, G., Uberti, S., Speranza, D., Filippi, S.: How will change the future engineers' skills in the industry 4.0 framework? A questionnaire survey. Procedia Manuf. **11**, 1501–1509 (2017). https://doi.org/10.1016/j.promfg.2017.07.282
12. Rad, F.F., Oghazi, P., Palmié, M., Chirumalla, K., Pashkevich, N., Patel, P.C., Sattari, S.: Industry 4.0 and supply chain performance: a systematic literature review of the benefits, challenges, and critical success factors of 11 core technologies. Ind. Mark. Manag. **105**, 268–293 (2022). https://doi.org/10.1016/j.indmarman.2022.06.009
13. Safitra, M.F., Lubis, M., Fakhrurroja, H.: Counterattacking cyber threats: a framework for the future of cybersecurity. Sustainability **15**(18), 13369 (2023). https://doi.org/10.3390/su151813369
14. Büthe, T., Alshadafan, A.F.: The international electrotechnical commission. In: Delimatsis, P., Bijlmakers, S., Borowicz, M.K. (eds.) The evolution of transnational rule-makers through crises, pp. 310–342. Cambridge University Press, Cambridge (2023)
15. Tripathi, S., Gupta, M.: A holistic model for global industry 4.0 readiness assessment. Benchmarking Int. J. **28**(10), 3006–3039 (2021). https://doi.org/10.1108/BIJ-07-2020-0354
16. Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W., Ueda, K.: Cyber-physical systems in manufacturing. CIRP Ann. **65**(2), 621–641 (2016). https://doi.org/10.1016/j.cirp.2016.06.005
17. Gregolinska, E., Khanam, R., Lefort, F., Parthasarathy, P.: Capturing the true value of industry 4.0. (2022), (accessed 2 September 2024), [online] Available, https://www.mckinsey.com/capabilities/operations/our-insights/capturing-the-true-value-of-industry-four-point-zero.
18. Phillips, R.L., Ormsby, R.: Industry classification schemes: an analysis and review. J. Bus. Finance Librariansh. **21**(1), 1–25 (2016). https://doi.org/10.1080/08963568.2015.1110229
19. Schatz, D., Bashroush, R., Wall, J.: Towards a more representative definition of cyber security. J. Dig. Forens. Secur. Law (2017). https://doi.org/10.15394/jdfsl.2017.1476
20. Mohamed, M.: Challenges and benefits of industry 4.0: an overview. Int. J. Supply Oper. Manag. **5**(3), 256–265 (2018). https://doi.org/10.22034/2018.3.7
21. MacDougall, W.: Industrie 4.0: smart manufacturing for the future, Germany Trade & Invest. (2014)
22. McKinsey Digital.: Industry 4.0: how to navigate the digitalization of the manufacturing sector. (2015) (accessed 17 September 2024), https://www.mckinsey.com/~/media/mckinsey/business%20functions/operations/our%20insights/industry%2040%20how%20to%20navigate%20digitization%20of%20the%20manufacturing%20sector/industry-40-how-to-navigate-digitization-of-the-manufacturing-sector.ashx
23. Deloitte.: Industry 4.0. challenges and solutions for the digital transformation and use of exponential technologies. 45774ADeloitte Zurich Switzerland. (2015) (accessed 19 September 2024), https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/manufacturing/ch-en-manufacturing-industry-4-0-24102014.pdf.
24. IBM.: What is industry 4.0?. (2020) (accessed 10 September 2024), https://www.ibm.com/topics/industry-4-0.
25. Z. Al Sati, (2022)"Why Energy Companies Must Prioritize Cybersecurity to Leverage Industry 4.0," (accessed 23 May 2022), https://www.siemens-energy.com/mea/en/news/magazine/fully-benefit-from-industry-40-gccs-critical-must-ziad-al-sati.html.
26. Moteff, J., Ave, I.: CRS report for congress received through the CRS web risk management and critical infrastructure protection: assessing, integrating, and managing threats, vulnerabilities and consequences. Risk Manage. (2004) (accessed 14 September 2024), http://www.fas.org/sgp/crs/RL32561.pdf.
