A Review of Advanced Cyber Threat Detection Techniques in Critical Infrastructure: Evolution, Current State, and Future Directions

MURITALA AMINU[1], AYOKUNLE AKINSANYA[2], OYEWALE OYEDOKUN[3], OLADAYO TOSIN AKINWANDE[4]

[1]*Department of Cyber Security, Dell Inc*

[2]*Department of Information Systems, Bowie State University*

[3]*Department of Applied Statistics, Western Illinois University*

[4]*Department of Software Engineering, Veritas University*

Abstract- Cyber threats pose substantial risks to critical infrastructure, necessitating the development and implementation of advanced detection techniques to protect against possible attacks. This review examines the evolution, current state, and prospects of cyber threat detection techniques in critical infrastructure. Conventional signature-based approaches provided more sophisticated strategies like anomaly detection, machine learning algorithms, and behavior-based analysis in the evolution of cyber threat detection techniques. Although these techniques offer promising abilities in terms of identifying and reducing cyber threats, they also have several drawbacks, such as the speed at which threats are evolving, the complexity of environments involving critical infrastructure, and the vulnerabilities brought about by novel technologies. The future of cyber threat detection in critical infrastructure has the potential to improve resilience and lessen the risks posed by cyber threats in a world that is increasingly becoming digitally connected and interconnected by embracing emerging technologies and implementing proactive security strategies.

Indexed Terms- Interconnectivity, Critical Infrastructure, Threat, Network Security, Safety

I. INTRODUCTION

As the world becomes increasingly interconnected, critical infrastructure, including energy grids, transportation networks, and communication systems, remains the backbone of modern society. Critical infrastructures (CI) are those material resources, services, networks, information technology systems, and infrastructure assets that, in the event of damage or destruction, would have a major impact on the vital functions of society, such as the supply chain, health, and security, as well as the social well-being of the population (De Felice et al., 2022). However, these systems are now more susceptible to cyberattacks due to their growing digitization and interconnectedness (Chehri et al., 2021).

Due to the recent advances in information and communication technology (ICT), the world is rapidly becoming more digital (Alqudhaibi et al., 2023) and this has created an array of growth opportunities. Nonetheless, 30% of CI institutions, as predicted by Gartner (2021) will have a security breach by 2025, which could force the shutdown of mission-critical cyber-physical systems (CPS). Additionally, the report also projects that by 2025, attackers will have successfully turned a CI's CPS into a weapon, endangering lives (Tehrani, 2020). Cyberattacks have increased in all industries, with hackers taking advantage of vulnerable information such as the personal data of employees and customers as well as the intellectual property of institutions (Latino & Menegoli, 2022; Oueslati et al., 2019). Thus, understanding the cost of an information compromise requires taking into account several variables, including the location and activity of the company, the sensitivity of the stolen data, and the extent of the security breach, which may have unanticipated effects and damages.

Cyberattacks that target vital infrastructure present serious risks, from threats to national security to the interruption of vital services (Li & Liu, 2021). In order to combat constantly changing threats, threat detection tools and techniques are developing, with an emphasis on early detection and intervention to minimize damage and data loss (Sarker, 2021). Specifically, the need for robust security protocols in CI sectors has increased due to the emergence of advanced cyber threats, such as ransomware, malware, and targeted attacks. Antivirus software and firewalls are examples of traditional security measures that are no longer adequate for preventing the evolving strategies of cyber adversaries (Hart et al., 2020). Furthermore, threat intelligence, security event detection technology, network threat technology, endpoint threat technology, and user and attacker behaviour analytics are just a few of the techniques used for threat detection. In the context of rising cyber threats, research is vital for machine learning-based threat detection systems to improve cybersecurity and threat mitigation efforts. As a result, proactive threat detection and response techniques have gained prominence.

Advanced cyber threat detection solutions for CI have been made possible in recent years by the convergence of big data analytics, artificial intelligence (AI), and threat intelligence (Tagarev et al., 2020). These solutions use artificial intelligence (AI) and machine learning to analyze massive amounts of data in real-time, making it possible to identify intricate attack patterns and unusual behaviour. Moreover, by integrating threat intelligence feeds, organizations can proactively recognize and address new threats by using contextual data (Saeed et al., 2023). CI operators face numerous challenges in adequately protecting their systems, even with recent advances in cyber threat detection technologies (Choraś et al., 2016; Li & Liu, 2021). These difficulties include the proliferation of attack vectors, resource limitations, regulatory compliance requirements, and the complexity of interconnected infrastructure networks (Jha, 2023). Given this, there is an increasing need for all-encompassing and flexible cyber defense plans that integrate proactive risk hunting, incident response, and advanced detection capabilities. Therefore, this review will explore the evolution of advanced cyber threat detection techniques for CI, and the current approaches, and suggest possible future directions for research and advancement. The goal of this research review is to provide insights that can inform the design and implementation of beneficial cybersecurity strategies for safeguarding CI assets by examining its effects, and new trends in cyber threat detection.

II. OVERVIEW OF CYBER THREATS IMPACTING CRITICAL INFRASTRUCTURE (CI)

According to Dave et al., (2023), Nation-states, individuals, criminal groups, and even insiders within an organization are just a few of the many potential sources of cyber threats. Firstly, personnel, sometimes referred to as "script kiddies," use free or low-cost internet tools to initiate attacks motivated by curiosity, attention-seeking, or causing trouble (Salas-Fernández et al., 2021). Secondly, financial gain drives criminal organizations, which are a major source of cyber threats. They engage in a variety of criminal activities, such as identity theft, ransomware attacks, and credit card theft (Sudhakar & Kumar, 2020). Thirdly, nation-states are powerful sources of cyber threats because they have sophisticated cyberwarfare capabilities. They carry out a wide range of operations, from obtaining intelligence to possibly undermining or destroying vital infrastructure (Sharma et al., 2019). Lastly, insiders within a company can also be a major cyber threat because they can launch attacks or compromise important assets by abusing their access to sensitive data or systems (Samtani et al., 2020).

