Journal of Information Security and Applications 83 (2024) 103786

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Current approaches and future directions for Cyber Threat Intelligence sharing: A survey

Poopak Alaeifar [a], Shantanu Pal [b,*], Zahra Jadidi [a], Mukhtar Hussain [c], Ernest Foo [a]

[a] School of Information and Communication Technology, Griffith University, Gold Coast Campus, QLD 4222, Australia
[b] School of Information Technology, Deakin University, Melbourne, VIC 3125, Australia
[c] School of Information and Communication Technology, Griffith University, Nathan Campus, QLD 4222, Australia

ARTICLE INFO

Keywords:
Cyber threat intelligence
Information sharing
Machine learning
Security
Blockchain
Artificial intelligence

ABSTRACT

Cyber Threat Intelligence (CTI) is essential knowledge concerning cyber and physical threats aimed at mitigating potential cyber attacks. The rapid evolution of Information and Communications Technology (ICT), the Internet of Things (IoT), and Industry 5.0 has spawned a multitude of sources regarding current or potential cyber threats against organizations. Consequently, CTI sharing among organizations holds considerable promise for facilitating swift responses to attacks and enabling mutual benefits through active participation. However, exchanging CTI among different organizations poses significant challenges, including legal and regulatory obligations, interoperability standards, and data reliability. The current CTI sharing landscape remains inadequately explored, hindering a comprehensive examination of organizations' critical needs and the challenges they encounter during CTI sharing. This paper presents a comprehensive survey on CTI sharing, beginning with an exploration of CTI fundamentals and its advancements in assessing cyber and physical threats and threat actors from various perspectives. For instance, we discuss the benefits of CTI, its applications, and diverse CTI sharing architectures. Additionally, we extensively discuss a list of CTI sharing challenges and evaluate how available CTI sharing proposals address these challenges. Finally, we provide an inventory of unique future research directions to offer insightful guidelines for CTI sharing.

1. Introduction

In recent years, there has been a considerable growth in the number of reported cyber attacks, e.g., ransomware, phishing, and social engineering that create a significant attention for both private and public sectors [1]. For example, in 2022, 68% of the reported cyber attacks worldwide were ransomware [2]. Adversaries exploit ever-changing sophisticated attack methods to overcome the cyber attack defenders [3]. Attackers use knowledge sharing techniques in their network and communities to establish technical and operational advantages [4]. They also gain benefits from security vulnerabilities and weaknesses in government agencies, corporate, and individual systems to infiltrate them [5]. These attacks have severe consequences affecting private, public sectors and national security. At the same time, it has been apparent that the traditional cyber defense models and tools, e.g., antivirus, firewalls, signature-based Intrusion Detection Systems (IDS), etc., in isolation, are not capable of keeping pace with the ongoing trend of cyber attacks [6–8]. For this reason, an extensive number of protection strategies have been proposed to survive the rise of cybercrime. Among these solutions, proactive cybersecurity methods, e.g., Cyber Threat Intelligence (CTI) sharing seems to be more promising [9–11] and more recommended by cybersecurity experts. CTI is referred to the relevant, timely and actionable information about the latest threats and attacks that is the outcome of the timely process of collecting cyber threat information from various sources, e.g., open source, internal and external sources, and analyzing and processing the collected information [12,13].

The process of sharing CTI necessitates the utilization of tools, techniques, and an appropriate platform for the collection, analysis, and processing of threat information to generate various forms of CTI. It also requires resources to share the generated CTI with both internal and external stakeholders. The platform in question should be both collaborative and secure, enabling the seamless and timely exchange of anonymous CTI between sources and consumers. Moreover, the platform should be able to preserve the anonymity, traceability, and privacy of data, to protect trust relationship among participants (sources and destinations). At the same time, the platform needs to be capable enough for addressing various challenges, e.g., performance,

* Corresponding author.
E-mail address: shantanu.pal@deakin.edu.au (S. Pal).

https://doi.org/10.1016/j.jisa.2024.103786

Available online 17 May 2024

scalability, interoperability issues, and integrity with different standards, and languages [14]. In this paper, the CTI sharing platform refers to the tool for collecting, analyzing, generating CTI and sharing heterogeneous CTI to the consumers in an automated manner to establish proper and effective defensive capabilities. CTI sharing on a global scale involves various privacy and legal requirements related to sharing sensitive information. Because of that, CTI sharing platforms should be able to operate with such governance compliance requirements [15].

Therefore, CTI sharing has been the subject of academic and business projects to enhance the community's collective knowledge, experience, and capability to understand the threats completely. There are several commercial platforms and vendors available for CTI sharing including, Splunk, CrowdStrike, and IBM X- Force [16]. However, they have several issues, e.g., heterogeneity, interoperability, network bandwidth, security, etc, for a seamless CTI sharing among the organizations. These issues have recently gained significant attention from researchers to propose various CTI sharing solutions to improve existing commercial CTI sharing platforms.

1.1. Significance of CTI sharing

CTI sharing enables organizations to benefit in many ways. Among others, we list a few of them as follows:

- *Shared Situational Awareness:* Sharing the intelligence of threats and vulnerabilities allows organizations to develop situational awareness. Through CTI sharing, organizations can leverage the knowledge, experience, and analytical capabilities collected from their sharing entities to better assess security vulnerabilities and enhance their defense capabilities [15,17,18]. Moreover, participating in sharing CTI helps other organizations to improve their security safeguard. Contributing a new piece of accurate and validated information about threat actors or indicators of compromise (IoCs) can increase the awareness of the entire community. In fact, by CTI sharing, threat detection process that an attacked-organization approached becomes the prevention process for another organizations [19,20].
- *Improved Security Posture:* CTI sharing can help organizations to understand their cyber threat environment better, e.g., knowing their asset vulnerabilities, the effectiveness of their security controls, and the level of automation in their security programs. Thus, organizations can use the gained knowledge and implement protective measures, increase the capabilities of threat detection, effectively respond to security incidents and faster response and recover from the incidents [17]. Organizations that share threat information and mitigate threats not only improve their overall security posture but also provide security protection information to other organizations and, as a result, reduce the number of potential attack vectors for threat actors [15].
- *Knowledge Maturation:* The value of threat information develops during the CTI sharing process. This is done through observing threats, analyzing and processing of collected data by different organizations. Thus, the threat information achieves a level maturity by being more contextual and scalable and more effectively enhance the cyber defense [19].
- *Greater Defensive Agility:* CTI sharing can allow organizations to receive information about new variations of threat information. Threat actors continually change their TTPs to exploit new vulnerabilities and bypass security controls. Therefore, information about the most recent changes can help organizations rapidly detect and quickly respond to cyber threats and reduce the cost associated with defensive techniques [15].

Despite the CTI sharing benefits and significance, successful CTI sharing has been challenging due to the various technical (e.g., network scalability, heterogeneity in devices, etc.), commercial (e.g., incentives, supply chain issues), and policy enforcement (e.g., sharing agreement) perspectives [21–24]. Intelligence about cyber threats can increase defensive agility if it is accomplished in real-time, while current platforms for CTI sharing are still challenging to achieve the real-time sharing [25]. The existing CTI sharing platforms lack effective sharing methods that cause limitations which must be re-examined further. CTI sharing still requires more research and work to fully acquire knowledge maturation and situational awareness in organizations. Moreover, the content of CTI generated and used in CTI sharing may be of low quality. The quality of CTI is measured by specific parameters, e.g., completeness, interoperability, timeliness, integrity, and false-positive ratio, and the existing CTI feeds are challenging to fully achieve these parameters.

1.2. Existing surveys on CTI sharing and our contributions

Several proposals try to combine the diverse aspects of CTI and their associated challenges and opportunities. However, only a few comprehensively discuss the CTI sharing issues, focusing on different aspects of CTI sharing approaches. In Table 1, we present the comparison of our survey to the existing surveys on CTI sharing. For example, Wagner et al. [27] provides a survey of CTI sharing and list some challenges focusing on technical issues (e.g., privacy and anonymity) and non-technical issues (e.g., CTI sharing regulations) along with the CTI actionable attributes (e.g., relevance, timeliness, accuracy, completeness, and ingestibility). It discusses various areas of CTI sharing, including indicators, advantages, risks, human role, industry sector sharing, cultural and language barriers, automation and collaboration, and it also includes use cases for elaborating CTI actionable attributes. The paper mainly focuses on the CTI sharing requirements and does not focus on a comprehensive discussion of various available approaches to CTI sharing. Proposal [28] presents an analysis of the existing threat intelligence platforms and sharing mechanisms. It reviews the development of CTI sharing and discusses the critical challenges faced by threat intelligence sharing, e.g., legal barriers, CTI quality, budget issues, and lack of trust. The authors propose a 'threat intelligence alliance' model to develop regional network security capabilities. Proposal [29] provides an overview of the threat information sharing benefits, challenges and existing standards. It also studies the CTI concept and the process of producing functional, actionable threat intelligence extracted from CTI collection and assessment. In the context of the CTI proposal, [10] presents a survey on cybersecurity information sharing based on the methodologies implemented to address the cybersecurity information-sharing problems. The main focus of their survey is to analyze the works that applied game-theoretical models in their proposed approaches. In a similar aspect of [10], proposal [26] discusses the dimensions of cybersecurity information sharing and evaluates different legal, economic, and regulatory issues. In [3], the authors propose a survey of the existing platforms for threat intelligence sharing based on their applied methodologies, protocols and tools.

The state of the art surveys in CTI sharing show that only a few surveys explore the various challenges of CTI sharing, e.g., [3,27–29], and some others, e.g., [10,26] discuss the importance of CTI without the detailed motivation of CTI sharing. There is a significant lack in the existing surveys of a comprehensive discussion that covers the different visions on CTI sharing and its challenges, including emerging approaches and platforms to address CTI sharing in a secure, efficient, and fine-grained way. There is also a lack of discussion regarding how the various CTI sharing platforms and architectures can address the significant challenges of decentralized sharing, security, privacy, and trust issues, alongside the various characteristics (e.g., mobility, heterogeneity, resource-constrained nature of the devices, etc.) of a dynamic system like the IoT to meet the critical requirements of CTI sharing.

Table 1
Previous surveys on CTI sharing and their comparison with our work (year of publication in ascending order).

Ref.	Year	Blockchain integration	ML models	Use of incentives	Commercial platforms	Collaborative sharing	Hybrid models	CTI life cycle	CTI sharing architectures	CTI sharing challenges	Adv. computing platforms	Consider IoT
[26]	2016	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
[3]	2018	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗
[27]	2019	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓
[10]	2019	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗
[28]	2020	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗
[29]	2021	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
[**Our survey**]	2023	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

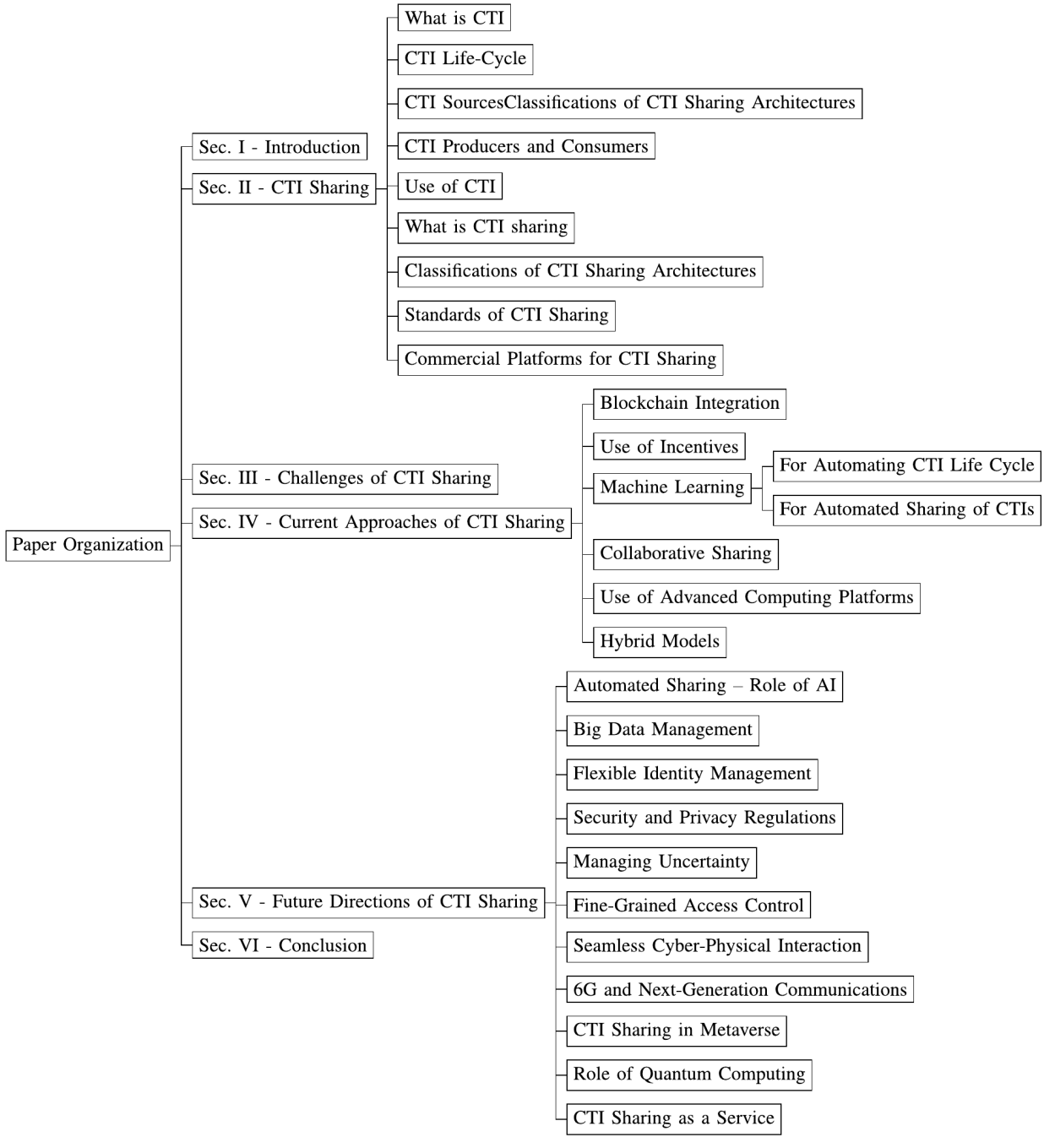

Fig. 1. The outline of the organization of the paper.

In this survey, we provide a comprehensive study on CTI sharing. To the best of our knowledge, our work is the first one that discusses the various aspects of CTI sharing, including the basics of CTI, various CTI sharing architectures, challenges of CTI sharing, and an in-depth analysis of future CTI sharing in a single piece of literature. Moreover, unlike the existing surveys, we include the difference between CTI and general information sharing approaches and explicitly consider the literature on CTI sharing. Furthermore, we classify the various possible architectures of CTI sharing and see the potential approaches and methods that could fit into this domain. Finally, our devised list of challenges is compared with the existing approaches for CTI sharing and examines how the available proposals address these challenges. Significantly, our survey brings the latest development in CTI sharing using emerging technologies, e.g., blockchain, machine learning, and edge intelligence, which are craved in recent surveys. The major contribution of the paper can be summarized as follows:

- Existing surveys on CTI sharing primarily focus on the CTI information and the integration into one or more inter-related systems. They pay little attention to the fundamental challenges of CTI sharing and the list of approaches and methods for CTI sharing. In this survey, we provide a thorough investigation and analysis of CTI sharing approaches and methods.
- We include the basics of CTI and CTI lifecycle, CTI sharing architectures, and the commonly used platforms, protocols, and standards for CTI sharing. We also highlight the explicit distinction between our survey paper and existing survey works on CTI sharing.
- We comprehensively analyze the CTI sharing challenges in terms of sixteen district issues. Then, based on these challenges, we examine the available CTI sharing approaches and provide critical analysis of how the present approaches meet such issues.
- We present a list of essential future research directions for CTI sharing, many of which have not been noted in previous works. These future research directions summarize to exploit the benefits of the next generation of CTI sharing at scale along with the employability of emerging technologies.

1.3. Paper organization and roadmap

We collect articles from a broader period of time on CTI sharing, CTI basics, and CTI sharing applications and uses. We consider book chapters, journals, magazines, conferences and workshops, and opened-sources articles from multiple disciplinary repositories (e.g., technical reports and arXiv documents). During the primary article selection process on CTI relevant to our survey, we mostly search the keywords CTI, CTI sharing, CTI applications, and cyber threat in the abstract and introduction. Then, we evaluate the articles by examining whether it illustrates an architecture, present a survey, explore different CTI sharing mechanisms, etc. Thompson Routers, IEEE Explore, Computing Classification System (ACM), and Google Scholar are used for our case. Therefore, our methodology for collecting and analyzing CTI articles combines a systematic approach with comprehensive search strategies and evaluation criteria described above. By following this methodology, we provide a thorough overview of the current landscape of CTI research, encompassing diverse perspectives and insights from academic and professional sources.