27. Chaudhary, P., Singh, A.K., Gupta, B.B.: Dynamic multiphase DDoS attack identification and mitigation framework to secure SDN-based fog-empowered consumer IoT networks. Comput. Electr. Eng. (2025). https://doi.org/10.1016/j.compeleceng.2025.110226
28. George, A.S., Baskar, T., Srikaanth, P.B.: Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Part. Univ. Int. Innovat. J. **2**(1), 51–75 (2024). https://doi.org/10.5281/zenodo.10639463
29. Sharma, A., Gupta, B.B., Singh, A.K., et al.: Advanced persistent threats (APT): evolution, anatomy, attribution and countermeasures. J. Ambient. Intell. Human Comput. **14**, 9355–9381 (2023). https://doi.org/10.1007/s12652-023-04603-y
30. Al-Matari, O.M.M., Helal, I.M.A., Mazen, S.A., Elhennawy, S.: Integrated framework for cybersecurity auditing. Inf. Secur. J.

Glob. Perspect. **30**(4), 189–204 (2020). https://doi.org/10.1080/19393555.2020.1834649
31. Rudner, M.: Cyber-threats to critical national infrastructure: an intelligence challenge. Int. J. Intell. Counterintell. **26**(3), 453–481 (2013). https://doi.org/10.1080/08850607.2013.780552
32. Thakur, M.: Cyber security threats and countermeasures in digital age. J. Appl. Sci. Educ. **4**(1), 1–20 (2024). https://doi.org/10.54060/a2zjournals.jase.42
33. Keay, S., Kirby, S.: Defining vulnerability: from the conceptual to the operational. Polic. J. Poli. Pract. **12**(4), 428–438 (2018). https://doi.org/10.1093/police/pax046
34. Rostami, M., Bucking, S.: A framework for integrating reliability, robustness, resilience, and vulnerability to assess system adaptivity. ASME Int. Mech. Eng. Congr. Exposit. Proc. (IMECE) **13**, 1–8 (2021). https://doi.org/10.1115/IMECE2021-73021
35. Kampourakis, K.E., Gkioulos, V., Kavallieratos, G., Lin, J.C.: Digital twin-enabled incident detection and response: a systematic review of critical infrastructures applications. Int. J. Inf. Secur. **24**(5), 1–42 (2025)
36. Mumby, P.J., Chollett, I., Bozec, Y.M., Wolff, N.H.: Ecological resilience, robustness and vulnerability: how do these concepts benefit ecosystem management? Curr. Opin. Environ. Sustain. **7**, 22–27 (2014). https://doi.org/10.1016/j.cosust.2013.11.021
37. Bazaz, A., Arthur, J.D.: Towards a taxonomy of vulnerabilities. Proc. Ann. Hawaii Int. Conf. Syst. Sci. (2007). https://doi.org/10.1109/HICSS.2007.566
38. International Telecommunication Union (ITU), Definition of cybersecurity (accessed 23 May 2022), https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets.
39. National Institute of Standards and Technology (NIST): Developing cyber-resilient systems: a systems security engineering approach. (2021) https://doi.org/10.6028/NIST.SP.800-160v2r1.
40. National Initiative for Cybersecurity Careers and Studies (NICCS): Compilation of existing cybersecurity and information security related definitions. (2014) (accessed 18 September 2024), https://static.newamerica.org/attachments/175-compilation-of-existing-cybersecurity-and-information-security-related-definitions/OTI_Compilation_of_Existing_Cybersecurity_and_Information_Security_Related_Definitions_Updated122015.pdf.
41. Mullet, V., Sondi, P., Ramat, E.: A review of cybersecurity guidelines for manufacturing factories in Industry 4.0. IEEE Access **9**, 23235–23263 (2021). https://doi.org/10.1109/ACCESS.2021.3056650
42. Wylde, V., Rawindaran, N., Lawrence, J., et al.: Cybersecurity, data privacy and blockchain: a review. SN Comput. Sci. **3**, 127 (2022). https://doi.org/10.1007/s42979-022-01020-4
43. Tuptuk, N., Hailes, S.: Security of smart manufacturing systems. J. Manuf. Syst. **47**, 93–106 (2018). https://doi.org/10.1016/j.jmsy.2018.04.007
44. Ani, U.P.D., He, H.(M.), Tiwari, A.: Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. J. Cyber Sec. Technol. **1**(1), 32–74 (2016). https://doi.org/10.1080/23742917.2016.1252211
45. Batteau, A.W.: Creating a culture of enterprise cybersecurity. Int. J. Busin. Anthropol. (2011). https://doi.org/10.33423/ijba.v2i2.1179
46. Chowdhury, N., Gkioulos, V.: Key competencies for critical infrastructure cyber-security: a systematic literature review. Inf. Comput. Secur. **29**(5), 697–723 (2021). https://doi.org/10.1108/ICS-07-2020-0121
47. Alexander, O., Belisle, M., Steele, J.: MITRE ATT&CK ® for industrial control systems: design and philosophy. (2020) pp. 1–43, (accessed 19 September 2024), https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf.