Previous research by Algarni et al., (2021) has shown that there remains a challenge with regard to the quantitative assessment of cyber security. The combination of ICTs and physical components has created new risks for the CPS. There are numerous instances nowadays where attackers have exploited weak points in complex systems to compromise them. These attacks have frequently directly affected physical components. As a result, efforts are being made to fully integrate the cyber components of CPS using extensive tools and techniques that frequently make use of a broad range of non-technical and technical methods. Some of the following problems that encompass the current CPS challenges include safety, the ability to scale complexities, and subsystem compatibility (Tyagi & Sreenath, 2021). According to the study by the Centre for Strategic and International Studies (CSIS), a noteworthy list of cyberattacks is provided by the CSIS. A major cyberattack is defined by the CSIS as one that causes damage of at least $1 million. Cyber-attacks on defense, high-tech, and government agencies, as well as attacks on other CIs that result in losses exceeding one million dollars, are classified as significant cyber-attacks. The report also presented an exponential increase, with a projection of 2000 total significant cyberattacks through 2025.

2.1 The Emergence of a Cybercriminal Economy

The global emergence of the cybercriminal economy has made it possible for various kinds of cyberattacks to be offered as services. Though the emphasis in these sections is on cyberattacks, many other forms of criminal activity are made possible by the cybercrime economy. A thorough and consistent survey of the services utilized by the cybercrime industry, arranged according to the value chain perspective, as reported in a review by Huang et al., (2018), to better understand cyberattacks methodically revealed that knowledge about the specialization, monetization, and collaboration involved in organizing a cyberattack is gained.

Users can better comprehend the current cybercrime ecosystem and hacking innovations by utilizing the framework of cyberattacks "as a service" The creation of malicious software, network scanning, denial of service, phishing, target ranking, training and recruiting, and money laundering are a few services that help enable cyberattacks. Subscriptions, licenses, pay-per-records, or commission-based services are the ways in which these services are offered (Huang et al., 2018; Gunduz & Das, 2020). Advance persistent threats (APTs) are CIs' main source of concern. APTs are organizations that target the victim's CI over an extended period with support from their host countries. Data theft from the victim is the main objective of APTs. APTs typically aim to steal data from their target. They do, however, also target the CI's components and control management systems (Gunduz & Das, 2020). The smart grid is a top priority due to the impact of blackouts and the vital role that the power infrastructure plays in ensuring socioeconomic stability (Tufail et al., 2021). Since they are paid for their activities, APTs are a subset of the cybercrime economy and frequently contribute to the economy of the host country. This is because rival countries' economies are being slowed down by the deceit of vital infrastructures. Electricity theft is an emerging factor for the electrical infrastructure and a significant cause of nontechnical losses in the smart grid's distribution systems (Wei et al., 2017).

Money laundering is one of the functions of the cybercrime economy. The use of cryptocurrencies by the victims to transfer money to the attacker is indicative of this activity. When a cryptocurrency transaction such as paying a ransom occurs, the attacker converts the cryptocurrency into a different currency. Therefore, since cryptocurrencies are useful currencies for communication networks that run independently of conventional banks, they are particularly well-suited for this kind of application (Riggs et al., 2023). Information theft may be facilitated by trojan malware. The Ransomware on the Rise in CI Sector (2021) report revealed that if a database on an enterprise system is breached, personally identifiable information may be sold online. There are black markets on the internet, and law enforcement regularly tracks them down. However, because it is simple to move software frameworks between different IT infrastructures, well-known and well-liked digital black markets frequently reappear at a new location. The ransoming of vital computer systems is another illustration of how the cybercriminal economy operates. Hospitals and other vital services are the targets of these ransomware-based attacks (Chokshi, 2019). It is evident why these services are being targeted, the public depends on them, and those who get infected are prepared to spend hefty sums of money to have ransomware removed from their computer systems.

2.1.1 Ransomware Cyberattack

The malevolent function of ransomware is to either encrypt, lock, or exfiltrate data; the ransomware is platform-specific. Because different operating systems have different libraries and functions, the ransomware will use these to carry out malicious actions. They primarily target Windows-powered devices and workstations (Oz et al., 2022). Some organizations function as Ransomware-as-a-

Corporation (RAAC) in the cybercrime economy. However, attackers using the alias RAAC regularly release press releases and communicate using business terminology. The Ransomware on the Rise in Critical Infrastructure Sector (2021) report also stated that the operational systems of the victims will continue to be unavailable if the ransom is not paid, and any sensitive personal data that has been compromised will be exposed on a dark web leak site, harming the company's operations and reputation.

Despite the fact that the cyber-physical system (CPS) is not the target of any current ransomware campaigns, CI and its CPS are more likely targets for ransomware due to CI's installation of more sophisticated electronic devices in the field. Future ransomware attacks that target this new environment will increasingly target smart technologies as they proliferate and become more integrated into buildings, homes, cars, and cities. Consequently, there will be an increase in ransomware targeting industrial CPS intelligent electronic devices (Oz et al., 2022; Hanna et al., 2021; Zhi et al., 2019). The most common way that ransomware is distributed is through emails. Ransomware is typically sent as an attachment in malicious emails. These emails can be addressed and customized to particular people or organizations, or they are frequently distributed as spam to a large number of email addresses. A file or link in the attachment may start the ransomware installation process (Oz et al., 2022). In addition, supply chain ransomware is ransomware distributed via a reputable software method, especially when an IT support provider offers a software updater. The global attack impacted companies including pharmacies, railroads, and retail establishments. Businesses that depended on the IT service company's software updating system were put at risk when the attack took advantage of a flaw in the system (Riggs et al., 2023).