As illustrated in Fig. 1, Section 2 discusses the basics of CTI sharing, its lifecycle, significance, standards, and different CTI sharing architectures. In Section 3, we introduce a list of challenges for CTI sharing. Section 4 presents a comprehensive list of current approaches to CTI sharing and their critical analysis to address the list of challenges. In Section 5, we provide a list of unique future research directions for CTI sharing. Finally, Section 6 concludes the paper. In Table 2, we provide a list of notations used in this survey.

Table 2
List of acronyms used in this survey.

Acronyms	Full form
ABAC	Attribute-Based Access Control
AI	Artificial Intelligence
AML	Automation Markup Language
API	Application Programming Interface
CIF	Collective Intelligence Framework
CIO	Chief Information Officer
CIS	Communication and Information System
CISO	Chief Information Security Officer
CPS	Cyber Physical systems
CTI	Cyber Threat Intelligence
CTO	Chief Technology Officer
CVRF	Common Vulnerability Reporting Format
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IR	Incident Response
IoT	Internet of Things
IIoT	Industrial Internet of Things
IoC	Indicators of Compromise (IoC)
MAEC	Malware Attribute Enumeration and Characterization
NFT	Non-Fungible Token
OTX	Open Threat Exchange
OVAL	Open Vulnerability and Assessment Language
OSINT	Open-Source Threat Intelligence
PRE	Proxy Re-Encryption
QoD	Quality of Detection
QoM	Quality of Mitigation
RBAC	Role-Based Access Control (RBAC)
RID	Real time Inter-network Defense
SIEM	Security Information and Event Management
SOC	Security Operations Center
STIX	Structured Threat Information eXpression
TTP	Tactics, Techniques, and Procedures
TAXII	Trusted Automated eXchange of Indicator Information
TRADE	TRusted Anonymous Data Exchange
TTE	Trusted Execution Environment

2. Cyber threat intelligence sharing

In this section, we provide a discussion on CTI and CTI sharing. At first, we present the definition of CTI and then explore the various issues, e.g., CTI life cycle, CTI sources, platforms and protocols for CTI sharing, including different CTI sharing architectures.

2.1. What is CTI?

Before defining CTI, it is useful to distinguish between the terms *data*, *information*, and *intelligence* to understand their differences and relationships. Data refers to raw, unfiltered, unanalyzed outputs usually generated in large volumes in an operational environment, e.g., a series of IP addresses, logs, domain names, and signals. Data becomes information when collated, processed, and refined to represent meaningful outputs for an end-user. For example, the series of IP addresses are now sorted by whether they are linked to suspicious activities in the network. The refined information is then analyzed and transformed into intelligence, which involves contextualizing the information with other information, e.g., the history of previous incident reports and formatting the information into human and/or machine-readable formats. The finished intelligence products could inform decision-making regarding responsive action, e.g., detecting a potential threat and developing a mitigation strategy.

CTI is a collection of information about potential attacks that can threaten the cyber safety of organizations and assist organizations in identifying, analyzing, monitoring, and responding to cyber threats [30]. CTI should have three main characteristics including (i) evidence based, (ii) actionable, and (iii) effectiveness [31–33]. CTI is best defined as evidence-based knowledge that contains various types of information, including indicators, mechanisms, consequences, framework, and actionable instruction about current or emerging cyber

threats to assets, which can provide effective decision-making support to organizations regarding the threat response. CTI can be categorized into the following four distinct categories [34]:

- ***Strategic*** – refers to non-technical information with the aim of supporting executives in decision making including CIOs, CISOs, CTOs and Executive boards. All strategic CTI deliverables are written in a language for policy makers and strategists.
- ***Operational*** – includes information about the threat actors and their behaviors. Operational CTI investigates the capabilities and deals with TTPs. These types of CTIs are mostly useful for threat hunters. 'security operations centers' (SOCs) analysts, incident response teams and vulnerability management teams.
- ***Tactical*** – deals with identifying the IoCs and TTPs are and also the low-level, technical details of individual attacks and attackers. Tactical CTI is usually produced for the incident response (IR) team, SOC analysts, risk analysts, IT, and IT tools including SIEM, firewalls, IDS/IPS, endpoints.
- ***Technical*** – consists of technical information that can be seen on threat intelligence feed about malware and adversarial campaigns. This contains an attacker's assets, attack vectors used, command and management domains used, and vulnerabilities exploited.

2.2. CTI life-cycle

CTI is produced in a methodical, ongoing process known as CTI life cycle. In Fig. 2 we illustrate a CTI life cycle. In this process, data and information related to threats identified and collected for producing CTI [32]. The produced CTI in this life cycle will be ready to share with consumers. CTI life cycle consists of the following five stages:

- ***Stage 1 – Planning and Direction:*** CTI lifecycle starts with planning and direction which is the most important stage. At this stage, the CTI consumers, intelligence requirements, and intelligence priorities are identified. Significant collaboration between the consumer and producer of CTI happens at this stage. The output of planning and direction phase often outlines the intelligence collection plan which includes the scope and purpose of intelligence.
- ***Stage 2 – Collection*** In this stage the desired intelligence data that is defined in stage one is collected from various sources. Organizations actively collect a wide range of threat types, including phishing attempts, compromised credentials, vulnerabilities, and network logs, for processing and exploitation in the next stage. The collection of logs is typically carried out by specialized security teams within the organization. These logs may include various types of data, e.g., network logs, system logs, application logs, and security event logs.
- ***Stage 3 – Processing and Exploitation:*** In this stage, the data obtained from the last stage is processed for exploitation. The collected data in Stage 2 is in the form of raw data and in the processing stage, collected threat data are normalized, structured, arranged, and transformed into useful information to be directly used in the next stage (Stage 4). At this stage (Stage 3) some automated tools may be used to apply data processing functions such as structuring, data correlation, parsing, data reduction decryption, language translation, filtering, and data aggregation.
- ***Stage 4 – Analysis and Production:*** At this stage, the processed intelligence from the previous stage is analyzed, integrated, interpreted, evaluated, and translated into meaningful intelligence and contextual information, e.g., threat actors, events, and attributes. The analysis stage target is mainly qualitative and often human-oriented process [35,36]. However, other data analysis techniques may be applied at this stage to provide both qualitative and quantitative analyses, e.g., machine-learning-based techniques, and statistical methods. After analyzing the threat intelligence, the severity, significance, and consequence of the threat intelligence based on the business and environmental context gets assessed that further helps in developing appropriate countermeasures to respond to the identified threats.
- ***Stage 5 – Dissemination and Feedback:*** The intelligence that is the outcome of Analysis and Production Stage (Stage 4) is reported in this step considering the intelligence priority and confidentiality that is defined in the analysis stage. The dissemination stage requires the threat intelligence to be translated into a standard format and present the results to the consumers [35].

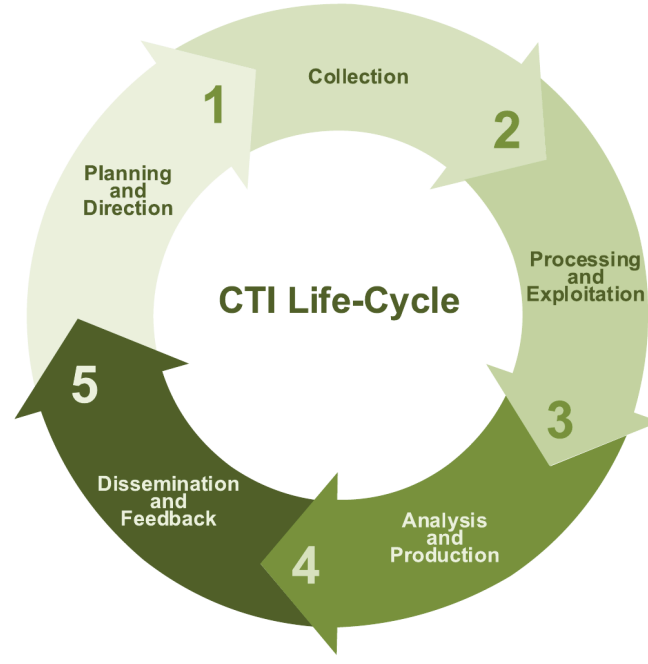

Fig. 2. Different stages of a CTI life-cycle discussed in [32].

2.3. CTI sources

The collection phase of CTI involves collecting the necessary data from various sources. The sources should meet the requirement of intelligence and be trusted and relevant. For example, the dark web is a CTI source that receives significant attention from CTI platforms. The dark web includes social media platforms and online markets where hackers use it globally to trade and sell malicious hacking software, tools, content, knowledge, and other cyber assets on hacker forums [37]. Although hackers and cyber criminals use it, analyzing the dark web is considered an effective method for generating CTI [38,39]. In general, CTI sources are categorized into three major types:

- ***Internal*** sources that are internally available in organizations including IoCs, network event logs, firewall logs, router logs, IDS, records of past incident responses, vulnerability scans, etc. [16,40].
- ***External*** sources are those that are outside of the organizations, and they include threat intelligence feeds, structured data reports that are sourced from the TAXII and MISP platforms (shown in Table 3 in Section 2.9), and unstructured reports [13,16,41]
- ***Open-Source Threat Intelligence*** (OSINT) refers to the intelligence from publicly available sources including newspapers and magazines, published academic researches and articles, application or system vulnerability data, publicly shared indicators of cyber attacks like IP addresses and domain names, social media

activity, news feeds, vendor blogs. The collected intelligence from this source is often unstructured, free, and legal [16,41].

2.4. CTI producers and consumers

CTI producer refers to an entity that uses a threat intelligence process to produce CTI [42]. The CTI producer follows a methodology for collecting reliable, relevant and useful data related to the requirements of intelligence consumers. This methodology can be defined and selected in the first stage of the CTI life cycle [43].

CTI consumer refers to an entity that can use CTI to improve its cyber defense mechanisms and make decisions about cybersecurity issues [42]. In addition, CTI consumers usually subscribe to CTI feeds provided by CTI producers to receive the latest threat intelligence on time [44]. Note that a CTI producer can be a CTI consumer, and similarly, a CTI consumer can act as a CTI producer. However, in which context they will act accordingly (i.e., CTI consumers or producers) remains an open question.

2.5. Use of CTI

Sharing CTI is an effective strategy to defend against cyber threats and improve cybersecurity [42]. Organizations use CTI to prevent, identify, and defend against the cyber threats that target an organization's resources. The valuable knowledge about cyber threats that CTI brings helps organizations establish adequate protection and mitigation mechanisms more proactively. In addition, CTI supports 'communication and information system' (CIS) security to enhance threat models used in the organization's decision-making process. For example, in NATO, a military organization, CTI provides the commander with critical intelligence about the adversaries, their objectives, and capabilities while operating in and through cyberspace [45]. During the years 2017 to 2019 and in 2021, the SANS institute has conducted comprehensive studies [46–49] about CTI, and the result of these studies show that CTI has many uses in an organization, from strategic services such as resource allocation and prioritization to tactical applications, e.g., threat alerting and response. Following processes are among the most common usage of CTI in organizations that have been identified in the above studies:

- Security operations (including proactively and continuously monitoring for threats)
- Improving detection capabilities
- Blocking threats
- Security awareness
- Threat management (for identified threats)
- Vulnerability management
- At-risk asset identification
- Incident response
- Threat hunting
- Risk management
- Prioritizing security controls
- Vulnerability remediation prioritization
- Cyber threat modeling
- IT operations (troubleshooting infrastructure)
- Security awareness training for staff
- Security standards compliance
- Decision making for security budgets

2.6. What is CTI sharing?

Recall that CTI sharing is a promising information exchange strategy attracting significant attention and support among cyber defenders and security professionals. It involves the exchange of contextual information and knowledge about advanced cyber threats between the producers and consumers, which could be presented in the form of

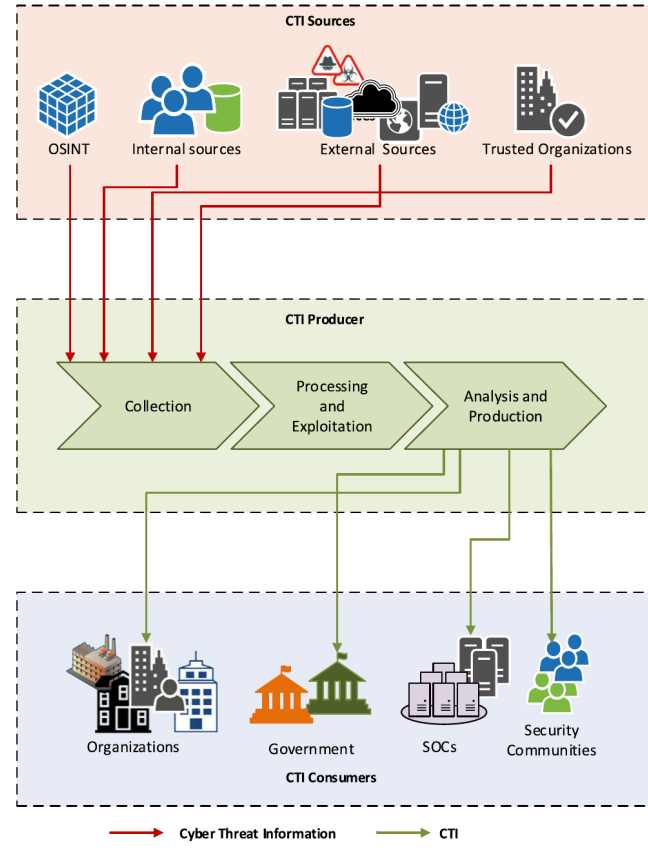

Fig. 3. A conceptual overview of a CTI sharing platform model composed of CTI sources, producers, and consumers.

IoCs, TTP, and best practice guides to detect, prevent, or mitigate the impact of security incidents [44]. In Fig. 3, we illustrate a generic model of the CTI sharing platform and show the relationships among CTI sharing components, e.g., sources, produces, and consumers. CTI producers collect cyber threat information to generate CTI. Then, the generated CTI is transferred to the CTI consumers.

2.7. Classifications of CTI sharing architectures

In this section, we examine the different architectures in which the CTI sharing would function. We present a classification of available CTI sharing architectures and note that they fall on the three commonly used network architecture classes, namely, centralized, decentralized, and distributed. In Fig. 4, we illustrate these architectures, and a description of each of them are listed as follows:

2.7.1. Centralized

Centralized architecture represents the 'hub-and-spoke' models [50]. In centralized CTI sharing, typically, a hub acts as a central repository for receiving data from the spokes (participating members of CTI sharing, which can be CTI producers or consumers, or they can hold both roles simultaneously). The central repository (hub) forwards the information to the consumers either directly or can improve the CTI before distributing it to the designated participants. One of the benefits of this model is that if the centralized hub uses open, standard data formats and transport protocols, participants may not need to employ multiple formats and protocols for CTI exchange with others. Moreover, in centralized models, the participants only connected to the centralized hub. However, a centralized network may cause a single point of failure because the CTI exchange in such a model is highly dependent on the central hub. The poor functioning or failure of the

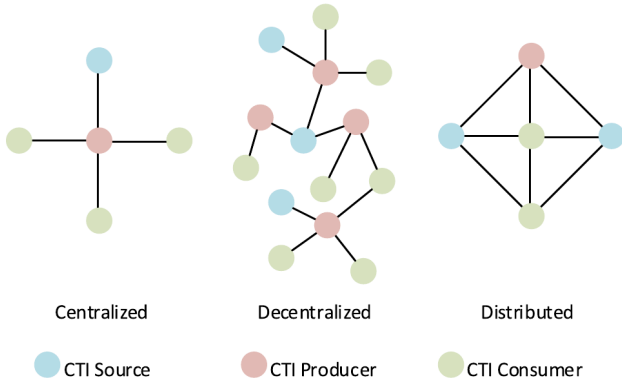

Fig. 4. A conceptual representation of different CTI sharing architectures.

hub will negatively impact the functionality of the participants. In addition, centralized hubs are a tempting target for attackers (due to the possibility of infecting the entire system through a single point of entry). Centralized hubs further do not address the scalability issue to a greater extent [51].

2.7.2. Decentralized

Decentralized architecture usually represents 'Peer-to-Peer' (P2P) models. There is no central hub in this architecture, and the participants can directly consume the information and share the CTI [52]. Furthermore, all the participants are involved in improving the distribution of CTI to the other participants. As a result, sharing is done much faster than in a centralized architecture. Decentralized architecture also provides higher robustness and does not cause a single point of failure because the information is available through different channels. Further, compared to centralized architecture, decentralized architectures are less likely to be the attacker's target into a single point of entry. The main drawback of a decentralized architecture is that it may not be able to support standard formats and transfer protocols required for seamless distribution of CTI among the participants. Therefore, the participants need to support different formats and protocols, which may cause some interoperability issues. The increasing number of participants may also grow the cost of managing and operating of system's functionality [50,53].