48. Assante, M.: Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems Security Blog, (2016) pp. 1–26, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
49. da Veiga, A., Astakhova, L.V., Botha, A., Herselman, M.: Defining organisational information security culture—perspectives from academia and industry. Comput. Secur. **92**, 101713 (2020). https://doi.org/10.1016/j.cose.2020.101713
50. Dojkovski, S., Lichtenstein, S., Warren, M.: Developing information security culture in small and medium size enterprises: Australian case studies. Proceedings of the 6th European conference on information warfare and security, pp. 55–65 (2007)
51. Bada, M., Nurse, J.R.C.: Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Inf. Comput. Secur. **27**(3), 393–410 (2019). https://doi.org/10.1108/ICS-07-2018-0080
52. Kshetri, N.: Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun. Policy **41**(10), 1027–1038 (2017). https://doi.org/10.1016/j.telpol.2017.09.003
53. Sonkor, M.S., de García Soto, B.: Operational technology on construction sites: a review from the cybersecurity perspective. J. Constr. Eng. Manag. (2021). https://doi.org/10.1061/(asce)co.1943-7862.0002193
54. Murray, G., Johnstone, M.N., Valli, C.: The convergence of IT and OT in critical infrastructure. Proceedings of the 15th Australian Information Security Management Conference, AISM 2017, pp. 149–155, (2017) https://doi.org/10.4225/75/5a84f7b595b4e.
55. National Defense Industrial Association (NDIA): Cybersecurity for manufacturing networks a white paper. pp. 1–88 (2017) http://www.ndia.org/-/media/sites/ndia/divisions/working-groups/cfam/ndia-cfam-2017-white-paper-20171023.ashx?la=en.
56. Mittal, S., Khan, M.A., Romero, D., Wuest, T.: A critical review of smart manufacturing & Industry 4.0 maturity models: implications for small and medium-sized enterprises (SMEs). J. Manuf. Syst. **49**, 194–214 (2018). https://doi.org/10.1016/j.jmsy.2018.10.005
57. Paulsen, C.: Cybersecuring small businesses. Computer (Long Beach. Calif.) **49**(8), 92–97 (2016). https://doi.org/10.1109/MC.2016.223
58. Wei, X., Jiang, X.: Comprehensive Analysis of Network Security Situational Awareness Methods and Models. Proceedings of the IEEE 2nd Int. Symp. Instrum. Meas. Sensor Netw. Autom. (IMSNA), pp. 176–179 (2013) https://doi.org/10.1109/IMSNA.2013.6743245.