2.1.2 Phishing and Remote Attack

Social engineering techniques are the foundation of phishing and remote attacks, which attempt to deceive the victim into disclosing personal information or downloading malicious software. According to Alkhalil et al., (2021), phishing is a very common tactic used in cyberattacks against corporate networks. In this regard, fraudulent communications are sent by attackers to victims in an attempt to force them to divulge classified credentials or other information. With the right credentials, one can carry out additional attacks like malware installation, remote access, or information theft. Credentials can be ransomed by attackers using the threat of publication (Fruhlinger, 2020).

2.2 Effects of Cyberattacks on Critical Infrastructure

Cyberattacks on CI have serious, multidimensional repercussions that affect national security, society, and the economy. Attacks of this nature have the potential to economically disrupt industries and businesses by causing downtime and operational losses for those whose operations depend on the compromised infrastructure (Avraam et al., 2023; Lis & Mendel, 2019). Therefore, economic burdens can be made more severe by the financial expenses associated with incident response, system recovery, and regulatory fines. In addition, physical harm to infrastructure assets may require expensive replacements and repairs, further taxing available funds. Cyberattacks on CI put society at risk by interfering with necessities like emergency response systems, transportation, and even healthcare (Hüscha & Lahmann, 2022). The social unrest that ensues may have a negative effect on individuals and communities, posing a risk to people's safety and causing inconvenience and distress. Furthermore, cyberattacks on vital infrastructure pose a serious threat to national security since they have the ability to weaken defenses, destabilize governments, and interfere with military actions (Li & Liu, 2021). In essence, adversaries may use strategic cyberwarfare techniques to weaken opponents and influence geopolitical dynamics by taking advantage of weaknesses in CI. Thus, creating strong cybersecurity plans, boosting resilience, and defending national interests require an understanding of the wide-ranging effects of cyberattacks on CI.

2.2.1 Economic Impacts

The study by Lis & Mendel (2019) to examine the economic and financial implications of cyberattacks on CI revealed that modern states, businesses, and individuals depend more and more on digital or cyber technologies to run their operations; this trend is also evident in many aspects of CI. Regulators and service providers need to pay attention to the new cybersecurity area of attacks and threats that CI presents. If CI systems are deployed without adequate cybersecurity, they may be susceptible to malicious attacks or intrinsic failures, which could have catastrophic consequences.

Lis & Mendel (2019) argued that governments and providers of CI should make sure that a comprehensive cost-benefit analysis of cybersecurity initiatives, accounting for both internal and external costs, is a crucial component of their decisions. However, the paper also revealed a dearth of representative data on cyberattacks, which could be used to obtain data on damages and their likelihood. Furthermore, the lack of data makes it impossible for analysts to determine the scope of external expenses and advantages related to cyberattacks and cybersecurity, therefore making the development of efficient internalizing externality mechanisms challenging.

According to Hassan et al., (2012), some consequences of cybercrime include a decline in an organization's ability to thrive over, time wastage, sluggish financial growth, a delay in production, an increase in overhead costs, and damage to the reputation of a country. Loss of privacy and monetary losses are two other significant effects. A few consequences of cybercrime are outlined in brief:

Loss of Competitive Edge: When a hacker obtains a company's private data and plans and sells it to a rival, the company may lose its competitive edge and incur losses. The time that IT staff wasted on fixing malicious events brought on by cybercriminals could have been used to generate revenue for the company (Riedy & Hanus, 2016).

Productivity Losses and Increasing Costs: Although businesses take precautions to prevent cybercrime by securing their networks, cybercrime also lowers productivity within an organization. This takes a lot of time and reduces output. Moreover, companies purchase security software to manage malware and viruses and lower the likelihood of attacks. Thus, computer crime lowers profit margins and raises overhead costs. The use of computer and network resources as well as the expense of human time and attention in removing undesired messages are additional effects (Ibrahim, 2020).

Monetary Losses: Financial fraud, intellectual property theft, reputational harm, decreased productivity, and third-party liability are just a few of the monetary losses that cyberattacks cause to economies and businesses. A portion of the reported cost of viruses and cyberattacks is made up of opportunity cost, which includes lost sales and decreased productivity. Opportunity costs, however, do not always result in expenses for the overall economy. Financial fraud and online theft of intellectual property pose a greater threat to businesses. There will therefore undoubtedly be severe financial repercussions in areas where cybercrime is prevalent, particularly concerning businesses and financial institutions. According to a Ponemon Institute research study report from 2016, using a sample of 237 businesses from six countries, the cost of cybercrime in six countries: the United States, Japan, Germany, the United Kingdom, Brazil, and Australia ranged from USD$4.3 million to USD$17.3 million in 2016.

Ibrahim (2020) also reported that cybercrime is undoubtedly negatively impacting Nigeria's reputation, which continues to be a major cause of humiliation for the nation. The use of ICT has been avoided by some due to fear of cybercrime. The welfare of the populace and investors is negatively impacted and the actions of cybercriminals can undermine trust in a country's financial system. Both tourists and potential investors are terrified, and the public's perception of the country is damaged. Residents face reputational risk: in the current global economy, a country cannot afford to have its financial system or its reputation damaged by being linked to cybercrime. Engaging in meaningful social interaction with the rest of the world might become difficult for a citizen when every citizen is thought to be a potential cyber-criminal.

2.2.2 Societal Impacts and National Security Implication

Cyberattacks on CI can potentially have serious, far-reaching effects on many facets of society (Choraś et al., 2016). These attacks translate into a serious risk to public safety and well-being by resulting in fatalities. Attacks on transportation or power grids, for example, may have direct or indirect effects that put lives in danger (Krause et al., 2021). In addition, cyberattack-related disruption may culminate in social unrest, causing essential services to break down (Bada & Nurse, 2019). Therefore, when essential infrastructure malfunctions, the populace may become irate out of fear, uncertainty, or frustration.