2.7.3. Distributed

Distributed architectures do not have a central node. Instead, each node (i.e., participant) has equivalent access, process, and sharing permission of information and therefore to the CTI, and the participant's privileges may be enabled exclusively in the nodes when required. Also, all the activities (i.e., access, process, and sharing of information) are shared among peers in an entirely distributed manner. Moreover, in a distributed CTI sharing, the resources (e.g., storage) are shared between participants in a distributed way which can improve the overall system's performance in terms of scalability, information dissemination, and accountability. This architecture is more stable and is safe from a single point of failure. However, it is more challenging to maintain than the decentralized and centralized models due to their highly dynamic nature [50,51].

These architectural classifications for CTI sharing can help to understand better the challenges based on the various purposes they serve. There is always a trade-off between these systems and their use in CTI sharing. For instance, on the one hand, a centralized CTI sharing architecture may provide more control over CTI data but suffers from a single point of failure and scalability issues. On the other hand, a distributed CTI sharing architecture can provide more scalability in CTI sharing but incorporates more security concerns to the system. Shan: That said, in a distributed architecture, system components are spread across multiple nodes or locations but still operate under a central authority or control. Decentralized architecture, however, lacks a central authority or control point. Instead, decision-making and control are distributed across multiple nodes. Note that distributed and decentralized architectures are distinct in their structures and more flexible than centralized architecture. However, the main difference between these two architectures is in their applications. Decentralized architecture promotes flexibility, security, and autonomy, while distributed networks focus more on scalability, efficiency, and high availability. However, selecting these architectures for the CTI sharing process highly depends upon the system's requirements and the designer's choice.

2.8. Standards of CTI sharing

Several standards and protocols have been developed to facilitate sharing and management of CTI. They collectively enable the effective use of CTI. In Table 3, we illustrate the most common standards and protocols used in recent literature.

STIX and TAXII have been developed by MITRE corporation to share CTI [54]. STIX is the most commonly used standard because of its modular structure which allows other protocols, e.g., CybOX, IODEF, and OpenIOC to be embedded into STIX. CybOX provides a standardized way to represent cyber observables events. Meanwhile, IODEF and OpenIOC extensions provide a way to express non-standard indicator patterns which are easy for human understanding. However, IODEF may not be suitable for automated integration of CTIs because it lacks elements to connect information. On the other hand, TAXII is transport protocol for STIX enables automated sharing of the CTI using HTTP/HTTPs.

MAEC provides a standardized framework for describing the characteristics and behaviors of malware, aiding in malware analysis and detection. However, MAEC's primary focus on malware attributes and behaviors may limit its usefulness for organizations seeking broader threat intelligence. TLP categorizes information into four color-coded levels (red, amber, green, and white), each indicating the degree of sensitivity and the extent to which the information can be shared [55].

2.9. Commercial platforms for CTI sharing

Commercial platforms are useful for any business model that creates value by facilitating CTI sharing between two or more organizations. However, these platforms must be commercially feasible and analytically valid. The existing CTI sharing standards and protocols (cf. Table 3) are being used in several commercial security products. In addition, different security tools, including the new generation of antiviruses, endpoint detection systems, vulnerability monitoring systems, and threat detection systems, must be enhanced by exchanging threat intelligence features to be effective and agile. Among the all available standards and protocols, the most commonly used ones in commercial products are STIX, and TAXII. Next, we list existing standards and protocols used for CTI sharing by the commercial platforms.

- **IBM X-Force Exchange** is a centralized, collaborative, cloud-based platform to ingest and share threat intelligence, and also act on it. This platform is supported by both human and machine-generated intelligence. IBM X-Force Exchange enables the consumers to be informed of emerging threats, research the security threats, gather actionable threat intelligence, collaborate with other consumers, and receive consultations from security experts. The platform uses STIX and TAXII standards and a RESTful (Representational State Transfer) API in JSON format to access information. Therefore, it can be integrated with other platforms. This platform can be used with IBM X-Force Exchange API, which is a commercial API to grant consumers and users programmatic access to open standards and to support contextualized security events [66] .

Table 3
A list of standards/protocols used for CTI sharing.

Standard/Protocol	Description
Structured Threat Information eXpression (STIX)	STIX is an open-source structured standardized language which is expressive, flexible, and extensible. It is developed to represent structured information about cyber threats. STIX is currently the most common language used to exchange CTI [16].
Trusted Automated eXchange of Indicator Information (TAXII)	TAXII is a protocol of application layer that is used for a simple and scalable way of communicating CTI. Using HTTP and HTTPS, TAXII can leverage the existing protocols. TAXII allows organizations to share CTI by defining an API designed based on a commonly used sharing model (e.g., P2P). TAXII is designed to enable the exchange of CTI represented in STIX [56].
Malware Attribute Enumeration and Characterization (MAEC)	MAEC is an expressive and standardized malware information sharing language for sharing and encoding high-fidelity structured information about malware based on the malware-specific attributes (i.e., malware behaviors, artifacts, and attack patterns) [16].
Open Threat Partner Exchange (OpenTPX)	OpenTPX is an open-source format for sharing network security operations data and threat intelligence, which are machine-readable. OpenTPX format is based on JSON and enable data exchange between connected systems [16,57].
Open Indicators of Compromise (OpenIOC)	OpenIOC is an open framework written in XML for threat intelligence exchange in a machine-readable format. The base schema of OpenIOC is extended for adding additional indicators from various sources. The users of OpenIOC can leverage its format to add their threat-related Indicators of Compromise (IoCs) and share them with other organizations [19].
Vocabulary for Event Recording and Incident Sharing (VERIS)	VERIS is a framework containing a collection of JSON-based metrics to record and classify security incidents. It allows defining the security incidents in a structured and repeatable way [58,59].
Incident Object Description Exchange Format (IODEF)	IODEF is a data model for describing computer security incidents information that can be shared with Computer Security Incident Response Teams (CSIRTs). IODEF has XML format [60].
The Cyber Observable eXpression (CybOX)	CybOX is a standardized structured language that enables encoding, and systematic communication of any observable cyber event in the operational cyber domain [61].
The Traffic Light Protocol (TLP)	TLP is a simple protocol established to facilitate sharing of data related to information security. TLP can promote effective collaboration and can ensure the appropriate sharing of sensitive information [62].
The Collective Intelligence Framework (CIF)	CIF is a threat intelligence client/server management system. CIF is used for sharing Threat intelligence and allows organizations to collect known malicious threat information from various sources for threat identification, threat detection, and mitigation [16,63]. In addition, CIF can enable CTI exporting for particular security tools.
Real time Inter-network Defense (RID)	RID is a standard for CTI communication. RID defines a communication method that is proactive and inter-network and enables quickly sharing of incident data. RID allows current mechanisms of incident detection, tracing, source identification, and mitigation to be integrated and create a complete incident-handling solution [64].
Open Threat Exchange (OTX)	OTX is a publicly available service and an open community of threat intelligence. OTX is designed by Alien Vault and used for communicating threat data, including indicators, malware details, and threat actors. It provides an automated mechanism for sharing CTI data. [65].

- **AT&T Cybersecurity USM Anywhere** is a unified cloud-hosted platform for threat detection, incident response and compliance management for cloud and on-premises environments. This platform automatically and constantly receives threat intelligence from Alien Labs security research team and from its crowd-sourced collaborative Open Threat Exchange (OTX). AT&T Alien Labs is the threat intelligence unit of AT&T Cybersecurity. Using the superb marketing visibility into the AT&T IP backbone, the global USM Sensor network, the AT&T Alien Labs Open Threat Exchange (OTX), and other sources of threat data, AT&T Alien Labs deliver tactical and timely threat intelligence for UMS unit [67].
- **CrowdStrike Falcon X** is a threat intelligence platform with automated malware investigation features. CrowdStrike Falcon X has three optional tiers, which are used for automatically investigating incidents and facilitating threat alert prioritization and threat responses. In addition, the platform has a real-time IoC feed and available APIs that allows integration with other security tools [68].
- **OpenCTI** is an open-source platform for managing CTI knowledge and observables. This platform allows consumers to structure, store, manage and visualize technical and non-technical cyber threat information. The structure of cyber threat information is based on the STIX2 standards and designed as a web application. OpenCTI can be integrated with other applications and tools, e.g., MITRE ATT&CK, MISP, and TheHive [69].
- **ThreatConnect Threat Intelligence Platform** is a threat intelligence platform that allows organizations to collect, analyze, and manage threat intelligence data. The platform supports STIX and TAXII [70].
- **BrightPoint Sentinel of BrightPoint Security** is a threat intelligence exchange platform that allows automation, threat analysis, and sharing threat insight into cyber threats. It uses machine learning and automated sharing of threat intelligence and supports various standards and feeds including TAXII, STIX, and CybOX [71].
- **Splunk Enterprise Security** is another next generation security intelligence sharing platform. It can be integrated with STIX, TAXII, and OpenIOC to provide access to threat intelligence [72].
- **Cisco Talos Intelligence Group** is a commercial threat intelligence team that is comprised of researchers, analysts and engineers. The objective of this team is to defend Cisco customers against cyber threats (known and new threats), discover vulnerabilities in common software. The team is supported by telemetry and systems to actionable threat intelligence for Cisco customers, products and services [73].

In Table 4, we present the list of commercial platforms, the architecture (e.g., centralized, decentralized, and distributed) that these commercial platforms have used, and the corresponding standards and protocols. Despite the well-argued advantages of CTI towards cyber resilience in academic literature, cost constrains may hinder the wide adoption of CTI sharing solutions in many organizations [74]. For instance, the lack of open platforms require organizations to invest in the initial licensing fee to procure a commercial CTI sharing platforms as shown highlighted in Table 4. The high cost of CTI sharing extends beyond the initial procurement, e.g., training of cyber security staff and maintenance/upgradation of CTI tools. This cost challenge can be effectively overcome with the return benefits linked to other challenges discussed in the next section, e.g., intelligent intelligence, automation, and timeliness.

3. Challenges of CTI sharing

The barriers to rapid and transparent CTI sharing are numerous. In this section, we outline the various challenges of CTI sharing. These challenges range from network communication to efficient collaboration and incentives. In Table 5 we summarize these challenges.

Table 4
List of commercial platforms, supported architecture, and corresponding standards and protocols used for CTI sharing.

Commercial platforms	Supported architecture	Standard/Protocol	Licensing
IBM X-Force Exchange	Centralized	TAXII, STIX	Commercial
AT&T Cybersecurity USM Anywhere	Centralized	Using OTX for STIX/TAXII feedserver	Commercial
CrowdStrike Falcon X	Centralized	Using API for conversation to standards	Commercial
OpenCTI	Centralized	STIX2	Open source
ThreatConnect	Centralized	STIX, TAXII	Commercial
BrightPoint Sentinel of BrightPoint Security	Distributed	TAXII, STIX, CybOX	Commercial
Splunk Enterprise Security	Centralized	STIX, TAXII, OpenIOC	Commercial
Cisco Talos Intelligence	Decentralized	STIX/TAXII, CVRF, OVAL	Commercial

Table 5
List of identified CTI sharing challenges (discussed in Section 3).

CTI sharing challenges	Description
Collaboration	A process of two or more entities working together to either accomplish a task or achieve a common goal.
Scalability	Scalability refers to the ability of a system to sustain its performance under changes to its workloads.
Automation	A method of making a process or a system operate automatically with minimal or no human intervention.
Timeliness	It refers to how up to date data is. In other words, it reflects the amount of time between the availability of data and the event that data describes (or shares).
Traceability	It is the ability to trace the originator of a particular piece of data.
Network bandwidth	Network bandwidth is the maximum rate of data that a network can transfer at a given time and across a given path.
Trust	It assists in resolving choices into decisions.
Privacy	It helps determine what information a system should share with others with appropriate authorization.
Integrity	It refers to accuracy, consistency and completeness of data throughout its entire lifecycle of an entity.
Standardization	It signifies the establishment of standards that relate to the data value chain.
Security	A mechanism protecting a system and information from unauthorized access, corruption, destruction, disclosure or theft of data.
Intelligent intelligence	CTI sharing systems as intelligence systems aim to provide information that is gathered from various data sources and is useful for security analysts or security systems.
Interoperability	It defines the basic ability of two or more systems or components to connect, exchange and use data across systems.
Integration	It refers to the process of linking different components and subsystems to a single, more extensive system so they can function as one.
Anonymity	Signifies keeping the identity of interacting entities separate from their activity. That is keeping the identity hidden from the others.
Heterogeneity	It reflects various circumstances and situations where the platforms and the entities may have different network domains, operating systems, technologies, protocols and administrative regulations.

3.1. Collaboration

It is the process of two or more entities working together to either accomplish a task or achieve a common goal. The practice of CTI sharing is tightly involved with the exchanging information. Proposal [44] defines CTI sharing as the exchange and collaboration on any security information that can enhance the security posture. Although collaboration by the means of sharing information is a promising way of addressing the cyber threats detection and prevention, it poses some challenges [75]. One of the collaboration challenges in CTI sharing is that entities would like to share their information but they cannot share due to the lack of collaborative CTI sharing models in which collaboration can be successfully addressed [27]. In addition, collaboration should happen in an agreed taxonomy so the issues related to taxonomy, policies and rules can negatively affect the collaboration [76].

3.2. Scalability

It refers to the ability of a system to sustain its increase performance under changes to its workloads. A scalable system should be able to continue working without being negatively affected when changes in size and volume of the work happens. A CTI sharing platform involves with various processes including data collection, data analysis, data exchange, management of participants and their requirements, etc [77]. Therefore, the CTI platform should be scalable enough to efficiently perform all the activities and manage large volume of data storage, data processing and data transformation without dismissing or disabling other attributes (timeliness, security, privacy, etc.) [78]. There are a number of scalability challenges that CTI sharing platforms face, including: (a) processing an extremely large number of CTI sharing participants (including consumers and producers), (b) managing the CTI sharing infrastructure, (c) distribution of CTI content, (d) managing the storage of data, and (e) consuming the resource [79].

3.3. Automation

It is the method of making a process or a system operate automatically with minimal or no human intervention. Security adversaries apply automation techniques to execute intelligence-driven attacks at machine speed while security defense systems heavily rely on manual defense techniques which has resulted in prolonged detection and response times [19]. Automation can significantly improve the effectiveness of the entire CTI sharing process but there are no complete and coherent mechanisms available for automating the CTI sharing in large scale [80]. Most of the available platforms have the lack of automation mechanism in intelligence collection process and sanitization of sensitive intelligence [81].

3.4. Timeliness

In the context of information, timeliness refers to how up to date information is. In other words, it reflects the amount of time between the availability of information and the event that information describes (or shares) [82]. Timeliness signifies an important characteristic of actionable cyber threat information, and it helps security defenders address security vulnerabilities before they are exploited and reduce the number of infections. Therefore, CTI sharing platforms should be able to share actionable information in real-time to be consumable for recipients in a timeliness manner. Also, because the threat environment changes quickly, the CTI must be acted upon quickly [80]. However, there are a number of issues that make it challenging for CTI sharing platforms to address the timeliness. On the one hand, actionable information is often the result of the analysis that requires time [83], and this is more time-consuming when the data and information sharing elements are prominent. On the other hand, to provide timely sharing of

CTI, an efficient and standardized approach is required that defines the data to be exchanged in the same way as reflected by the development of standards. However, most of the standards for information exchange emphasize the threat detection and threat response phases [84].

3.5. Traceability

It is the ability to trace the originator of a particular piece of information. In information security, traceability is an essential factor in verifying the context of data and validating the data [85]. Therefore, traceability can effectively increase the validity of data in CTI sharing systems. However, since CTI recognizes as a sensitive type of information for organizations, to build a traceable CTI sharing platform, sharing participants are required to define and enforce a policy that specifies the data to be shared, with whom and under what circumstances [86].

3.6. Network bandwidth

It is the maximum rate of data that a network can transfer at a given time and across a given path. Network bandwidth is measured by calculating the total amount of data traffic the network can send and receive in a specific time. In data sharing systems, network bandwidth is a very critical factor that can directly affect the performance of system. CTI sharing platforms require a mechanism for bandwidth management to perform communication activity efficiently. The architecture of network, data format and data sharing protocols are some of the factors that affect the bandwidth usage [87].

3.7. Trust

In information sharing systems, trust or trust relationship is an essential requirement. Sharing information about cyber threats and vulnerabilities requires a high level of confidence (i.e., trust) because of the level of shared sensitive information [88]. In a dynamic and scalable CTI sharing environment, commonly, trust refers to the trust between participants (i.e., trustors and trustees), trust in the quality of threat intelligence, and trust in the used sharing platform [89]. CTI sharing systems should be able to establish a trusted threat sharing environment which is a challenging issue and is not adequately addressed by current approaches. As identified by [15], establishing a trust relationship is one of the critical barriers to extensive and effective threat sharing.