59. Yang, S.J., Du, H., Holsopple, J., Sudit, M.: Attack projection. In: Kott, A., Wang, C., Erbacher, R. (eds.) Cyber defense and situational awareness. Advances in information security, vol. 62. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11391-3_12
60. Leau, Y.-B., Manickam, S.: Network Security Situation Prediction: A Review and Discussion, pp. 424–435. Springer, Heidelberg, Germany (2015). https://doi.org/10.1007/978-3-662-46742-8_39
61. Gheyas, I.A., Abdallah, A.E.: Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Anal **1**, 6 (2016). https://doi.org/10.1186/s41044-016-0006-0
62. Ramaki, A.A., Atani, R.E.: A survey of IT early warning systems: architectures, challenges, and solutions. Secur. Commun. Networks **9**(17), 4751–4776 (2016). https://doi.org/10.1002/sec.1647

63. West, J.: A prediction model framework for cyber-attacks to precision agriculture technologies. J. Agric. Food Inf. **19**(4), 307–330 (2018). https://doi.org/10.1080/10496505.2017.1417859
64. Abdlhamed, M., Kifayat, K., Shi, Q., Hurst, W.: Intrusion prediction systems. In: Alsmadi, I., Karabatis, G., Aleroud, A. (eds.) Information fusion for cyber-security analytics. Studies in computational intelligence, vol. 691. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-44257-0_7
65. King, Z.M., Henshel, D.S., Flora, L., Cains, M.G., Hoffman, B., Sample, C.: Characterizing and measuring maliciousness for cybersecurity risk assessment. Front. Psychol. **9**(FEB), 1–19 (2018). https://doi.org/10.3389/fpsyg.2018.00039
66. Ahmed, A.A., Zaman, N.A.K.: Attack intention recognition: a review. Int. J. Netw. Secur. **19**(2), 244–250 (2017). https://doi.org/10.6633/IJNS.201703.19(2).09
67. Fernandes, D.A.B., Soares, L.F.B., Gomes, J.V., et al.: Security issues in cloud environments: a survey. Int. J. Inf. Secur. **13**, 113–170 (2014). https://doi.org/10.1007/s10207-013-0208-7
68. Mathane, V., Lakshmi, P.V.: Predictive analysis of ransomware attacks using context-aware AI in IoT systems. Int. J. Adv. Comput. Sci. Appl. (2021). https://doi.org/10.14569/IJACSA.2021.0120432
69. Datta, P., Lodinger, N., Namin, A. S., Jones, K. S.: Predicting consequences of cyber-attacks. 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, pp. 2073–2078, (2020) https://doi.org/10.1109/BigData50022.2020.9377825.
70. Kaluarachchi, P., Tsokos, C., Rajasooriya, S.: Cybersecurity: a statistical predictive model for the expected path length. J. Inf. Secur. **7**, 112–128 (2016). https://doi.org/10.4236/jis.2016.73008
71. Daria, L., Dmitry, Z., Anastasiia, Y.: Predicting cyber attacks on industrial systems using the Kalman filter. 2019 third world conference on smart trends in systems security and sustainability (WorldS4), London, UK, pp. 317–321 (2019) https://doi.org/10.1109/WorldS4.2019.8904038.
72. Veksler, V.D., Buchler, N., LaFleur, C.G., Yu, M.S., Lebiere, C., Gonzalez, C.: Cognitive models in cybersecurity: learning from expert analysts and predicting attacker behavior. Front. Psychol. **11**, 1049 (2020). https://doi.org/10.3389/fpsyg.2020.01049
73. Orojloo, H., Abdollahi Azgomi, M.: Predicting the behavior of attackers and the consequences of attacks against cyber-physical systems. Secur. Commun. Networks **9**(18), 6111–6136 (2016). https://doi.org/10.1002/sec.1761
74. Abraham, S., Nair, S.: A novel architecture for predictive cybersecurity using non-homogenous markov models. IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland **2015**, 774–781 (2015). https://doi.org/10.1109/Trustcom.2015.446
75. Movahedi, Y., Cukier, M., Gashi, I.: Predicting the discovery pattern of publically known exploited vulnerabilities. IEEE Trans. Dependable Secur. Comput. **19**(2), 1181–1193 (2022). https://doi.org/10.1109/TDSC.2020.3014872
76. Ben Fredj, O., Mihoub, A., Krichen, M., Cheikhrouhou, O., Derhab, A.: CyberSecurity attack prediction: a deep learning approach. 13th International Conference on Security of Information and Networks (SIN 2020). Association for Computing Machinery, New York, NY, USA, Article 5, pp. 1–6 (2021) https://doi.org/10.1145/3433174.3433614.
77. Alattas, K., Mardani, A.: A novel extended internet of things (IoT) cybersecurity protection based on adaptive deep learning prediction for industrial manufacturing applications. Environ. Dev. Sustain. **24**, 9464–9480 (2022). https://doi.org/10.1007/s10668-021-01835-w
78. Pokhrel, A., Katta, V., Colomo-Palacios, R.: Digital twin for cybersecurity incident prediction: a multivocal literature review. Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, pp. 671–678 (2020) https://doi.org/10.1145/3387940.3392199.
79. Lei, J., Li, Z. –t.: Using network attack graph to predict the future attacks. 2007 Second International Conference on Communications and Networking in China, Shanghai, China, pp. 403–407, (2007) https://doi.org/10.1109/CHINACOM.2007.4469413.