In terms of national security risks, cyberattacks on CI present serious risks to national security, affecting a nation's capacity to fend off external threats and uphold stability (Maurer & Nelson, 2021). These assaults can therefore have the potential to compromise private data, interfere with defense mechanisms, and erode a country's security posture. These societal repercussions highlight how crucial it is to have effective cybersecurity defenses and proactive tactics in place to preserve CI and shield the general public from the devastating effects of cyberattacks.

III. EVOLUTION OF CYBER THREAT AND DETECTION TECHNIQUES

Cybersecurity threats have been an issue since the inception of computer networks. The quantity and complexity of these threats skyrocketed as technology developed and the Internet spread (Conti et al., 2018). An outline of the development of cybersecurity threats is provided below:

In the early years (1970 – 1990s), with the introduction of early computer networks in the 1970s, the first cybersecurity threats appeared. Hackers started taking advantage of the vulnerabilities and limitations in software and operating systems, usually just for unauthorized access. The majority of these early threats were isolated occurrences, and inadequate safety was established (Housen-Couriel, 2015).

Computer viruses and malware (1990 – 2000): These issues first surfaced in the 1990s and were frequently disseminated via email attachments or contaminated floppy discs. Released in 1991, the notorious Michelangelo virus infected thousands of computers all over the world. Worms and trojans were also used by cybercriminals to obtain unauthorized access and steal data (Corallo et al., 2022).

Increasingly Potent Cyber and Web-Related Risks (2000s–2010s): New kinds of threats have surfaced as a result of the expansion of the Internet and the widespread use of web-based technologies. Phishing attacks have become commonplace, wherein attackers use false emails to trick users into disclosing sensitive information Alkhalil et al., (2021). A serious threat also emerged from distributed denial of service (DDoS) attacks, in which numerous computers flood a target website or server with traffic, causing an overload and temporary shutdown (Edwards, 2019).

Advanced Persistent Threats (2010 – present): APTs have grown to be a significant worry in recent years. APTs are highly skilled, precisely targeted attacks that are frequently funded by nation-states and intended to compromise particular people, companies, or sectors of the economy (Nasir et al., 2019). Social engineering, malware, and network exploitation techniques are all used in these attacks. Because APTs are stealthy, they can be challenging to identify and mitigate (Hussain et al., 2020)

Ransomware and Extortion: In recent times, there has been a notable surge in ransomware attacks. Malware known as ransomware encrypts a victim's data and prevents it from being accessed until the attacker receives a ransom (Li & Li, 2018).

Threats to the Internet of Things (IoT): As more technological equipment is linked to the Internet, worries regarding the security of the IoT are becoming more and more prevalent. Wearable devices, home automation systems, and smart appliances are just a few examples of IoT systems that are susceptible to cyberattacks (Raimundo & Rosário, 2022). These attacks can take many different forms, such as obtaining illegal access, compromising personal information, or even taking over actual devices, and because of their widespread deployment and inherent security flaws, IoT devices are a popular target for cybercriminals (Schmittner & Macher, 2019)

Cloud-Based Threats: As cloud computing has become more widely used, new cybersecurity risks have surfaced. Cloud-based attacks may involve the theft of private information from cloud-based apps, the compromise of cloud storage accounts, or the exploitation of security holes in cloud infrastructure (Sam et al., 2022). Making sure cloud-based systems and data are secure has become essential as more businesses shift their data and operations to the cloud (Shafqat & Masood 2016).

The necessity to adjust to new threats and technological developments has fueled the advancement of cyber threat detection techniques for CI. Cyber threat detection has developed over time, becoming more sophisticated, adaptive, and proactive. Early signature-based approaches gave way to more sophisticated anomaly detection and behavior-based analysis techniques.

The necessity to adjust to new threats and technological developments has fueled the advancement of cyber threat detection techniques for CI. Cyber threat detection has developed over time, becoming more sophisticated, adaptive, and proactive. Early signature-based approaches enabled more sophisticated anomaly detection and behavior-based analysis techniques (Jeffrey et al., 2023). In general, Artificial Intelligence (AI) has revolutionized cybersecurity as organizations now protect themselves against cyber threats in an entirely novel approach, due to their capacity to analyze enormous amounts of data, identify patterns, and make informed choices in real-time. The efficacy and efficiency of cyber threat detection have been greatly improved by developments in AI, machine learning, and big data analytics, allowing establishments to better safeguard their CI assets against a constantly changing array of threats (Merve Ozkan-Ozay et al., 2024). Substantial ways AI is improving cybersecurity for CI systems are stated:

Advanced Threat Detection: AI-driven cybersecurity systems can potentially recognize and evaluate a variety of cyber threats, such as DDoS assaults, malware, and phishing scams (Sarker et al., 2021). AI systems are capable of swiftly identifying and addressing possible threats because they are continuously monitoring network traffic and examining anomalies.

Automated Incident Response: AI can start an automated incident response when a cyber threat is identified, greatly cutting down on response time (Chahal, 2023). This minimizes possible damages by accelerating the attack's containment and mitigation.

Behavioural Analysis: AI systems can examine user behaviour and spot any irregularities or questionable activity (Pawar et al., 2023). This makes it possible for enterprises to identify malicious activity and insider threats that would go undetected by more conventional security measures.

Threat Intelligence: To keep abreast of the most recent patterns and strategies used by cybercriminals, AI can compile and evaluate threat intelligence from a variety of sources, including security feeds and forums (Saeed et al., 2023), to proactively defend their engineering systems from new threats.

Predictive analytics: AI can anticipate future cyber threats and vulnerabilities by utilizing machine learning algorithms and historical data (Bharadiya, 2023). This makes it possible for businesses to effectively allocate resources and prioritize security efforts.