3.8. Privacy

Privacy or privacy-preserving is an important principle of information-sharing systems. An effective information sharing system is required to maintain the privacy of the shared data in different situations and under various conditions without any compromise [90]. Privacy preservation of shared threat data can encourage entities to contribute to threat data sharing. However, cyber threat data sharing across organizational boundaries involves risks of data exposure, including personal information and the organization's internal information [91].

3.9. Integrity

It refers to accuracy, consistency and completeness of data throughout its entire lifecycle. In CTI sharing platforms, assuring data integrity is challenging. Threat sharing participants may have no control over how their data is being maintained and who is using their shared data, therefore the CTI sharing platform must ensure participants' confidence of the integrity of their data. To assure data integrity in CTI sharing, it is required to address: (1) how to collect and store data, (2) how to validate CTI consumers requests, (3) in which format data can be stored and transferred (4) how to manage data versions [92].

3.10. Standardization

Data standardization means establishing standards that relate to the data value chain. For example, data standards may relate to the dataset's terminology, structure, and organization or may cover the rules and regulations of data collection, storage, and usage, e.g., transferring protocols. Data standardization is a critical factor in facilitating and improving the use of data where portability and interoperability of data are required [93]. Therefore, data sharing platforms, e.g., CTI sharing platforms, require efficient and effective data standardization. However, one of the challenges that threat sharing organizations still deal with is the ability to structure cyber threat information to meet various sharing requirements with participants and consumers. For example, there are still many organizations that prefer to exchange information in a format that is both human-readable and machine-readable. Thus, in CTI sharing the threat information requires to be presented in a standardized and structured way so that the information is automatable, readable, meaningful, flexible, and extensible [61]. Yet with the increasing developments of CTI sharing techniques, the current state of data standardization suffers from constraints that negatively affect the performance of CTI sharing [94]. For example, some standards do not have representation elements for affected IT assets, or STIX does not have representation elements for tactics.

3.11. Security

Data security refers to the practice of data protection throughout its entire lifecycle from unauthorized access, corruption, destruction, disclosure or theft. Data security as concepts covers every aspect of information security including from the data storage and hardware security, administrative and access controls, and it also includes organizational policies and procedures [95,96]. Data security of participants in CTI sharing is a major requirement and platforms should be able to maintain it when data is in transit (during distribution) as well as when data is at rest (when data is stored in the data storage). Data security must be addressed without impairing data availability. Supporting data security in CTI sharing could be challenging due to different issues including, (a) inadequate security controls, (b) lack of data governance, (c) data discovery and classification, and (d) activity monitoring.

3.12. Intelligent intelligence

CTI sharing systems as intelligence systems aim to provide information that is gathered from various data sources and is useful for security analysts or security systems. This means the intelligence that such systems produce needs to be intelligent (e.g., meaningful and actionable) so that it can be easily understandable by various analysis systems (including machines and human analysts), contextual, accurate and can be leveraged in a timely manner [97]. That is, how specific a CTI is relevant to a particular organization. Security systems that are enhanced with intelligent CTI sharing can be more efficient and accurate with lower rate of false-positive alerting.

3.13. Interoperability

It defines the basic ability of two or more information systems to connect, exchange and use information across systems [98]. Sharing CTI with different entities especially with external CTI consumers have several interoperability challenges. These challenges are mainly related to technical standards, strategies and policies among CTI participants and legal barriers to sharing information [99].

3.14. Integration

It refers to linking different components and subsystems to a single, more extensive system so they can function as one. Integration can significantly enhance the overall outcome of the information-sharing processes, e.g., CTI sharing, allowing the information to be expedited and facilitating a better response across all systems. Integrating external intelligence feeds, integration with the existing CTI sharing technologies (e.g., TAXII) or integration with current techniques of incident detection, reporting and visualization is essential to improve the practical viability of CTI sharing platforms [9]. In addition, integrating CTI into security management systems is required to improve the information security posture of organizations [100]. However, integration has become a challenge for CTI sharing platforms primarily due to the incompatible protocols and formats for sharing or delivering CTI and the lack of technical capability to integrate CTI tools into an organization's security management systems [100,101].

3.15. Anonymity

Anonymity in the context of information security means keeping the identity of interacting entities separate from their activity. That is keeping the identity hidden from the others. In ICT services, it can be referred to as (i) *data anonymity* which means keeping the identifying information away from the exchanged data of a system or application, and (ii) *connection anonymity*, that is concealing the identity information of the source and destination throughout the entire process of data transfer [102]. Significantly, the CTI sharing platforms must require to satisfy the entities' privacy by anonymizing the content information. Therefore, to provide privacy in CTI sharing platforms (and therein to the systems), both data anonymity and connection anonymity is needed, and this can reflect the trust and reputation attributes, as well as privacy [27].

3.16. Heterogeneity

The CTI sharing must happen in various circumstances and situations where the platforms and the entities may have different network domains, operating systems, technologies, protocols and administrative regulations. This is true for the users who interact with the systems. Therefore, an appropriate CTI sharing solution must be provided at each stage of this composition and should be preserved by the system as a whole [103].

4. Current approaches of CTI sharing

In this section, we discuss the available approaches to CTI sharing. We examine these various approaches and see how they can address the different challenges identified in the previous section related to CTI sharing.

4.1. Blockchain integration

Blockchain is a distributed digital ledger consisting of sequence of encrypted blocks that record transactions [104,105]. The digital ledger (or database) is shared between members of a P2P network. Every node in a blockchain keeps the same copy of the updated digital ledger. Blockchain has no central authority and for this reason, in blockchain there is no single point of failure [106]. That is, blockchain has built in a distributed nature of structure in which the information cannot be manipulated, and it allows every node to access the entries of every other node so no central entity can grant control of the network [107]. Due to the structure of blockchain, it has a number of key features that are described as follow [108,109]:

- *Immutability:* The information in the blockchain cannot be changed due to applying advanced cryptography.

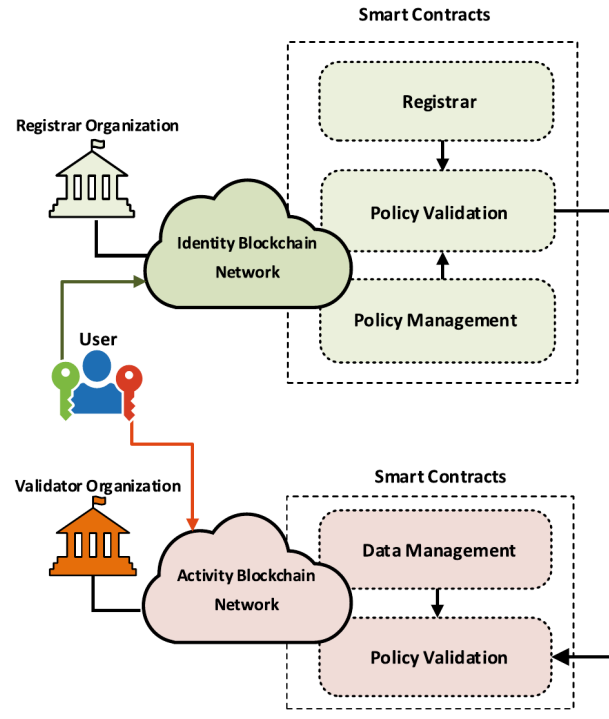

Fig. 5. Blockchain-based TRADE network architecture [111].

- *Transparency:* Since every node in a blockchain keeps the same copy of the updated digital ledger, the blockchains are transparent in information dissemination.
- *Decentralization:* There are no central entities that can gain the control of the blockchain network.
- *Authenticity:* All nodes have updated ledger that is accurate and consistent.
- *Anonymity:* Blockchain nodes can use anonymous and unique address numbers (private and public keys) which keep the node's identity private.
- *Auditability:* It allows every node to easily verify and trace the previous records. The nodes can access every other node and perform auditing process. Auditability property stems from the immutability and transparency of blockchain technology [110].

The inherent characteristics of blockchain help to build decentralized and distributed networks more reliably and securely, and it can be adopted for various systems, including CTI sharing [112,113]. Several CTI sharing models and frameworks have been proposed using blockchain technology. For example, Purohit et al. [114] introduce a novel DefenseChain platform that uses blockchain technology in threat intelligence sharing platform to improve the defense mechanisms against various types of cyber attacks (i.e., DDoS, APTs, and crypto-jacking). The DefenseChain model provides organizations with an incentive-based, trustworthy method of sharing threat intelligence. The model architecture reference is implemented using a consortium blockchain that allows sharing of threat data before and after attacks. In this way, the threat intelligence requester, affected by cyber attacks, can request a timely and robust manner of the threats defense from the detector(s) and mitigator(s) services. DefenseChain architecture is implemented for evaluation using NSF cloud infrastructure. This architecture has a peer federation network of organizations in which the peer organizations are connected through a central root switch. Every peer can carry out detection and mitigation protocols through its own dedicated equipment, including a controller and a 'quarantine virtual machine' (QVM). In the designed model, a Hyperledger is installed

on the controller component of each organization. The model has on-chain and off-chain components used for threat storage, processing, and sharing. DefenseChain addresses the scalability, integration and timeliness challenges of CTI sharing.

TRADE (TRusted Anonymous Data Exchange), proposed by Allouche et al. is another threat intelligence sharing platform based on blockchain [111]. The model allows P2P threat sharing, offers a distributed network without being required to use any trusted third party, and provides the information producer complete control of her shared threat information. TRADE platform can be easily adapted to organizations' threat sharing systems due to its flexibility in integration with commonly used threat sharing standards, including TAXII. By using blockchain technology, TRADE can simulate the P2P trust model without delays, and gap coverage and all activity transactions of network members are recorded on the blockchain, for example, when a member contributes to access or enriches the threat information. This trust model enables an immutable way to record the history of information flow that can be used for auditing purposes later. TRADE decoupled network architecture comprises two permissioned blockchain networks: (i) *Identity Blockchain Network* that stores the organization's profile and policies, which contributes to sharing and consuming threat information, and (ii) *Activity Blockchain Network* that monitors and logs the activities of organizations which contributes in sharing and consume threat information (cf. Fig. 5). The platform also has policy-based access control, enabling the organization to use various sharing policies reflecting different trust levels. In addition, smart contracts are used to enforce access and security policies in the framework.

Proposal [85] introduces a blockchain-based CTI platform known as 'BLOCIS', which allows the CTI system to be Sybil-resistance using smart contracts. BLOCIS increases the validity of the source and content of the data while it can detect and remove inaccurate data for resistance to a Sybil attack. BLOCIS platform architecture comprises three layers, including: (i) user layer, (ii) blockchain network layer, and (iii) feed layer. The user layer gathers CTI data from different sources, the blockchain network layer uses smart contracts to evaluate the validity of contributors' data, and the feed layer provides CTI data-sharing services. In addition, the blockchain network layer verifies data integrity and traceability. This layer stores the record of user layer reported data, contributors' information, the data collection procedure, and consumers' records and the feeds (that provide CTI data sharing services). BLOCIS uses smart contracts to conduct all the processes, including user requests, reporting, querying, and recording the history of data received from the feed layer.

To address the blockchain-based CTI sharing issues of performance in speed, scalability and security, proposal [30] discusses a novel blockchain-based CTI model. The model uses distributed reputation management systems and consortium blockchain to achieve automated analysis and processing and the response of the tactical threat intelligence (cf. Fig. 6). In addition, to meet the effectiveness and security requirements, the proposed model uses PoR (Proof-of-Reputation) based reputation model. The architecture of this model consists of (i) the original CTI obtained by CTI partner organizations from external or internal cybersecurity systems, and (ii) CTI sharing collaboration consortium, which is composed of – (a) proposal generation component, (b) intelligence decision component, and (c) analysis component.

Proposal [115] presents a CTI sharing model based on blockchain. The model offers an enhanced version of the peers and provides economic incentives to all involved parties. It also offers an Ethereum blockchain smart contract marketplace which is used better to incentivize sharing of CTI data between all involved parties. As a representation value for The CTI in the marketplace, the model creates a CTI token, a digital asset.

Hajizadeh et al. [116] proposes a secure distributed model to facilitate CTI sharing among diverse participants in which blockchain technology is used to assure tamper-proof record-keeping. It also uses

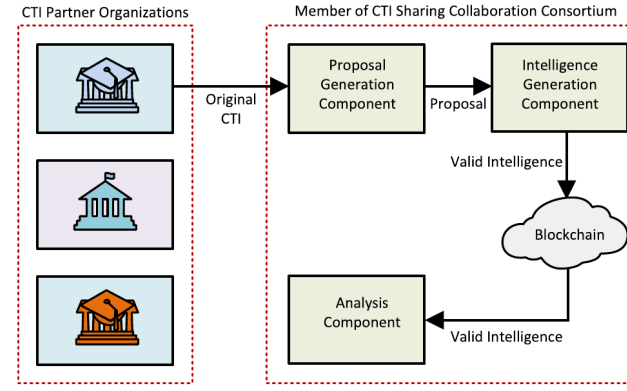

Fig. 6. A blockchain-based CTI sharing model discussed in [30].

smart contracts to guarantee immutable logic. The model utilizes an open-source permissioned blockchain platform, Hyperledger Fabric, to implement the blockchain application. Furthermore, unlike the other blockchain-based approaches, the model applies the flexibility and management capabilities of Software Defined Networking (SDN) to be integrated with the sharing platform to enhance defense perspectives against threats in the system.

Badsha et al. [106] employed a blockchain-based framework with a fine-grained access control mechanism to propose the BloCynFo-Share for cybersecurity information sharing among various organizations in a privacy-preserving manner. The model uses blockchain to provide the tamper-proof and non-repudiation attributes in which the record is stored in the format of chained hash and can be used for auditing in case malicious activity happens. By leveraging the blockchain benefits, the organizations in this model can have fine-grain access control so that they will be able to have control over which organizations can be granted access to their cybersecurity information. The architecture of this model comprises three entities: (i) Organization, (ii) Cloud Server/Proxy Server, and (iii) Trusted Manager. The source organization sends the encrypted CTI information to the cloud and stores the data-related hash (i.e., the hash of its data) in the blockchain.

Proposal [89] utilizes blockchain and Trusted Execution Environment (TEE) technologies in the proposed decentralized sharing framework named 'TITAN' for using the P2P reputation system. Using blockchain, this model ensures the security, integrity, and privacy of CTI information sharing. The typical TITAN architecture is made up of three layers: (i) the TI sharing layer, which is the P2P logically connected TI Sharing community, (ii) the reputation layer which is the core functionality of the system, and consists of two principal components including — the reputation system and TI quality assessment, and (iii) trusted execution layer that uses blockchain and TEE to store the trust and reputation score data and provide security and integrity against manipulation of the scores.

Mendez et al. [117] discuss a blockchain-enabled CTI sharing network (an Ethereum network) that applies distributed data collection technique to defend IoT devices used in the consumer market (e.g., home-based IoT devices). Using blockchain in this network allows for the sharing of critical information in a secure and immutable manner with smart contracts without requiring any centralized trust entity. To understand this process, when a known attack is recognized by a node (a participant), it interacts with the Ethereum network and triggers a blockchain transaction to be distributed to all the other nodes of the network. Then, the Ethereum network automatically initiates the proper defense against the attack.

To simulate the proposed network and all the resources, Microsoft Azure Ethereum proof-of-authority consortium template is employed. The simulated platform comprises three main components including (i) a server that acts as an administration gateway to the other parts of the

Table 6
Comparison of blockchain-based CTI sharing approaches based on discussed CTI sharing challenges in Section 3.

CTI sharing challenges	[85]	[111]	[30]	[115]	[116]	[114]	[106]	[117]	[89]	[118]	[119]
Year of publication	2020	2021	2021	2020	2020	2020	2020	2021	2019	2023	2023
Collaboration	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗
Network bandwidth	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Scalability	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	✓
Intelligent intelligence	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Automation	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
Security	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓
Privacy	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓
Trust	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✓
Traceability	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗
Timeliness	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗
Integrity	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓	✓
Standardization	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Interoperability	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Integration	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗
Anonymity	✗	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓
Heterogeneity	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗

network and is directly connected to the internet, (ii) a GNS3 server that connects to the local clients through TCP protocol, (iii) a series of replicated servers with same software load that represent the Ethereum blockchain network. In addition, this model utilizes the end user's first-hand data, including their network devices (e.g., IoT devices) and their detection systems, to share the threat intelligence information through blockchain.

Proposal [118] introduces an architecture for decentralized threat intelligence sharing system that utilizes STIX/TAXII standard, over a Hyperledger Fabric network. The proposed system implements a private permissioned blockchain network, Hyperledger Fabric, to enhance the confidentiality, integrity, availability, non-repudiation, and auditability. The decentralized architecture of this system consists of several components including (i) front-end, (ii) organization API gateway, (iii) peer nodes, (iv) state database, (v) certificate authority node, and (vi) ordering service that collaborate with each other to provide seamless threat intelligence sharing functionality.