80. Schwab, K.: The fourth industrial revolution, world economic forum. (2017) (accessed 30 June 2024), https://www.weforum.org/focus/fourth-industrial-revolution/
81. Akwetey, H. M., Danquah, P.: Predicting cyber-attack using cyber situational awareness: the case of independent power producers (IPPs). arXiv preprint arXiv:2202.01778, (2022) https://doi.org/10.48550/arXiv.2202.01778.
82. Goh, K.H., Wang, L., Yeow, A.Y.K., et al.: Artificial intelligence in sepsis early prediction and diagnosis using unstructured data in healthcare. Nat. Commun. **12**, 711 (2021). https://doi.org/10.1038/s41467-021-20910-4
83. da Silveira Dib, M., Ribeiro, B., Prates, P.: Federated learning as a privacy-providing machine learning for defect predictions in smart manufacturing. ASTM International. Smart Sustain. Manuf. Syst. (2021). https://doi.org/10.1520/SSMS20200029
84. Liu, C.: Risk prediction of digital transformation of manufacturing supply chain based on principal component analysis and backpropagation artificial neural network. Alex. Eng. J. (2021). https://doi.org/10.1016/j.aej.2021.06.010
85. Bilge, L., Han, Y., Dell'Amico, M.: RiskTeller: Predicting the Risk of Cyber Incidents," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). Association for Computing Machinery, New York, NY, USA, pp. 1299–1311 (2017) https://doi.org/10.1145/3133956.3134022.
86. Hutchens, J.: The language of deception: weaponizing next generation AI. Wiley (2023)
87. Oueslati, N.E., Mrabet, H., Jemai, A. and Alhomoud, A.: Comparative study of the common cyber-physical attacks in industry 4.0. 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Tunis, Tunisia, pp. 1–7 (2019) https://doi.org/10.1109/IINTEC48298.2019.9112097.
88. Ferland, J.: Cyber insurance-what coverage in case of an alleged act of war? Questions raised by the Mondelez v. Zurich case. Comput. Law Secur. Rev. **35**(4), 369–376 (2019). https://doi.org/10.1016/j.clsr.2019.06.003
89. Manning, L., Kowalska, A.: The threat of ransomware in the food supply chain: a challenge for food defence. Trends in Organized Crime, pp. 1–29 (2023) https://doi.org/10.1007/s12117-023-09516-y.
90. Greig, J.: Marine industry giant Brunswick corporation lost $85 million in cyberattack, CEO Confirms. The Record (2023) (accessed 5 September 2024), https://therecord.media/marine-industry-giant-brunswick-lost-millions.
91. Muncaster, P.: CEO Sacked after $56 million whaling attack. Infosecurity Magazine (2016) (accessed 30 September 2024), https://www.infosecurity-magazine.com/news/ceo-sacked-after-56-million/.
92. Al-Ansari, A. O., Alsubait, T. M.: Predicting cyber threats using machine learning for improving cyber supply chain security. 2022 fifth national conference of Saudi computers colleges (NCCC), Makkah, Saudi Arabia, pp. 123–130 (2022) https://doi.org/10.1109/NCCC57165.2022.10067692.
93. Tawalbeh, L.A., Muheidat, F., Tawalbeh, M., Quwaider, M. and Saldamli, G.: Predicting and preventing cyber attacks during COVID-19 time using data analysis and proposed secure iot layered model. 2020 fourth international conference on multimedia computing, networking and applications (MCNA), Valencia, Spain, pp. 113–118 (2020) https://doi.org/10.1109/MCNA50957.2020.9264301.