IV. CURRENT STATE OF CYBER THREAT DETECTION TECHNIQUES IN CRITICAL INFRASTRUCTURE

Owing to the fact that the foundation of critical national infrastructures like power grids, transportation networks, home automation systems, and so on is made up of CPS, the field of CPS has changed significantly over the past few decades in response to advancements in microprocessor technology and the accessibility of fast wired and wireless networks.

IT and legacy Operational Technology (OT) environments, each with different priorities, are combined to form CPS. Whereas OT networks prioritize availability, integrity, and confidentiality, traditional IT networks place more emphasis on confidentiality. There have been constant challenges as OT and IT networks combine to form modern CPS because of their different priorities. Whereas OT networks have historically placed more emphasis on availability, IT networks place a great deal of emphasis on authentication and authorization. However, because the OT and IT networks are interconnected, CPS is susceptible to network-based attacks like replay attacks, DDoS, Man-in-the-Middle (MitM), spoofing, impersonation, and false data injection. Although there are efforts to expand the Intrusion Detection System/Intrusion Prevention System (IDS/IPS) capabilities of IT networks into OT networks, threat detection is severely hampered by the lack of standardized protocols and interfaces for the physical components (Rakas et al., 2020).

Secure CPS design and operation are hampered by the proprietary nature of these systems and the absence of established communication protocols. An industry consortium called O-PAS (Open Process Automation Standard) is working to create a set of open, collaborative standards on communication protocols and security postures, intending to standardize the diverse array of proprietary CPS (Bartusiak et al., 2020). Considerable advantages can be obtained from an accelerated product development lifecycle and continuous efficiencies over the course of the CPS lifecycle by designing a CPS to support open standards. Although IDS/IPS is widely used in IT networks for anomaly detection, it still has a problem with too many false positives in OT networks. Mahbooba et al., (2021) suggested a technique for utilizing Explainable Artificial Intelligence (XAI) to increase the precision of anomaly detection in IDS by involving the CPS's human operator in the process, delivering a comprehensible justification for the IDS alert, enabling the human operator to approve or disapprove the anomaly detection. The decisions made by the human operators of the CPS are incorporated back into the learning model, which eventually improves accuracy and boosts their confidence. A synopsis of each category is included in Table 1.

Table 1. Threat Detection Techniques

Category	Overview	Author
Comparison of Anomaly Detection (AD) Strategies	There are three types of AD strategies: threshold-based, behavior-based, and signature-based.	Wu et al., 2017; Altunay et al., 2021; Rubio et al., 2019
Anomaly Detection with IDS/IPS Integration	IDS/IPS are well-established tactics in IT networks, but because false positives are far more expensive in OT networks, they are still not very effective.	Huang & Zhu, 2020; Sheng et al., 2021; Zohrevand & Glasser, 2020
Artificial Intelligence and Machine Learning (AI/ML) Applications for Anomaly Detection	The main application of AI/ML strategies is behavior-based AD, where learning algorithms are used to transform big data issues into useful information.	Bogdan & Pedram, 2018; Ha et al., 2022; Zhu et al., 2022
Enhancing Anomaly Identification Using Testbeds and Simulators	Small-scale testbeds or simulations are an appealing substitute for large-scale CPS environments because it is not financially feasible to replicate their physical components for development and testing purposes.	Craggs et al., 2019; Gardiner et al., 2019
Detecting anomalies at the network's edge	In order to prevent network saturation, early data filtering and pre-processing at the network edge become essential as IoT/IIoT sensor networks multiply.	Eskandari et al., 2020; Tsukada et al., 2020
Zero-Trust Architecture (ZTA) and Trusted Systems	Industrial networks were historically intended to be completely trusted and isolated, but as public networks become more connected, ZTA adoption becomes more crucial.	Xiao et al., 2022; Alshomrani & Li, 2022

The techniques have advantages and disadvantages, so companies frequently use a mix of strategies to improve their capacity for threat detection and lessen the risks associated with cyberattacks (Safitra et al., 2023). Through the utilization of evidence-based research and a comprehensive understanding of the benefits and drawbacks of detection techniques, enterprises can formulate more potent and efficient cyber defense plans to safeguard critical infrastructure assets.

Declarations
Availability of data and materials
Not applicable
Funding
Not Applicable
Acknowledgements
Not applicable

CONCLUSIONS AND FUTURE DIRECTIONS

The swift advancement and complexity of cyber threats present a serious obstacle. Therefore, as a result of various confounding factors, the automated detection of anomalies and/or threats to CPS is still a field in rapid development. However, the effectiveness of cyber threat detection techniques in safeguarding critical infrastructure is impeded by several challenges and limitations, as demonstrated by recent research. Due to diversity, there appears to be a lack of a universally applicable anomaly detection model. A generic or universal framework for anomaly detection in CPS has been proposed by numerous researchers; however, to facilitate the rapid development of test cases, detection methods must necessarily reduce real-world fidelity, thereby becoming less representative of the actual CPS. Conversely, an increase in anomaly detection accuracy for a real-world CPS also results in a decrease in its generalizability to other CPS environments. A low-level generic framework with a modular architecture that enables the development of plugins for the special features of a given CPS may be beneficial.

The inability of existing detection techniques like signature-based and anomaly detection, to keep up with these dynamic threats, frequently produces more false positives and false negatives. Furthermore, traditional detection techniques face difficulties due to the increasing complexity and interconnectedness of critical infrastructure systems, as they might not be scalable or adaptive enough to monitor and defend against threats in a variety of distributed and heterogeneous environments. In addition, the introduction of new technologies and paradigms, like AI, cloud computing, and IoT, adds vulnerabilities and complexity to the process of detecting cyber threats. Although these technologies are very innovative and efficient, they also create new attack vectors and difficulties for defenses.