Proposal [119] introduces Awareness Architecture Based on Blockchain CTI Convergence $(ABC)^2$ which is a reputation-based CTI Feed evaluation system and provides CTI sharing using blockchain technology. The main objective of this system is to evaluate the CTI Feed using a specific quality-based parameters. The system also proposes a new consensus algorithm namely, Proof-of-Quality (PoQ), in which the consensus results are based on a voting process. This proposal delivers benefits on reliability, quality, reputation, security, and consensus aspects of CTI evaluation, and storing and sharing mechanisms including.

Summary: The use of blockchain has become widespread to address CTI sharing. The salient features of blockchain, e.g., auditability, transparency, consensus, use of smart contracts, etc., provide key properties for CTI sharing. Blockchain-based CTI sharing models improve the trustworthy cooperation among CTI sharing participants and enhance privacy-preserving, security, integrity, and accuracy to improve CTI sharing to a greater extent. However, implementing blockchain-based CTI sharing platforms with a dynamic size or large scale still requires considerable attention. In Table 6, we provide a comprehensive summary of various CTI sharing challenges (discussed in Section 3) based on blockchain-based approaches. We note that the above-mentioned blockchain-based CTI sharing proposals are primarily published between 2019 and 2023, which indicates that applying blockchain in CTI sharing is an emerging research topic. The result demonstrated in Table 6 shows that blockchain-based proposals cover almost all the related CTI sharing challenges except the network bandwidth, intelligent intelligence, and standardization challenges. Nearly 82% (9 out of 11 papers) of the discussed blockchain-based proposals provide security and privacy challenges. In addition, 54.5% of the papers address trust, and scalability and 45% consider anonymity and automation challenges. According to this result, employing blockchain-based solutions seem to be a promising approach to overcoming many of the challenges we list for CTI sharing.

Table 7
List of incentives used for CTI sharing and their short description.

Incentive types	Description
Situational awareness	• Discusses about cyber situation. • Situational awareness is the core objective of CTI sharing. • CTI sharing helps organizations to improve the cyber threat detection and mitigation.
Economic	• Financial motivations for organizations to participate in CTI sharing. • CTI sharing is cost saving by decreasing security expenditure costs. • Participants may receive subsidies or win financial awards for sharing CTI.
Privilege/Award gaining	• Participation in CTI sharing can reduce or remove the subscription cost. • Contribution in CTI sharing may bring privileges (i.e., gaining access to CTI from government, law enforcement, or security services which is not available to other sources).
Trust relationship	• Trust relationships form the basis of CTI sharing, but require effort to establish and maintain. • CTI sharing can establish trust between the participant organizations and maintain the trust.
Legal protection	• CTI sharing may entitle organizations to receive legal protections from governments. • Legal protections could be including Cybersecurity Information Sharing Act (CISA) in US that provides legal protection for organizations that participate in CTI sharing.

4.2. Use of incentives

With the growing need for making improved decisions and the importance of CTI sharing, it is essential to learn how to minimize the barriers to sharing quality information and better align the benefits. One of the barriers to CTI sharing is the lack of incentives that encourage threat sharing among participants. In CTI sharing process, participants in CTI sharing plays a crucial role, but the studies, e.g., [27, 115,120], and [121] indicate that many organizations and users are reluctant to participate in sharing data due to various reasons including the lack of trust relationship between entities [114], participation cost [122], lack of financial allurement to participate [9,122], fear of reputations harm [120], and obligations and sanctions barriers [115].

Incentives can be a monetary reward, social reputation, or award for trusted collaboration. In Table 7, we present a list of incentives used

in CTI sharing. Next, we provide a list of the available approaches that aim to use incentives in CTI sharing. Note that the following approaches may use one or more technologies, platforms, or services to employ the incentive mechanism.

For example, Naghizadeh et al. [123] use a game-theoretic approach to employ incentives of entities for participating in security information sharing. This work proposes a repeated game formulation of security information-sharing games. To encourage the participant's cooperation in information sharing, this model offers the application of inter-temporal incentives, e.g., future conditioning cooperation on the history of past collaborations. Similarly, proposal [122] presents an incentive model for data sharing based on the evolutionary game theory approach, which applies blockchain smart contracts to execute the incentives. The smart contract mechanism in this model provides the dynamic control of the excitation parameters (user participation, enabling more users to participate in and the benefits of data sharing). The proposed approach encourages users to participate in data sharing regularly. The model successfully finds four distinct constraints that support the design of an adaptive smart contract mechanism for motivating the users to participate in data sharing. The incentive mechanism establishes an efficient mechanism for data sharing, which can be used for CTI sharing platforms to mitigate the challenges of organizations' unwillingness to share their CTI with one another.

To provide efficient CTI sharing among the organizations, proposal [124] discusses a secure, private, and incentivized CTI sharing architecture using blockchain. The proposed architecture can facilitate the secure dissemination of CTI data among multiple stakeholders in large-scale industrial systems, e.g., IIoT and Industry 5.0. Furthermore, using the employed CTI sharing architecture, organizations can use the collective knowledge, experience, and analytical capabilities to improve their security posture, threat awareness, detection capabilities, and organizational cybersecurity readiness. Finally, a proof of the concept prototype has been discussed using real-world use case scenarios to show the usefulness of the architecture.

DefenseChain [114] is a blockchain-based incentive model that introduces effective and efficient threat intelligence sharing using smart contracts. Using this model, organizations can mitigate the possible impacts of cyber attacks in a trustworthy and incentive-based way of cooperation. For the incentive-based approach, the model considers domain reputation as a factor in the decision-making process that builds a foundation of distributed trust. The reputation system of the model is based on the 'Beta' reputation system in which a set of protocols is used to accurately rate the peers in terms of some cyber defense metrics, including 'Quality of Detection' (QoD) and 'Quality of Mitigation' (QoM). These cyber defense metrics also support the economic model of DefenceChain to create and maintain the consortium with proximal peers or distant peers. Furthermore, the economic model applies some concepts, including a deposit system and a request/response deadline, to support reducing and eliminating false reporting and free-riding issues. For example, it offers to apply fine charging in case of non-ideal reporting and adds incentives for successful services of threat detection and mitigation request within deadlines.

With a similar motivation of [114], 'DEALER' platform [9] is implemented based on blockchain. It presents a novel protocol based on verifiers and token-based incentives to encourage fair sharing of high-quality threat intelligence data among the participants. It provides additional incentives for information sharing between the entities involved by supporting fulfilling legal reporting obligations for security incidents. Nevertheless, the decentralized architecture is supported by independent blockchain operators and the participants themselves. In Fig. 7, we show the conceptual overview (interaction among the various components) of the DEALER platform.

Proposal [125] discusses a blockchain-based data-sharing model employing an incentive mechanism. This model utilizes two blockchains to create a secure and reliable data-sharing environment.

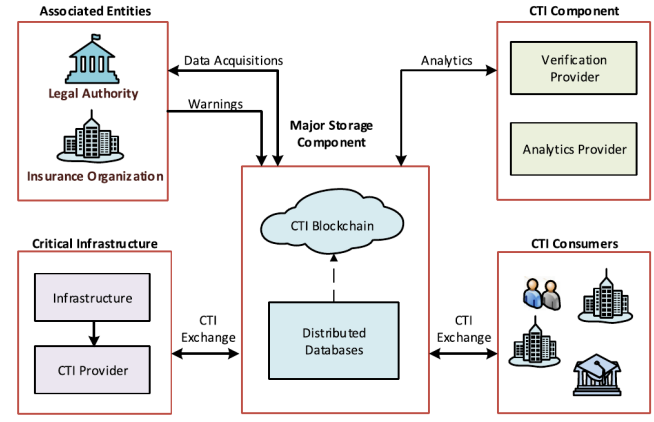

Fig. 7. The DEALER CTI sharing concept discussed in [9].

Table 8
Comparison of incentive-based CTI sharing approaches based on discussed CTI sharing challenges in Section 3.

CTI sharing challenges	[122]	[114]	[9]	[125]	[115]	[123]	[124]
Year of publication	2020	2020	2020	2019	2020	2016	2021
Collaboration	✓	✓	✗	✗	✗	✓	✓
Network bandwidth	✗	✗	✗	✗	✗	✗	✗
Scalability	✗	✓	✓	✓	✗	✓	✓
Intelligent intelligence	✗	✗	✗	✗	✗	✗	✗
Automation	✓	✓	✗	✗	✓	✗	✓
Security	✗	✓	✓	✓	✗	✓	✓
Privacy	✗	✓	✓	✗	✓	✓	✓
Trust	✓	✓	✗	✓	✓	✗	✓
Traceability	✗	✗	✗	✗	✗	✓	✗
Timeliness	✗	✓	✗	✗	✗	✗	✗
Integrity	✗	✗	✓	✗	✓	✗	✗
Standardization	✗	✗	✗	✗	✗	✗	✓
Interoperability	✗	✗	✗	✗	✓	✗	✗
Integration	✗	✓	✓	✗	✓	✗	✗
Anonymity	✗	✗	✓	✗	✓	✗	✓
Heterogeneity	✗	✓	✗	✗	✗	✗	✗

It also introduces a new incentive mechanism to motivate the organizations to use the system. The incentive mechanism in this proposal uses rewarding techniques in which the organizations that store the data receive rewards (economic incentives) like digital currency. The more data the organization stores, the more rewards it receives.

The authors in [115] propose an Ethereum blockchain-based CTI sharing model that offers economic incentives to all participants (both CTI producers and CTI consumers). The model uses a marketplace (CTI Marketplace) based on Ethereum blockchain smart contract to better incentivize all participants to cooperate in sharing. This proposal dedicates incentives for encouraging new types of participants in the CTI, sharing with different roles like investors, donors, and owners. The economic incentives used in this model include: (i) a new CTI token that represents the threat and risk intelligence data as a digital asset and can operate automatically between smart contracts, and (ii) cryptocurrencies to support the use of taxes in the exchange of knowledge (it can be paid per CTI use basis). Note that a smart contract can increase the economic incentives to CTI producers by creating a token the first time the contract is deployed (or the CTI producer shares a CTI). A token as a digital asset allows the possibility to invest in it so that its value may receive more interest in the CTI Marketplace. CTI consumers are required to pay a tax whenever they get the value of a reading transaction. Through each transaction a consumer executes, it receives important values, e.g., the knowledge of TTP detection algorithms beyond IoC.

Summary: Designing an effective incentive mechanism for CTI sharing is significantly desired to increase the accuracy and enhance the performance of the sharing process. In particular, we note the financial

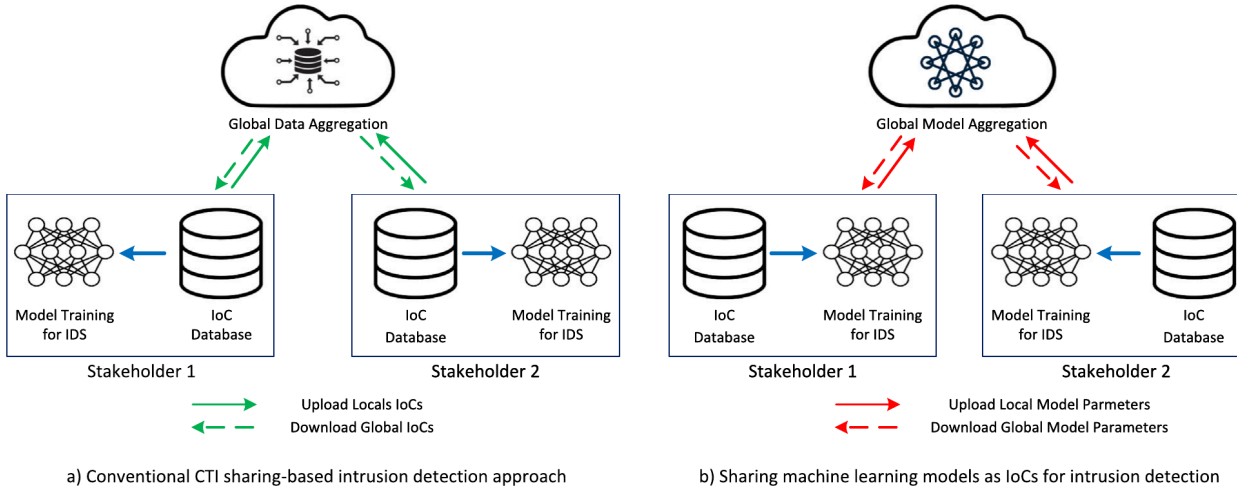

Fig. 8. Comparison between conventional versus machine learning-based CTI sharing approaches.

incentives that an organization or a participant offers to encourage certain behaviors or actions to be performed by other participants in sharing CTI. However, with the complexity of a multi-stakeholder system (public/government and private organizations and individuals) with different obligations and challenges for CTI sharing, it becomes more challenging to propose an ideal incentive-based approach for CTI sharing. In some cases, the game-theory approach is used as an effective mechanism to incentivize data sharing among firms. For instance, proposal [126] uses a multi-stage repeated game theory approach to establish incentives and improve the efficiency of information sharing among organizations. In this model, the reputation and punishment mechanisms are considered for organizations where the reputation is influenced by the strategies the organizations choose. The reputation will determine whether the organizations can participate in the next phase of sharing or not as well as the availability of sharing revenue. In addition, a punishment mechanism is used to modify behavior differently to encourage sharing information. In Table 8, we summarize the available approaches and the particular CTI sharing challenges they have addressed that we discuss in Section 3. According to Table 8, 71.4% (5 out of 7 papers) of the discussed incentive-based proposals for CTI sharing address the scalability, security, privacy, and trust challenges. In addition, 57% of the proposals consider collaboration and automation challenges, and almost 43% provide a solution to the integration and anonymity issues. However, none of the incentive-based proposals addresses the network bandwidth and intelligent intelligence challenges. The result signifies that incentive methods can improve CTI sharing, and they appear more effective in addressing the scalability, security, privacy, and trust challenges of CTI sharing.

4.3. Machine learning

The application of machine learning algorithms can be found in diverse fields, from engineering to social sciences [127]. A variety of machine learning algorithms has been developed in the past few decades to address diverse problems, e.g., classification, regression, and prediction analysis [128]. The main characteristics of machine learning algorithms involve clustering data based on similarities or differences and predicting future outcomes based on regression analysis [128]. These characteristics of machine learning algorithms may appear to be not well aligned with the CTI sharing requirements, e.g., collaboration, data confidentiality, privacy, anonymity, and interoperability [129], as discussed in Section 3. However, in this section, we argue that machine learning algorithms can play a vital role in the landscape of CTI sharing. First, we review the literature on how machine learning algorithms can address the challenges, e.g., automation, scalability, timeliness, and to automate different aspects of the CTI life cycle, e.g., CTI collection, CTI processing, and CTI analysis, which are in turn beneficial for CTI sharing [130]. Then we provide an overview of recent machine learning advances that offer a solution to CTI sharing challenges.

4.3.0.1. For automating different aspects of CTI life cycle. Recall, the scope of this paper is limited to CTI sharing aspect. Therefore, we provide a brief summary how approaches can be employed to automate different aspects of the CTI life cycle. For instance, Ghazi et al. [131] propose a machine learning-based approach to automate processing and analysis aspects of CTI life cycle. They proposed a natural language processing-based solution to extract threat feeds from unstructured CTI sources.

Koloveas et al. [132] propose a machine learning-based approach to automate the whole CTI life cycle, i.e., from planning and direction to dissemination of IoCs. Their framework makes use of structured sources, e.g., security databases and unstructured data sources, e.g., websites, social media, and marketplace forums to collect CTI data. For processing and analysis aspect of CTI life, they use natural language processing approach to extract intelligent intelligence and convert the collected data into actionable items. However, their framework relies on a particular existing machine-learning based platform for sharing collected CTIs. However, the proposed approach does not include an intrusion detection/prevention system (IDS/IPS) to detect anomalies in CTI data efficiently.

A detailed summary on the applications of machine learning approaches to automate different aspects of the CTI life cycle can be found in the review article by Montasari et al. [32]. In the following paragraphs, we summarize the literature on the application of machine learning algorithms for CTI sharing.

4.3.0.2. For automated sharing of CTIs. Recent efforts in the direction of automated CTI sharing based on machine learning algorithms are in several literature. For instance, Preuveneers and Joosen [133] suggest that traditional IoCs may not always capture the essence of a cybersecurity threat. Moreover, IoCs contain high-level information which is more suitable for human consumption. Therefore, information gathered by IoCs needs to be incorporated into IDS/IPS which can be time consuming and prone to error. Hence, this possibly leads to false alert fatigue and missed attack defections. To address this issue, proposal [133] further proposes a framework for sharing machine learning models instead of IoCs which can be directly incorporated into the target's IDS/IPS as shown in Fig. 8. Here, it can be observed that using federated learning approach, machine learning models can be trained locally and model parameters are then shared among stakeholders as shown in Fig. 8b instead of traditionally sharing the data or CTIs among stakeholders as shown in Fig. 8a. Hence, this federated

Table 9
Comparison of machine learning based CTI sharing approaches based on discussed CTI sharing challenges in Section 3.