94. Lekha, K. C., Prakasam, S.: Data mining techniques in detecting and predicting cyber crimes in banking sector. 2017 international

conference on energy, communication, data analytics and soft computing (ICECDS), pp. 1639–1643, IEEE. (2017)
95. Gaurav, A., et al.: AI-based model for securing cognitive IoT devices in advance communication systems. Int. J. Cogn. Comput. Eng. (2025). https://doi.org/10.1016/j.ijcce.2025.01.009
96. Al-Hawamleh, A.M.: Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. Momentum **3**(14), 15 (2023). https://doi.org/10.14569/IJACSA.2023.0140292
97. Yeboah-Ofori, A., Islam, S., Lee, S.W., Shamszaman, Z.U., Muhammad, K., Altaf, M., Al-Rakhami, M.S.: Cyber threat predictive analytics for improving cyber supply chain security. IEEE Access **9**, 94318–94337 (2021). https://doi.org/10.1109/ACCESS.2021.3087109
98. Wang, H., Ruan, J., Ma, Z., Zhou, B., Fu, X., Cao, G.: Deep learning aided interval state prediction for improving cyber security in energy internet. Energy **174**, 1292–1304 (2019). https://doi.org/10.1016/j.energy.2019.03.009
99. Langlois-Berthelot, J., Gaie, C., Lebraty, J.F.: Epidemiology inspired cybersecurity threats forecasting models applied to e-government. In: Gaie, C., Mehta, M. (eds.) Transforming public services—combining data and algorithms to fulfil citizen's expectations intelligent systems reference library, vol. 252. Springer, Cham (2021). https://doi.org/10.1007/978-3-031-55575-6_6
100. Alkahtani, H., Theyazn, H.H.A.: Developing cybersecurity systems based on machine learning and deep learning algorithms for protecting food security systems: industrial control systems. Electronics **11**(11), 1717 (2022). https://doi.org/10.3390/electronics11111717
101. Rahman, M.A., Al-Saggaf, Y. and Zia, T.: A data mining framework to predict cyber attack for cyber security. 2020 15th IEEE conference on industrial electronics and applications (ICIEA), Kristiansand, Norway, pp. 207–212 (2020) https://doi.org/10.1109/ICIEA48937.2020.9248225.
102. Alqudhaibi, A., Aloseel, A., Jagtap, S., Salonitis, K.: Identifying and predicting cybersecurity threats in industry 4.0 based on the motivations towards a critical infrastructure. In: Advances in manufacturing technology XXXV, pp. 10–16. IOS Press (2022). https://doi.org/10.3233/ATDE220599
103. Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., Salonitis, K.: Predicting cybersecurity threats in critical infrastructure for Industry 4.0: a proactive approach based on attacker motivations. Sensors **23**(9), 4539 (2023). https://doi.org/10.3390/s23094539
104. Alqudhaibi, A., Deshpande, S., Jagtap, S., Salonitis, K.: Towards a sustainable future: developing a cybersecurity framework for manufacturing. Technol. Sustain. **2**(4), 372–387 (2023). https://doi.org/10.1108/TECHS-05-2023-0022
105. Alqudhaibi, A., Krishna, A., Jagtap, S., et al.: Cybersecurity 4.0: safeguarding trust and production in the digital food industry era. Discov. Food **4**, 2 (2024). https://doi.org/10.1007/s44187-023-00071-7
106. Alqudhaibi, A., Albarrak, M., Jagtap, S., Williams, N., Salonitis, K.: Securing industry 4.0: assessing cybersecurity challenges and proposing strategies for manufacturing management. Cyber Sec. Appl. (2024). https://doi.org/10.1016/j.csa.2024.100067
107. Alqudhaibi, A., Krishna, A., Jagtap, S., Afy-Shararah, M., Salonitis, K.: Safeguarding food industry: understanding cyber threats and ensuring cybersecurity. Eng. Proc. **40**(1), 11 (2023). https://doi.org/10.3390/engproc2023040011
108. Dandamudi, S.R.P., Sajja, J., Khanna, A.: Advancing cybersecurity and data networking through machine learning-driven prediction models. Int. J. Innovat. Res. Comput. Sci. Technol. **13**(1), 26–33 (2025). https://doi.org/10.55524/ijircst.2025.13.1.4

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



https://dspace.org/

Proactive cybersecurity in industry 4.0: a survey of cybersecurity threat prediction approaches in manufacturing systems

Alqudhaibi, Adel; Albarrak, Majed; Aloseel, Abdulmosen; Munshi, Amr; Alsharif, Thamer ...

2026-02
Springer
https://doi.org/10.1007/s10207-025-01188-9
Alqudhaibi A, Albarrak M, Aloseel A, et al., (2026) Proactive cybersecurity in industry 4.0: a survey of cybersecurity threat prediction approaches in manufacturing systems. International Journal of Information Security, Volume 25, Issue 1, February 2026, Article number 14

Downloaded from a DSpace repository. https://dspace.org/