Future research and development efforts should concentrate on a few critical areas for innovation and improvement in order to address these issues and advance cyber threat detection. The development of information sharing and threat intelligence methods to improve situational awareness and facilitate proactive threat detection and response is one encouraging path. Organizations can gain a better understanding of evolving threats and take proactive measures to defend against new threats before they materialize into large-scale attacks by utilizing real-time threat intelligence feeds. More robust and adaptive detection techniques that can independently identify and mitigate threats in dynamic and heterogeneous environments are also becoming necessary. This includes investigating decentralized detection architectures, self-learning algorithms, and adaptive defense mechanisms that can change and adapt over time in response to new attack vectors and threats. Ultimately, the development of more reliable and scalable detection methods that function in the context of emerging technologies should be prioritized in future research.

REFERENCES

[1] Algarni, A. M., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems. *Applied Sciences*, *11*(8), 3678. https://doi.org/10.3390/app11083678

[2] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*(1). https://doi.org/10.3389/fcomp.2021.563060

[3] Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., & Salonitis, K. (2023). Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations. *Sensors*, *23*(9), 4539. https://doi.org/10.3390/s23094539

[4] Alshomrani, S., & Li, S. (2022). PUFDCA: A Zero-Trust-Based IoT Device Continuous Authentication Protocol. *Wireless Communications and Mobile Computing*, *2022*, 1–9. https://doi.org/10.1155/2022/6367579

[5] Altunay H. C., Zafer Albayrak, Ahmet Nusret Ozalp, & Muhammet Çakmak. (2021). Analysis of Anomaly Detection Approaches Performed Through Deep Learning Methods in SCADA Systems. *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. https://doi.org/10.1109/hora52670.2021.9461273

[6] Avraam C, Ceferino, L., & Dvorkin, Y. (2023). Operational and economy-wide impacts of compound cyber-attacks and extreme weather events on electric power networks. *Applied Energy*, *349*, 121577–121577. https://doi.org/10.1016/j.apenergy.2023.121577

[7] Bada, M., & Nurse, J. (2019). *The Social and Psychological Impact of Cyber-Attacks*. https://arxiv.org/ftp/arxiv/papers/1909/1909.13256.pdf

[8] Bartusiak, R. D., Bitar, S., Debari, D., Houk, B., Heaton, M., Strebel, R., Stevens, D., Fitzpatrick, B., & Sloan, P. (2020). *Open Process Automation: A standards-based, open, secure, interoperable process control architecture*. https://ifatwww.et.uni-magdeburg.de/ifac2020/media/pdfs/3672.pdf

[9] Berger, C., Eichhammer, P., Reiser, H. P., Domaschka, J., Hauck, F. J., & Habiger, G. (2022). A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms. *ACM Computing Surveys*, *54*(147), 1–39. https://doi.org/10.1145/3462513

[10] Bharadiya P. B. (2023). AI-Driven Security: How Machine Learning Will Shape the Future of Cybersecurity and Web 3. *American Journal of Neural Networks and Applications*, *9*(1). https://doi.org/10.11648/j.ajnna.20230901.11

[11] Bogdan, P., & Massoud Pedram. (2018). Toward Enabling Automated Cognition and Decision-Making in Complex Cyber-Physical Systems. *S. In Proceedings of the 2018 IEEE International Symposium on Circuits and Systems (ISCAS), Florence, Italy*. https://doi.org/10.1109/iscas.2018.8351868

[12] Chahal, S. (2023). AI-Enhanced Cyber Incident Response and Recovery. *International Journal of Science and Research*, *12*(3), 1795–1801. https://doi.org/10.21275/sr231003163025

[13] Chehri, A., Fofana, I., & Yang, X. (2021). Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. *Sustainability*, *13*(6), 3196. https://doi.org/10.3390/su13063196

[14] Chokshi, N. (2019, May 22). Hackers Are Holding Baltimore Hostage: How They Struck and What's Next. *The New York Times*. https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

[15] Choraś, M., Kozik, R., Flizikowski, A., Hołubowicz, W., & Renk, R. (2016). Cyber Threats Impacting Critical Infrastructures. *Managing the Complexity of Critical Infrastructures*, 139–161. https://doi.org/10.1007/978-3-319-51043-9_7

[16] Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber threat intelligence: challenges and op-portunities. *Cornell Computer Science > Cryptography and Security*, 1–16.

[17] Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*, 103614. https://doi.org/10.1016/j.compind.2022.103614

[18] Craggs, B., Rashid, A., Hankin, C., Antrobus, R., Serban, O., & Thapen, N. (2019). A Reference Architecture for IIoT and Industrial Control Systems Testbeds. *Living in the Internet of Things (IoT 2019)*. https://doi.org/10.1049/cp.2019.0169

[19] Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). The New Frontier of

Cybersecurity: Emerging Threats and Innovations. *ArXiv (Cornell University)*. https://doi.org/10.1109/ict60153.2023.10374044

[20] De Felice, F., Baffo, I., & Petrillo, A. (2022). Critical Infrastructures Overview: Past, Present and Future. *Sustainability*, *14*(4), 2233. https://doi.org/10.3390/su14042233

[21] Edwards, G. (2019). *Cybercrime investigators handbook*. John Wiley & Sons, Inc.