CTI sharing challenges	[133]	[134]	[130]
Year of publication	2021	2021	2022
Collaboration	✓	✓	✓
Network bandwidth	✗	✗	✗
Scalability	✓	✓	✓
Intelligent intelligence	✓	✓	✓
Automation	✓	✓	✓
Security	✗	✓	✗
Privacy	✗	✓	✗
Trust	✗	✗	✗
Traceability	✗	✗	✗
Timeliness	✓	✓	✓
Integrity	✗	✗	✗
Standardization	✗	✗	✗
Interoperability	✗	✗	✗
Integration	✓	✓	✓
Anonymity	✗	✗	✗
Heterogeneity	✗	✗	✗

learning approach addresses the challenges associated with CTI sharing, e.g., data confidentiality and privacy [129]. Preuveneers et al. [133] also showed that their approach can be incorporated into existing CTI sharing platforms, i.e., MISP, TheHive, and Cortex.

The use of machine learning technologies, when designed and assessed in a single organization, is proven to be an effective technique for detecting network attacks [135]. However, developing a CTI system that allows various organizations to exchange machine learning models for collaborating in designing, training, and evaluating a scalable machine learning-based network intrusion detection system is challenging. The main challenge is using heterogeneous samples of network data originating from multiple sources for training a machine learning model. To address this issue, Sarhan et al. [134] propose a federated learning-based solution for sharing IDS as a CTI system. In the proposed approach, the machine learning model is locally trained, where only the updated weights are exchanged with the remaining participants in the federated averaging process.

A machine learning based CTI sharing system can be used in automating the implementation process of shared CTI while maintaining the privacy of an organization [134]. However, it may raise trust issues among CTI sharing parties. To address this challenge, Suryotrisongko et al. [130] propose blending eXplainable AI (XAI) to improve the explainability of the machine learning model. Incorporating XAI also addresses the issue of automation bias due to the limitation of a dataset. However, it may raise privacy preservation concerns by explicitly disclosing a user's information regarding the shared CTI data.

Summary: We note that machine learning techniques are beneficial for automated sharing and consumption of CTIs, including real-time data processing. Hence, increasing the effectiveness of CTIs for threat detection, machine learning produces accurate results in threat analysis by developing fast and efficient algorithms. Furthermore, machine learning techniques for CTI sharing are also helpful in addressing privacy concerns using privacy-enhancing techniques, e.g., differential privacy, compressive privacy, and synthetic data generation. However, employing these techniques would depend upon the application context and the designer's choice. Nevertheless, some challenges are associated with using machine learning techniques for CTI sharing, e.g., sensitivity to data bias and interoperability among heterogeneous nodes still need to be investigated. In Table 9, we provide a summary of CTI sharing proposals based on machine learning techniques and their critical analysis when addressing the various CTI sharing challenges discussed in Section 4.3. The result shows that all available machine learning proposals consider collaboration, scalability, automation, timeliness, intelligent intelligence, and integration challenges. In addition, 33.3% (1 out of 3 papers) of the machine learning proposals covered security and privacy challenges. However, the rest of the challenges are not covered widely by any proposals. Machine learning techniques seem more effective in addressing the intelligent intelligence challenge than incentive and blockchain-based approaches.

4.4. Collaborative sharing

It is noted that the collaboration in information sharing supports participants to detect potential risks, prevent cyber attacks at an early stage, facilitate the incident response, and provide awareness [136]. Therefore, a collaborative approach for CTI sharing has significant potential to deliver practical solutions for cyber threat defense by detecting and preventing malicious behaviors proactively [137]. Collaboration can: (i) develop the cyber situation awareness by effectively manage information and knowledge in different forms, (ii) develop a proactive defense mechanism to achieve a shared goal, (iii) reduce the time of threat detection across organizations, (iv) extend the insights about the threat landscape, malicious actors, security vulnerabilities to all appropriate participants, and (v) increase the threat detection accuracy as a workflow system [138,139].

Wagner et al. [27], presented a list of common collaboration models for CTI sharing based on P2P sharing, peer to repository sharing, and hybrid sharing (which is the combination of peer to peer and peer to repository models). These collaboration models integrate the following information sharing/communication models [50]:

- *P2P Sharing Model:* In this model, two or more organizations directly share CTI with one another based on either on-demand or as a legal agreement.
- *Hub and Spoke Sharing Model:* In this model, one organization (Hub) works as the central management for CTI, and it is responsible for coordinating CTI exchange between participating organizations (Spokes). Spokes can generate or use CTI from the hub.
- *Source/Subscriber Sharing Model:* In this model, one organization is CTI producer and works as the single source of CTI, and transfers CTI to consumers (which are subscribers). The subscribers can only act as consumers to use the CTI and they cannot generate CTI.

Next, we discuss a list of available collaborative CTI sharing models. For example, Zhao et al. [136] proposes a collaborative information sharing framework to enhance community cybersecurity. The proposed framework applies the 'group-centric Secure Information Sharing' (g-SIS) model and designs new features to support the collaboration in information sharing inside a community (e.g., a group of organizations). The g-SIS model brings users and information together in a group to provide access, facilitate agile sharing of externally sourced information, and create new information within the group [140]. The g-SIS model is suitable for CTI sharing in a dynamic environment and can improve sharing while protecting data in an organization.

To address the effective collaboration in a large-scale CTI sharing, proposal [141] suggests a global collaborative framework for sharing and structuring CTI information. In addition, the proposal applies existing frameworks, including NIST Cybersecurity, Intrusion Kill Chains, and STIX Cyber Threat Intelligence Reference Model, to present a new approach for cyber intelligence information sharing. The approach consists of three components, including: (i) *Framework Profile* – that guides interested participants to find the cost-effective way of managing their security risks, implementing their security controls, policies and procedures, and developing their security profiles. This component can even facilitate data cleaning and sharing across the sectors securely and reliably, (ii) *Structuring Creation of Curated Data* – is responsible for producing customized CTI for a specific set of group of organizations, and finally (iii) *Cyber Threat Analysis and Detection System (CTADS)* – enhances an analytical intelligence model that analyzes the IoC and observable patterns to provide information about the intrusion nature,

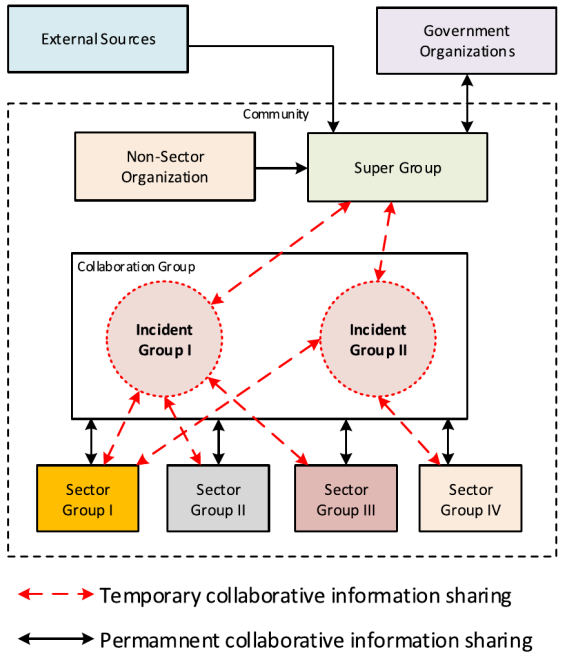

Fig. 9. Collaborative information sharing framework for community cybersecurity [142]. The black uni-directional arrow indicates the CTI feeds from external sources.

course of action and the level penetration. In addition, CTADS serves as a tool that supports cyber threat analysts in recreating the successful intrusion phases before detection.

To provide a privacy-aware collaborative CTI sharing, Wagner et al. [80] presented a CTI sharing framework that emphasizes the anonymity of the CTI producers and CTI consumers. For anonymous and automated sharing in collaboration using an MISP platform, the framework provides a model implementation of an anonymizing tool. This model employs the open-source and community-driven MISP, which manages and shares the CTI in human-readable and machine-readable data formats. To install the implemented model, Oracle's Virtual Box with Linux Ubuntu Server is used where it stores STIX-based CTI.

Proposal [142] presents a collaborative information-sharing framework based on group-centric models. This proposal considers a community comprising all entities within a particular geographical region, including government, academic, and industry organizations of both public and private sectors. This framework renders a formal policy model based on the community's requirements for information sharing. The policy model is created by developing different attributes for groups, users, and objects used in the model and defining the operations for the user and object membership, information flow, administration of groups and inter-group level relationships. This effectively enhances the CTI sharing among a wider group of participants distributed in diverse geographical locations. Fig. 9 depicts the conceptual outline of the framework. Red arrows show the cyber threat information flow during the period that an incident occurs. During the event of an incident, 'incident groups' dynamically are established inside the collaborative groups to support incident-specific information sharing. The black bi-directional arrows represent permanent information flow during the period with no incident where the 'sectors group', 'super group' and 'collaboration group' share information directly. Note, 'sector groups' represent the major sectors, e.g., finance, healthcare, police, telecommunications, etc. The black uni-directional arrow indicates the CTI feeds from external sources.

In recent years, the blockchain-based collaborative framework has been used for CTI sharing. For example, proposal [116] uses blockchain for CTI sharing, highlighting the need for collaborative CTI sharing.

Table 10
Comparison of collaborative CTI sharing approaches based on discussed CTI sharing challenges in Section 3.

CTI sharing challenges	[116]	[136]	[141]	[80]	[142]	[140]
Year of publication	2020	2012	2018	2017	2014	2011
Collaboration	✓	✓	✓	✓	✓	✓
Network bandwidth	✗	✗	✗	✗	✗	✗
Scalability	✗	✗	✗	✗	✗	✗
Intelligent intelligence	✗	✗	✗	✗	✗	✗
Automation	✗	✗	✓	✓	✓	✗
Security	✓	✓	✓	✗	✓	✓
Privacy	✓	✓	✗	✗	✓	✓
Trust	✓	✓	✗	✗	✓	✗
Traceability	✓	✗	✗	✗	✗	✗
Timeliness	✓	✗	✗	✗	✓	✗
Integrity	✗	✗	✗	✗	✗	✗
Standardization	✗	✗	✓	✗	✗	✗
Interoperability	✗	✗	✗	✓	✗	✗
Integration	✓	✗	✓	✗	✓	✗
Anonymity	✗	✗	✗	✓	✗	✗
Heterogeneity	✗	✗	✗	✓	✗	✗

This model aims to create collaborative cyber attack defense in SDN and address the common CTI collaboration issues, e.g., lack of trust among participants that derive from the possibility of information exploitation during the process of CTI sharing, privacy concerns about attackers gaining access to the shared CTI data, and lack of incentives for organizations to contribute to active CTI sharing. The proposed CTI sharing model also enhances a secure privacy-preserving platform where CTI producers and CTI consumers can collaboratively share sensitive CTI information.

Summary: The available approaches show that collaboration in exchanging threat intelligence is one of the primary objectives of CTI sharing. It can significantly increase the quality of CTI, accuracy, and effectiveness of threat sharing. However, designing a collaborative CTI sharing platform has been challenging in many cases because of communication limitations, lack of efficient collaboration mechanisms, standardization issues, cross-domain regulatory challenges, and fear of reputation loss. In Table 10, we list the available collaborative CTI sharing approaches and their critical analysis to the list of CTI sharing challenges devised in Section 3. The result illustrates that all available collaborative approaches for CTI sharing were published broadly from 2011 to 2020. We note that 83% (5 out of 6 papers) of the proposals address the security challenges, while 50% consider automation, trust, and integration. Notably, compared to other approaches to CTI sharing, e.g., blockchain, incentive, and machine learning, a collaborative sharing approach seems more effective in overcoming the standardization challenge.

4.5. Use of advanced computing platforms

Now we discuss three advanced technological platforms, namely, cloud computing, edge computing and fog computing, to address CTI sharing issues. These advanced computing platforms can provide more flexible and improved monitors of global cyber threats. They also offer flexibility for intelligence CTI data management and sharing platforms for using global data to identify, mitigate and remediate security threats.

Cloud Computing: It is a platform that delivers a set of configurable computing resources (e.g., networks, servers, storage, applications, and services) with universal, convenient, and on-demand network access. Cloud computing requires minimum management work and service provider interaction to release and provision rapidly [143]. Significant characteristics of cloud include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. In addition, cloud computing allows its users to use the computing resources and services per their requirements. Cloud computing is very similar to distributed computing [144].

Fog Computing: It places an intermediate decentralized computing layer between the source of data (e.g., cloud storage) and end users (e.g., edge devices) [145]. Fog computing is a virtualized platform that provides services like computing, storage, and networking between end devices and data centers located mostly at the edge of the network. Some of the notable characteristics of fog computing are including, (i) heterogeneity, (ii) low latency (iii) location awareness; (iv) mobility, (v) extended geographical distribution, and (vi) high number of distributed nodes [146].

Edge Computing: It refers to a set of connected network systems and devices that provide data collection, storing, processing, and analysis closer to the data sources. Edge computing enhances data processing while protecting the security and privacy of data because processing happens closer to where the data is generated. Therefore, the processing is done at a greater speed without requiring high bandwidth to transfer data to the cloud for processing and storage. The benefits of edge computing are considered as (i) extremely low latency because edge computing can bring the computation resources and services closer to the end-users and reduce the time required for accessing the services [147], (ii) scalability, edge computing can hierarchically design the end devices, edge computing devices, and cloud data centers that provide computing resources. Therefore, it can scale with the number of users without requiring a central location [148], and (iii) relatively low operating costs because of its ability to restrain the large volume of data to be transferred to the cloud (or other data centers) for computing operation. Consequently, it cuts down the bandwidth and energy cost [149,150].

Use of Cloud, Fog, and Edge Computing for CTI Sharing: The use of cloud, edge, and fog computing for CTI sharing may require different computing and storage resources [150–152]. Therefore, employing these technologies for CTI sharing frameworks must consider the context and particular need for CTI sharing [153–155].

The emergence of cloud computing is well discussed in IT sectors [156] and has become a popular distributed computing platform offered by commercial providers. In addition, the advent of fog and edge computing has considerably improved the services running on the wide-area network, including deploying IoT services. The combination of edge, fog and cloud provides different computing resources with various capabilities and offers distinctive benefits in information sharing. Deployment of applications on the cloud with different data flow and system models has been analyzed and still is an active area of research. However, applications programming and development models for edge and fog are still emerging concepts in CTI sharing context with several open research issues of security and privacy [157].

Proposal [158] presents a framework supported edge computing (called OpenEI) for intelligent processing and data sharing capability using a light-weight software platform at the edge devices. The proposed framework can potentially empower CTI sharing models, which are designed based on edge intelligence (of the devices), by addressing some of its challenges, including data sharing and collaborating and computing power limitations. The primary goal of deploying OpenEI is to make all the used computing hardware, regardless of its type, become an intelligent edge. The framework consists of three main components, including: (i) a package manager which runs inference and prepares the model locally, (ii) a model selector that selects the most fitting model for the edge, and (iii) a library that includes a RESTful API for data sharing. This framework can potentially support existing edge intelligence-based CTI sharing models by empowering edge nodes' processing and sharing capability.

Proposal [153] discusses that fog computing improves the applicability of systems that use cloud computing methods by bringing all the required resources to the end points (end users) towards the edge of the network. Proposal [153] further presents an infrastructure for information sharing and integrating a micro-distributed Security, Incident and Event Management (SIEM) - like architecture with the fog computing paradigm. The SIEM-like system is composed of a neural network for collecting, analyzing and sharing threat information. The infrastructure is based on OSSEC (note, OSSEC is an Open Source Host-based Intrusion Detection System) agents that are customized and locally installed, and it communicates with a central 'AlienVault' [65] deployment for event correlation. The proposed infrastructure can be implemented in the fog computing design as a fog controller where the compute node locates on the edge of the network and can inspect all the incoming network traffic. Threat information in this model is defined by STIX expressions, and by adding a TAXII server, the model can share the information with external organizations. The proposed infrastructure can be used as a CTI sharing model, especially in an IoT environment where threat analysis can be executed on end devices. This can reduce the system's computing load and increase CTI sharing efficiency.

Proposal [159] presents a framework for data sharing using fog computing. It explores the benefits of fog computing to address one-to-many data-sharing applications. The proposed framework can leverage

Table 11
Comparison of the advanced computing technologies CTI sharing approaches based on discussed CTI sharing challenges in Section 3.