[22] Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An Intelligent Anomaly Based Intrusion Detection System for IoT Edge Devices. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/jiot.2020.2970501

[23] Fruhlinger, J. (2020, February 12). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* CSO Online. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

[24] Gardiner, J., Craggs, B., Green, B., & Rashid, A. (2019). Oops I Did it Again: Further Adventures in the Land of ICS Security Testbeds. In ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC'19). *Bristol Research (University of Bristol)*. https://doi.org/10.1145/3338499.3357355

[25] *Gartner Predicts 30% of Critical Infrastructure Organizations Will Experience a Security Breach by 2025*. (2021). Gartner. https://www.gartner.com/en/newsroom/press-releases/2021-12-2-gartner-predicts-30--of-critical-infrastructure-organi

[26] Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*(107094), 107094. https://doi.org/10.1016/j.comnet.2019.107094

[27] HÜSCHA, P., & LAHMANN, H. (2022). *Home - The Geneva Academy of International Humanitarian Law and Human Rights*. Www.geneva-Academy.ch. https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Societal%20Risks%20and%20Potential.pdf

[28] Ha, D. T., Hoang, N. X., Hoang, N. V., Du, N. H., Huong, T. T., & Tran, K. P. (2022). Explainable Anomaly Detection for Industrial Control System Cybersecurity. *IFAC-PapersOnLine*, *55*(10), 1183–1188. https://doi.org/10.1016/j.ifacol.2022.09.550

[29] Hanna, Y., Mumin Cebe, Suat Mercan, & Akkaya, K. (2021). Efficient Group-Key Management for Low-bandwidth Smart Grid Networks. *Conference: 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) Authors:* https://doi.org/10.1109/smartgridcomm51999.2021.9631988

[30] Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, *95*, 101827. https://doi.org/10.1016/j.cose.2020.101827

[31] Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cyber crime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology*, *2*(7), 626, 631.

[32] Housen-Couriel, D. (2015). Cybersecurity and anti-satellite capabilities (asat) new threats and new legal responses. *Journal of Law & Cyber Warfare*, *4*(3), 116–149.

[33] Huang, K., Siegel, M., & Madnick, S. (2018). Systematically Understanding the Cyber Attack Business. *ACM Computing Surveys*, *51*(4), 1–36. https://doi.org/10.1145/3199674

[34] Huang, L., & Zhu, Q. (2020). A dynamic games approach to proactive defense strategies against Advanced Persistent Threats in cyber-physical systems. *Computers & Security*, *89*, 101660. https://doi.org/10.1016/j.cose.2019.101660

[35] Hussain, A., Mohamed, A., & Razali, S. (2020). A review on cybersecurity: Challenges & emerging threats. *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*.

[36] Ibrahim, U. (2020). *THE IMPACT OF CYBERCRIME ON THE NIGERIAN ECONOMY AND BANKING SYSTEM*. https://ndic.gov.ng/wp-content/uploads/2020/08/NDIC-Quarterly-Vol-

34-No-12-2019-Article-The-Impact-Of-Cybercrime-On-The-Nigerian-Economy-And-Banking-System.pdf

[37] Jeffrey, N., Tan, Q., & Villar, R. (2023). A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems. *Electronics*, *12*(15), 3283–3283. https://doi.org/10.3390/electronics12153283

[38] Jha, R. K. (2023). Cyber-Physical Security Framework for Critical Infrastructure Protection in Power Systems. *Cyber-Physical Security Framework for Critical Infrastructure Protection in Power Systems*. https://doi.org/10.21203/rs.3.rs-3127087/v1

[39] Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors*, *21*(18), 6225. https://doi.org/10.3390/s21186225

[40] Latino, M. E., & Menegoli, M. (2022). Cybersecurity in the food and beverage industry: A reference framework. *Computers in Industry*, *141*, 103702. https://doi.org/10.1016/j.compind.2022.103702

[41] Li, X., & Li, H. (2018). A Visual Analysis of Research on Information Security Risk by Using CiteSpace. *IEEE Access*, *6*, 63243–63257. https://doi.org/10.1109/access.2018.2873696

[42] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports*, *7*(7), 8176–8186. Sciencedirect. https://doi.org/10.1016/j.egyr.2021.08.126

[43] Lis, P., & Mendel, J. (2019). Cyberattacks on Critical Infrastructure: an Economic Perspective. *Economics and Business Review*, *5*(19), 24–47. https://doi.org/10.18559/ebr.2019.2.2

[44] Mahbooba, B., Timilsina, M., Sahal, R., & Serrano, M. (2021). Explainable Artificial Intelligence (XAI) to Enhance Trust Management in Intrusion Detection Systems Using Decision Tree Model. *Complexity*, *2021*, 1–11. https://doi.org/10.1155/2021/6634811

[45] Maurer, T., & Nelson, A. (2021). *The Global Cyber Threat to Financial Systems – IMF F&D*. International Monetary Fund. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

[46] Merve Ozkan-Ozay, Akin, E., Aslan, Ö., Selahattin Kosunalp, Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access*, *12*, 12229–12256. https://doi.org/10.1109/access.2024.3355547

[47] Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, *44*, 12–22. https://doi.org/10.1016/j.jisa.2018.11.003

[48] Obarafor, V. (2019). Cyber crime in Nigeria, Causes, Effects, and solutions.pdf. *Figshare.com*. https://doi.org/10.6084/m9.figshare.9822392.v2

[49] Oueslati, N. E., Mrabet, H., Jemai, A., & Alhomoud, A. (2019). Comparative Study of the Common Cyber-physical Attacks in Industry 4.0. *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*. https://doi.org/10.1109/iintec48298.2019.9112097

[50] Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *ACM Computing Surveys*, *54*(11s). https://doi.org/10.1145/3514229

[51] Pawar, S., Borse, A., Pandit, G., Pokharkar, V., & Kamble, N. V. (2023). Detection of Suspicious Activity Using Artificial Intelligence. *International Journal of Research Publication and Reviews*, *4*(6), 220–225.

[52] Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the Internet of Things in Industrial Management. *Applied Sciences*, *12*(3), 1598. https://doi.org/10.3390/app12031598

[53] Rakas, S. V. B., Stojanovic, M. D., & Markovic-Petrovic, J. D. (2020). A Review of Research Work on Network-Based SCADA Intrusion Detection Systems. *IEEE Access*, *8*, 93083–

93108. https://doi.org/10.1109/access.2020.2994961

[54] *Ransomware on the Rise in Critical Infrastructure Sector*. (2021). JD Supra. https://www.jdsupra.com/legalnews/ransomware-on-the-rise-in-critical-1687319/

[55] Riedy, M., & Hanus, B. (2016). *Yes, Your Personal Data Is at Risk: Get over It Yes, Your Personal Data Is at Risk: Get over It Yes, Your Personal Data Is at Risk: Get Over It!* https://scholar.smu.edu/cgi/viewcontent.cgi?article=1030&context=scitech

[56] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors*, *23*(8), 4060. https://www.mdpi.com/1424-8220/23/8/4060

[57] Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers & Security*, *87*, 101561. https://doi.org/10.1016/j.cose.2019.06.015

[58] Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.3390/s23167273

[59] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, *15*(18), 13369. https://doi.org/10.3390/su151813369

[60] Salas-Fernández, A., Crawford, B., Soto, R., & Misra, S. (2021). Metaheuristic Techniques in Attack and Defense Strategies for Cybersecurity: A Systematic Review. *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities*, 449–467. https://doi.org/10.1007/978-3-030-72236-4_18

[61] Sam, M. F. M., Ismail, A. F. M. F., Bakar, K. A., Ahamat, A., & Qureshi, M. I. (2022). The Effectiveness of IoT Based Wearable Devices and Potential Cybersecurity Risks: A Systematic Literature Review from the Last Decade. *International Journal of Online and Biomedical Engineering*, *18*(9), 56–73.

[62] Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 135–154. https://doi.org/10.1007/978-3-319-78440-3_8

[63] Sarker, I. H. (2021). CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks. *Internet of Things*, *14*, 100393. https://doi.org/10.1016/j.iot.2021.100393

[64] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, *2*(3). https://doi.org/10.1007/s42979-021-00557-0

[65] Schmittner, C., & Macher, G. (2019). Automotive cybersecurity standards-relation and overview. *In Computer Safety, Reliability, and Security: SAFECOMP 2019 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, 38*, 153–165.

[66] Shafqat Narmeen, & Masood Ashraf Ali. (2016). Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security, 14*(1). https://doi.org/10.6084/m9.figshare.2069599.v1

[67] Sharma, B. K., Joseph, M. A., Jacob, B., & Miranda, B. (2019). Emerging trends in Digital Forensic and Cyber security- An Overview. *2019 Sixth HCT Information Technology Trends (ITT)*. https://doi.org/10.1109/itt48889.2019.9075101

[68] Sheng, C., Yao, Y., Fu, Q., & Yang, W. (2021). A cyber-physical model for SCADA system and its intrusion detection. *Computer Networks*, *185*, 107677. https://doi.org/10.1016/j.comnet.2020.107677

[69] *Significant Cyber Incidents. Center for Strategic and International Studies* |. (2019). Csis.org. https://www.csis.org/

[70] Sudhakar, & Kumar, S. (2020). An emerging threat Fileless malware: a survey and research

challenges. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-019-0043-x

[71] Tagarev, T., Sharkov, G., & Lazarov, A. (2020). Cyber Protection of Critical Infrastructures, Novel Big Data and Artificial Intelligence Solutions. *Information & Security: An International Journal*, *47*(1), 7–10. https://doi.org/10.11610/isij.4700

[72] Tehrani, K. (2020). A smart cyber physical multi-source energy system for an electric vehicle prototype. *Journal of Systems Architecture*, *111*, 101804. https://doi.org/10.1016/j.sysarc.2020.101804

[73] Tsukada, M., Kondo, M., & Matsutani, H. (2020). A Neural Network-Based On-Device Learning Anomaly Detector for Edge Devices. *IEEE Transactions on Computers*, *69*(7), 1027–1044. https://doi.org/10.1109/TC.2020.2973631

[74] Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies*, *14*(18), 5894. https://doi.org/10.3390/en14185894

[75] Tyagi, A. K., & Sreenath, N. (2021). Cyber physical systems: Analyses, challenges and possible solutions. *Internet of Things and Cyber-Physical Systems*, *1*. https://doi.org/10.1016/j.iotcps.2021.12.002

[76] Wei, L., Sundararajan, A., Sarwat, A. I., Biswas, S., & Ibrahim, E. (2017). A distributed intelligent framework for electricity theft detection using benford’s law and stackelberg game. *2017 Resilience Week (RWS)*. https://doi.org/10.1109/rweek.2017.8088640

[77] Wu, M., Song, Z., & Moon, Y. B. (2017). Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *Journal of Intelligent Manufacturing*, *30*(3), 1111–1123. https://doi.org/10.1007/s10845-017-1315-5

[78] Xiao, S., Ye, Y., Kanwal, N., Newe, T., & Lee, B. (2022). SoK: Context and Risk Aware Access Control for Zero Trust Systems. *Security and Communication Networks*, *2022*, 1–20. https://doi.org/10.1155/2022/7026779

[79] Zhang, J., Pan, L., Han, Q.-L., Chen, C., Wen, S., & Xiang, Y. (2021). Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey. *IEEE/CAA Journal of Automatica Sinica*, 1–15. https://doi.org/10.1109/jas.2021.1004261

[80] Zhi, Y., Fu, Z., Sun, X., & Yu, J. (2019). Security and Privacy Issues of UAV: A Survey. *Mobile Networks and Applications*. https://doi.org/10.1007/s11036-018-1193-x

[81] Zhu, N., Zhu, C., Zhou, L., Zhu, Y., & Zhang, X. (2022). Optimization of the Random Forest Hyperparameters for Power Industrial Control Systems Intrusion Detection Using an Improved Grid Search Algorithm. *Applied Sciences*, *12*(20), 10456. https://doi.org/10.3390/app122010456

[82] Zohrevand, Z., & Glasser, U. (2020). Dynamic Attack Scoring Using Distributed Local Detectors. *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. https://doi.org/10.1109/icassp40776.2020.9054264