CTI sharing challenges	[153]	[159]	[158]
Year of publication	2016	2017	2019
Collaboration	✗	✗	✓
Network bandwidth	✓	✗	✓
Scalability	✗	✓	✗
Intelligent intelligence	✗	✗	✗
Automation	✗	✗	✗
Security	✓	✓	✗
Privacy	✓	✓	✗
Trust	✗	✗	✗
Traceability	✗	✗	✗
Timeliness	✗	✓	✓
Integrity	✓	✗	✗
Standardization	✗	✗	✗
Interoperability	✗	✗	✓
Integration	✗	✗	✓
Anonymity	✗	✗	✗
Heterogeneity	✓	✗	✗

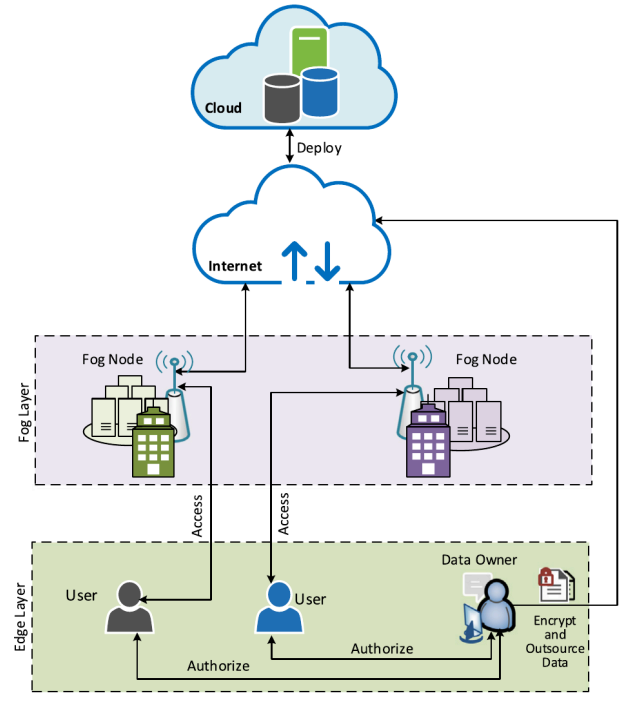

Fig. 10. A fog-based data sharing model discussed in [159].

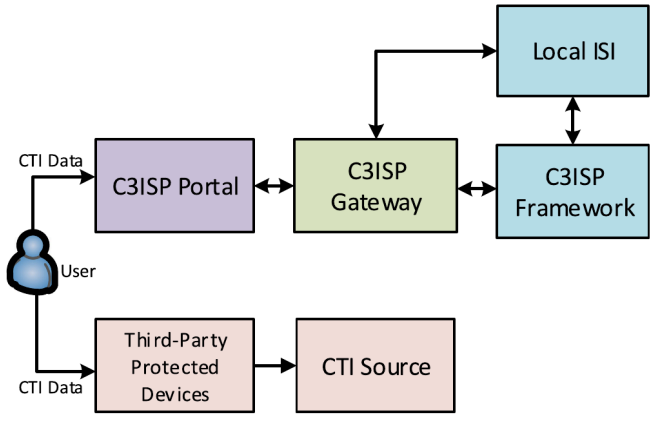

Fig. 11. The C3ISP architecture [121]. Organization's user can send CTI data to the framework either directly using the portal, or through the organization's third-party CTI protected devices.

Table 12
Comparison of hybrid CTI sharing approaches based on discussed CTI sharing challenges in Section 3.

CTI sharing challenges	[121]	[161]	[160]	[162]
Year of Publication	2020	2022	2021	2019
Collaboration	✗	✗	✗	✓
Network bandwidth	✗	✗	✗	✗
Scalability	✗	✗	✗	✗
Intelligent intelligence	✗	✗	✗	✗
Automation	✗	✗	✓	✗
Security	✗	✗	✗	✗
Privacy	✓	✗	✗	✓
Trust	✓	✗	✗	✗
Traceability	✗	✗	✗	✗
Timeliness	✗	✓	✗	✓
Integrity	✗	✗	✗	✗
Standardization	✗	✗	✗	✗
Interoperability	✗	✗	✗	✗
Integration	✗	✗	✓	✗
Anonymity	✓	✗	✗	✗
Heterogeneity	✗	✗	✗	✗

CTI sharing to improve (i) data confidentiality, (ii) fine-grained access control, (iii) scalability and efficiency, and (iv) real-time data sharing. This framework is based on the combination of 'key policy attribute-based encryption' (KP-ABE) and 'proxy re-encryption' (PRE) Fog techniques, and its sharing model uses a one-to-many mapping function. The proposed framework, Fig. 10, has four main components: data owner, cloud servers, fog nodes, and data users. The simulation results prove that the framework provides high scalability and data sharing in real time and with low latency, therefore, it offers a promising solution to securing data sharing in the developing fog computing environment. One potential application of the framework is CTI sharing in a fog environment, e.g., CTI sharing in IoT environment in which IoT devices can securely share CTI in a timely basis.

Summary: We note that the CTI sharing platforms can benefit from cloud, fog, and edge computing, to address the existing and emerging challenges. The present proposals of sharing and exchanging CTI using cloud computing, fog, and edge platforms show tremendous potential to address several challenges, including timeliness, scalability, and efficiency. However, these technologies are emerging computing models. Thus, their applications in diverse CTI sharing environments with various requirements of CTI sharing remain an open research issue. In Table 11 we summarize the available approaches of fog, edge, and cloud computing to address the list of CTI sharing challenges discussed in Section 3. The results demonstrate that almost 67% (2 out of 3 papers) of the available CTI sharing proposals based on the advanced computing technologies address the network bandwidth challenges as well as security, privacy, and timeliness, and 33% consider the heterogeneity issues. According to the result, compared to other approaches, the use of advanced computing platforms in CTI sharing shows to be the more effective technique to mitigate the challenges related to network bandwidth, heterogeneity, and timeliness.

4.6. Hybrid models

In CTI sharing, the combination of two or more approaches can be used to serve specific purposes. We denote them as a *hybrid* approach. For example, blockchain and machine learning together for CTI sharing. In this case, blockchain can be used to secure the storage and machine learning models can be used for efficient CTI data processing. Such a combination can be built purposefully to serve a specific CTI sharing requirement(s) and the context.

For example, Chadwick et al. [121] present a flexible cloud and edge-based data-sharing infrastructure (known as C3ISP) for CTI sharing. This work aims to address the issues regarding confidentiality and privacy of CTI sharing that can affect the level of sharing among participants. This infrastructure proposes a five-level trust model to allow the collaborators to share CTI confidentially. The infrastructure consists of different components, including the C3ISP framework, which is the main component and runs on the cloud, and the subsystems of the C3ISP framework, which include (a) the local 'information sharing infrastructure' (ISI) that runs in an edge device, (b) the C3ISP gateway, and (c) the C3ISP portal. The C3ISP subsystems, the gateway and portal, are designed in a way to operate in the user's edge devices and the cloud services as well. Fig. 11 shows an overview of the proposed infrastructure. Users of an organization can provide CTI data in multiple ways. The user is allowed to use a web browser to access the C3ISP portal directly, or the organization may outsource the CTI data collection to a third party, collecting the CTI data from users and sending it to C3ISP using the gateway. First, the CTI that the C3ISP gateway has collected is transferred to the local ISI to be processed and formatted into the STIX format and then to perform the protection operations on the formatted CTI. Next, the protected data is moved to the C3ISP framework for analysis. The framework can be deployed in four different identified sharing models, which are (i) fully centralized, where every subsystem of the C3ISP framework runs in the cloud only, (ii) hybrid, in which the components of ISI run on both an edge device and in the cloud, and the rest of subsystems run in the cloud, (iii) distributed, where only the ISI run on an edge device, and all other C3ISP subsystems run in the cloud, and (iv) fully-distributed, in which every subsystem of C3ISP framework run on edge devices. Note that the authors consider fully-distributed architecture when all the C3ISP framework subsystems are on edge devices. Fully-centralized architecture is when all the subsystems are in the cloud. Distributed architecture is when only the sharing subsystem (ISI) is on edge. Finally, the hybrid architecture is considered in which only the shared subsystem can run both on edge devices and in the cloud, and the rest of the subsystems run in the cloud. The proposed infrastructure is considered a hybrid CTI sharing framework because it is designed based on combining cloud and edge systems. It is flexible to be deployed in different sharing models.

Proposal [161] discusses a hybrid model using the deep learning (DL) model for CTI sharing to improve threat classification performance. This model does not directly insight a solution for CTI sharing. However, it provides a technical approach for CTI sharing models to enhance the cyber threat analysis accuracy and decrease the 'false positive rate' (FPR) of cyber threats for real-time analysis. The model is composed of two different neural network techniques: (i) a convolutional neural network (CNN) and (ii) a quasi-recurrent neural network (QRNN) and is tested on BoT IoT and TON IoT datasets. The test result verifies the enhancing effectiveness of data sharing by improving the classification accuracy and lowering the FPRs. This model can potentially be used for CTI sharing models to increase data processing

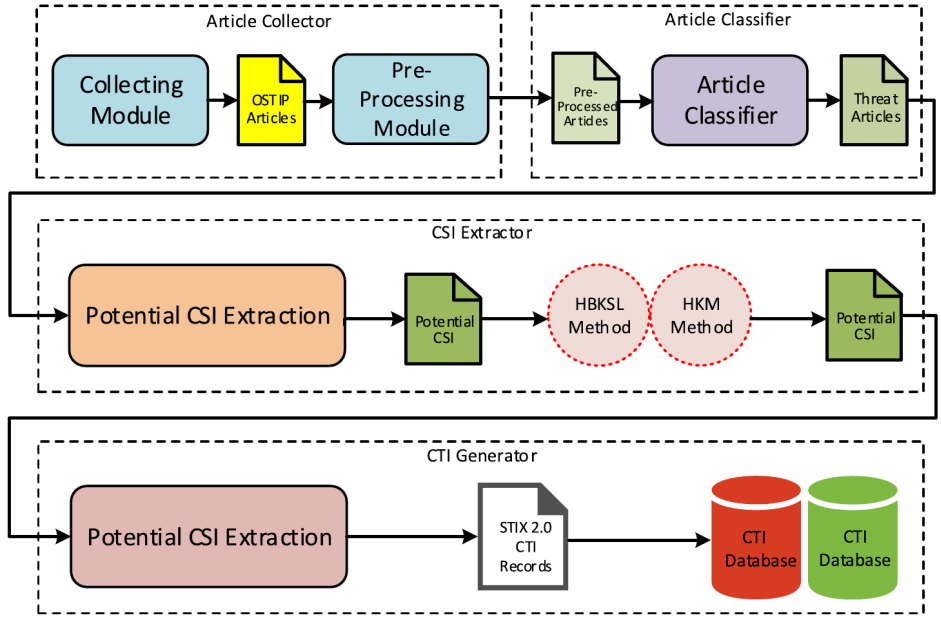

Fig. 12. An architecture using natural language processing and machine learning methods to generate the CTI records based on multi-type OSTIPs [160].

accuracy and real-time classification efficiency while sharing CTI at scale.

Proposal [160] offers an intuitive approach to generating the records of CTI based on multi-type 'open-source threat intelligence publishing platforms' (OSTIPs). It provides efficient CTI sharing by suggesting an automated, efficient CTI generation method for CTI sharing mechanisms. The proposal uses a hybrid model for gathering and generating CTI, combining the natural language processing (NLP) method, machine learning method, and cybersecurity threat intelligence knowledge. The architecture of the proposed CTI generation model, called 'GCO', is shown in Fig. 12. The architecture contains four main components, including (i) article collector, (ii) article classifier, (iii) 'cybersecurity intelligence' (CSIs) extractor, and (iv) CTI records generator. The components of the article collector and article classifier start the automated process in which it collects the articles from multi-type OSTIPs and classifies them. The article classifier component removes the articles that do not indicate a threat. The CSI extractor obtains all the details of CSIs from threat articles by applying the 'HTML-based key sentence location' (HBKSL) and 'hierarchical keyword matching' (HKM) methods. In the end, the CTI records generator converts the extracted CSI details into STIX 2.0 CTI records with mapping rules. Various CTI-sharing frameworks can widely use the extracted STIX 2.0-based records.

Proposal [162] presents a hybrid approach of CTI sharing combining a collaborative and incentive exchange platform known as 'Trustworthy collaboRative Intrusion DETection' (TRIDEnt). The platform is designed explicitly for CTI sharing. However, it enables and incentivizes organizations to exchange network alert data, including security alert sharing and correlation. TRIDEnT is a generic decentralized streaming marketplace and thus could be used for sharing any information, not just security alerts. The platform allows an organization to selectively advertise, sell and acquire security alerts in the form of (near) real-time P2P flow and therefore is considered adequate for CTI exchange. The proposed hybrid approach combines incentive and collaborative approaches, introducing an intuitive game-theoretic model and implemented based on the Ethereum blockchain. The TRIDEnT platform architecture is dissected into four conceptual layers, including (i) distributed ledger layer, which is the base layer of the architecture and moulds the trust foundations for the other layers by simulating a trusted third party, (ii) the trust management layer functions as a generalized reputation system that supports the trust management between organizations, (iii) marketplace layer that utilizes a token-based economic mechanism to provides economic incentives for trusted organizations based on the ratings, and (iv) data overlay layer that contains sharing channels for organizations where alert data and tokens are exchanged in a seamless and near-instantaneous way.

Summary: We note that designing an effective CTI sharing approach that addresses various challenges based on the context and application-specific scenarios may require applying different techniques together. For example, multiple phases of CTI sharing, including threat collection, analysis and sharing, can benefit from combining two or more approaches, e.g., machine learning techniques for more automatic analysis and processing of collected CTI, and blockchain for increasing the trust relationship and data storage security. Therefore, combining two or more approaches for CTI sharing, denoted as the hybrid model, can support addressing the CTI sharing challenges more efficiently using the advantages of different methods and techniques. In Table 12, we summarize the available hybrid CTI sharing models and analyze the CTI sharing challenges they have addressed that we list in Section 3. The result indicates that 50% (2 out of 4 papers) of the available hybrid approaches for CTI sharing consider the privacy and timeliness issues, whereas 25% address the collaboration, automation, trust, integration, and anonymity concerns. We note that the employability of hybrid models (and the combination of technologies) requires specific needs that could depend on the system's requirements and the designer's choice.

4.7. Summary of findings

The analysis of current approaches to CTI sharing reveals several key insights into the landscape of CTI-sharing methodologies. For example, blockchain emerges as a widespread solution for CTI sharing, leveraging its features like immutability, transparency, and decentralization. Despite its promising properties, challenges persist in implementing blockchain-based CTI-sharing platforms at scale, including issues related to network bandwidth, intelligent intelligence, and standardization. Blockchain solutions effectively address security and privacy concerns, making them particularly effective in mitigating these challenges.

We also note that the designing effective incentive mechanisms is crucial for enhancing the accuracy and performance of CTI sharing. Incentive-based proposals primarily address scalability, security,

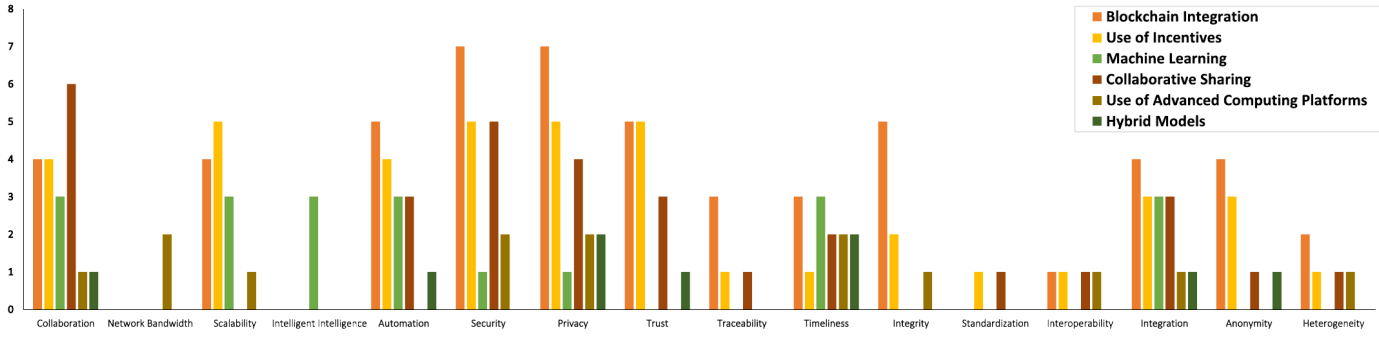

Fig. 13. The illustration of CTI-sharing approaches (discussed in 4) and the corresponding challenges (discussed in 3) they address. The X-axis represents the list of CTI sharing challenges, and the Y-axis represents the number of papers.

privacy, and trust challenges, but network bandwidth and intelligent intelligence challenges are overlooked. Incentive methods demonstrate promise in addressing scalability, security, privacy, and trust concerns. Similarly, the collaboration among participants (with the use of incentives) enhances CTI sharing effectiveness, leading to proactive threat detection and incident response. Various collaboration models facilitate efficient information exchange, improving cyber situation awareness and threat detection accuracy. Collaborative approaches effectively address security challenges and demonstrate effectiveness in overcoming standardization hurdles. Machine learning techniques offer automation capabilities for various aspects of the CTI life cycle, including processing and analysis. These techniques contribute to improving threat detection accuracy and efficiency, though challenges, e.g., data bias and interoperability persist. Machine learning approaches excel in addressing intelligent intelligence challenges but require further exploration in addressing other CTI sharing concerns comprehensively. Further, the use of advanced computing platforms, e.g., cloud, fog, and edge can offer flexible solutions for CTI sharing, addressing challenges, e.g., timeliness and scalability. These platforms show potential in mitigating network bandwidth issues, though further research is needed to explore their applicability across diverse CTI sharing environments.

In many cases, combining multiple approaches, e.g., blockchain and machine learning, offers tailored solutions for specific CTI sharing requirements. Hybrid models effectively address privacy and timeliness concerns, demonstrating flexibility in adapting to diverse CTI sharing scenarios. Overall, while each approach offers unique advantages in addressing specific CTI sharing challenges, combining multiple techniques in hybrid models holds promise for more comprehensive and effective CTI sharing solutions. Further research is necessary to enhance existing methodologies and develop robust CTI sharing frameworks capable of addressing the evolving landscape of cyber threats.

In Fig. 13, we present an illustration of the summary of findings from analyzing current approaches to CTI sharing, including blockchain integration, use of incentives, machine learning, collaborative sharing, use of advanced computing platforms, and hybrid approaches. As shown in this figure, blockchain integration and incentives are the dominant approaches in responding to most challenges of CTI sharing, where they address 13 and 14 challenges (out of 16 discussed in Section 3), respectively. Blockchain seems to be the most effective approach for mitigating security and privacy concerns, while incentive techniques have the highest percentage of proposals covering trust issues. Among the others, machine learning approaches are the only ones that provide solutions for addressing the intelligent intelligence challenge of CTI sharing. Advanced computing-based platforms only consider network bandwidth issues. We note that the CTI sharing can benefit from the effectiveness and strength of these approaches to address the diverse challenges. However, the result indicates that applying the analyzed techniques as an individual approach is not capable enough to overcome all the related CTI sharing concerns. Therefore, further research and investigation are still required to improve the most advanced and effective techniques to implement practical, robust, and effective CTI sharing.

5. Future directions of CTI sharing

In this section, we discuss the potential approaches, methods, and research issues that are paramount for efficient and effective CTI sharing. We emphasize the advances in critical issues, including the intelligence of machines and human interactions, next-generation communication technologies, and the capacity to deploy, automate, orchestrate and secure CTI sharing for small and large-scale organizations.

In Fig. 14, we illustrate an overview of these future research issues in CTI sharing. A description of these future research issues is presented as follows:

5.1. Automated sharing – Role of AI

We note that the CTI is a powerful tool for developing a successful and mature proactive system for threat detection and vulnerability assessment in organizations [163]. However, there are still a number of challenges that need researchers' attention to develop a robust, automated, and expert CTI sharing system. One of the main challenges for sufficiently utilizing this powerful tool is timely sharing and consumption of CTIs [27]. Identifying IoCs to be shared and incorporating a daily flood of available CTIs into the organization's threat detection system is currently considered the bottleneck in timely consumption of CTIs [133]. The reason is that the management of CTIs adds a layer of complexity to the tasks performed by the security team of an organization [32]. We argue that AI can play an essential role in the automated management of CTIs to address the challenge of timely sharing and consumption of CTIs. Recent efforts in this direction of automatic sharing and consumption of CTIs allow stakeholders to train their threat detection systems instead of sharing IoCs collectively.

We assert that there is some trade-off when implementing existing AI-based CTI sharing approaches, e.g., a centralized CTI sharing platform is required for AI-based CTI sharing approaches [133,134]. But a decentralized CTI sharing platform provides better performance in terms of scalability, information dissemination, and accountability [27]. We further argue that in future, decentralized AI techniques, e.g., [164,165], can be beneficial for addressing automated CTI sharing and consumption in a decentralized environment. In addition, a decentralized AI is also useful for managing the data privacy concern of stakeholders in the CTI sharing landscape because they can train their threat detection systems without disclosing their private datasets [166]. Therefore, future research on AI for CTI sharing needs the creation and application of algorithms for intelligence CTI sharing processes that can wisely learn from experience and perform automated tasks commonly associated with intelligent beings.

5.2. Big data management

Fundamentally, CTI is data that contain actionable information about the latest threats and attacks collected from structured sources (a

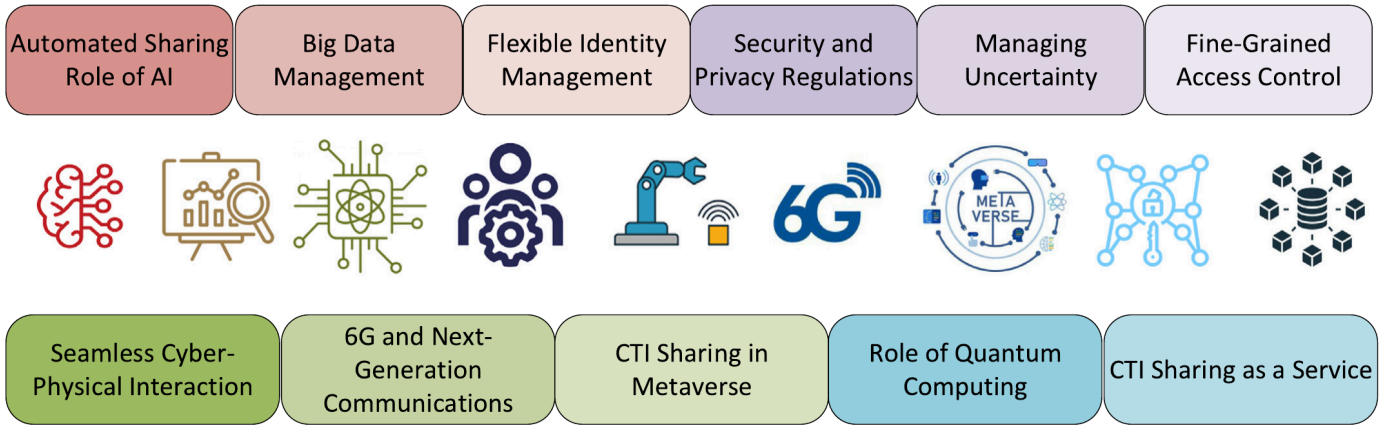

Fig. 14. A list of potential issues to be considered for future research directions in CTI sharing. Among others, we highlight the most notable future research trends of using various emerging technologies and applications that can significantly contribute to more flexible, robust, automated, and reliable CTI sharing. By focusing research efforts on leveraging these advanced methods and technologies, e.g., AI, 6G and next-generation communications, and quantum computing, it is possible to pave the way for developing innovative solutions that can address the core challenges and concerns associated with CTI sharing.

repository shared among stakeholders) or unstructured sources (e.g., social media, forums, or marketplaces) [167]. Frequently, the size of CTI data can reach up to terabytes which also need to be shared at a real-time speed to utilize this powerful tool [163] effectively. Hence, CTI shares the same 5 V features associated with Big Data, i.e., volume, variety, velocity, veracity, and volatility. Therefore, CTI data inherits the same challenges associated with Big Data, which traditional database mechanisms cannot deal with in terms of storage, processing, and analysis of CTI data. Hence, we argue that Big Data management approaches, e.g., [168,169] are beneficial for managing CTIs. There are several literature available on big data management which can be adopted in CTI sharing platforms.

In future, a sheer increase in the volume of CTI data is anticipated with the increase in the number of organizations participating in the CTI sharing platform and proliferation of heterogeneous security devices [170]. At the same time, high volatility, big volume, and high velocity of CTIs require an unprecedented amount of data storage and network resources. Towards this, we note that one possible solution to this problem is remote data analysis [171]. However, it has been seen that traditional big data management approaches do not scale well in a distributed environment. Therefore, we argue that parallel computing approaches for Big Data management approaches can be beneficial because the concept of parallelism aims to improve the speed-up, throughput, and scalability of data processing [172]. Another possible future direction is adopting distributed AI techniques (e.g., federated learning) such that only AI model parameters must be shared instead of transferring vast amounts of data in real time. Therefore, different methods and approaches are required for big data analytics to help organizations with effective data management in the future CTI sharing at scale.

5.3. Flexible identity management

Identity management can be defined as a framework of policies and technologies to ensure that the right users have appropriate access to IT resources while preserving the anonymity of users [173,174]. Identity management plays a key role in any IT infrastructure to facilitate the management of a user's digital identities for operations, e.g., authentication, authorization, and access [175]. Identity management determines the overall trustworthiness of a system in terms of performance, robustness, and privacy. In the CTI sharing context, many security problems related to identity management, e.g., impersonating malicious stakeholders may use the collected CTI to attack or compromise CTI data integrity [27]. Traditional digital identity management systems use One Time Password (OTP), Personal Identification Numbers (PINs) or digital certificates (e.g., X.509) as user identities which require credentials must be previously stored to authenticate users [173]. However, managing traditional identities in a decentralized environment are challenging for various reasons, including creating interoperable standards and governance or employing a robust trust management framework. We argue that in a CTI sharing platform, a flexible identity management system is required with the following attributes:

- *Undetectability* – to hide the user transactions, preventing the user's actions detection in a given system.
- *Unlinkability* – to hide the connection between user identities and history of transactions.
- *Confidentiality* – to enable the user's control over disseminating their attributes.

We note that blockchain-based identity management systems can be beneficial for managing identities in a distributed or a decentralized CTI sharing platform [176]. Blockchain-based identity management systems can also provide high-efficiency undetectability, unlinkability, and confidentiality to a higher extent. Other possible candidates for identity management include zero-knowledge [177] or federated identity management [178]. For the future, we find no dominating approach among the topics mentioned earlier that would be the primary research priority. However, we foresee some challenges to be addressed by future research on identity management in CTI platforms considering sensitive data management. In our opinion, other techniques and evaluation metrics can be beneficial for reliability evaluation in identity management, for example, risk assessment for devices, device profiles, and organizations. It is important to increase the level of trust for stakeholders, to consider the risk of access by certain devices (e.g., tablets or mobile phones) or access methods (e.g., private or public) to increase a stakeholder's level of trust in accessing resources or spreading attributes. Therefore, in the future novel techniques and methods are needed for CTI sharing to improve organizational security, customer experiences, and insights for reduced risk in data sharing.

5.4. Security and privacy regulations

In any information sharing or collaboration system, the security and privacy of data are always one of the primary concerns for system administrators. Security and privacy concerns are further escalated in the context of CTI sharing because CTI is not like normal data but contains actionable information that can be used to exploit unremedied vulnerabilities by a malicious user [179]. Hence, if a malicious actor gets access to CTI data, it can completely undermine the benefits of CTI sharing. At the same time, CTI sharing stakeholders are reluctant

to share information about breaches following the fear that it could damage their reputation [27]. Therefore, we argue that addressing the security and privacy concerns in the landscape of CTI sharing regulations requires a combination of technical and legislative approaches to secure CTIs and gain the trust of CTI sharing stakeholders [180].

From the technical perspective, there have been a several efforts over the past decade by technical standards development organizations, e.g., the Internet Engineering Task Force (IETF), the International Telecommunications Union Telecommunication Standardization Sector (ITU-T), to standardize technologies for CTI sharing [180]. Moreover, several technical approaches can be found in the literature to ensure the security and privacy of data in a CTI sharing system to gain the trust of stakeholders [27]. Anonymous sharing is one of the approaches to achieving privacy and anonymity. However, the anonymity of shared CTI content and metadata has to be established to ensure the privacy of stakeholders. Blockchain is a most promising tool to ensure the anonymity of CTI-sharing nodes/stakeholders. At the same time, several approaches can be adopted to ensure privacy by anonymizing CTI metadata, e.g., k-anonymity, l-diversity, or pseudonymization [181]. We argue that homomorphic encryption can be helpful in future CTI sharing for privacy preservation because stakeholders can utilize the shared data without decryption [182]. Furthermore, federated machine learning is another approach where stakeholders can collaboratively train their threat detection system (typically based on decentralized data) without sharing actual data [133,183].

We foresee challenges to be addressed in future research from the legislative perspective. We argue that legal constraints may impede stakeholders from sharing CTIs globally. Although the access to open-source CTI sharing platforms is not restricted by the geographical location of a stakeholder [184]. However, there are different laws and regulations in each region for sharing data that may contain personal or private information [185]. Therefore, disputes may arise based on the purpose of collecting data, the original location of collection, the destination location for transferring and disclosing, and the conditions in which data is transferred [180,185]. For example, an IP address in the United States is not considered personal information based on a case ruling [180]. On the other hand, in Germany, the court decided that IP address is personal information in some cases, so it must be protected [27]. Hence, managing global CTI sharing under varying regulations defined by each country is challenging. Currently, European Union (EU) General Data Protection Regulation (GDPR) is the most comprehensive legal framework for sharing data among the member states of the EU [186]. Many other countries, e.g., Canada, Australia, and New Zealand, have legislation based on the EU data protection model. However, there is not one legal framework for data sharing that applies to all these countries. Therefore, to exchange CTIs globally, we argue that a comprehensive legal framework is required which defines CTI sharing regulations among different states/countries domestically, and cross-border should be considered to foster CTI sharing among international stakeholders.

5.5. Managing uncertainty

With the increased automation based on IoT, Industry 4.0 and the inclusion of AI in cyber–physical systems, there is a high chance of uncertainty present in the system due to the information occurring from unreliable sources, experimental errors, or even equipment faults. The underlying uncertainty may reduce utility and increases automation risks to a greater extent for CTI sharing due to the sensitive nature of data. Commonly uncertainty can be classified into two forms. For instance, the uncertainty arises from noise or randomness (called *aleatory* uncertainty), and the uncertainty stems from a lack of knowledge in systems, both data and model (called *epistemic* uncertainty) [187].

Managing uncertainty in CTI sharing is significant for aggregated, transformed, analyzed, interpreted, or enriched data quality with a high degree of confidence. For instance, smart device malfunctions (due to noise in the sensors or attacks due to the unauthorized control of the devices) can produce uncertainty and generate incorrect data. This incorrect data can mislead CTI sharing. Further, this uncertainty in data may deceive the actual CTI information for accurate threat detection [188]. In collaborative CTI sharing, various types of uncertainty present in the data may impact the overall quality of CTI to a greater extent. It is possible to provide decision-making with a high degree of confidence if the results of a CTI sharing procedure are known (e.g., in a specific state). Similarly, the level of confidence decreases when the uncertainty level of the CTI sharing process outcome increases. The certain and uncertain states represent the CTI sharing degree of uncertainty (i.e., the data quality and the data effectiveness), and the confidence value can be used to measure the performance of a system [189].

We argue that the future CTI sharing must consider the uncertainty issue from the confidence of outcomes that determine the quality of information (while making a decision) and more profoundly evaluate the impact of uncertainty based on *security*, *privacy*, and *trust* attributes in a typical network system participating in CTI sharing [190].

Future CTI sharing must address the critical issue of representing uncertainty and measure the impact of uncertainty associated with a particular CTI sharing. To address uncertainty in CTI sharing, machine learning models (e.g., [191,192]), blockchain technology (e.g., [193, 194], and [195]), and techniques for trusted data sharing models (e.g., [191,196]) are promising. Machine learning models would help to estimate the presence of different types of uncertainty, blockchain can verify the digital data agreed by multiple stakeholders, and finally, data appropriate trust models allow for selection between two or more data sources based on the level of uncertainty present in those sources.

5.6. Fine-grained access control

Access control is a security mechanism that ensures the authentication of an entity and the corresponding access rights through authorization to gain access to a particular resource by the same entity [96]. That is, access control validates an entity's claim on who they are and if they have the appropriate access to a specific resource. The rapid adaptation of emerging technologies (e.g., IoT, AI, etc.) and heterogeneous network connectivity have introduced profound confidentiality, availability, and integrity challenges that impact access control for accurate authentication and authorization [197]. In CTI sharing, appropriate access control is substantial to protect sensitive information from unwanted users.

On the one hand, the characteristics of IoT [198], including the high mobility of devices, potentially large-scale systems with dynamic network topology, and wireless communication mediums, create challenges to developing a secure, robust, privacy-preserving, and scalable access control mechanism for CTI sharing. On the other hand, low-powered devices with limited storage and memory capacity and restricted processing power are often unable to support the implementation of traditional heavy-weight access control mechanisms for CTI sharing [199]. Present access control mechanisms, e.g., Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) for CTI sharing are not prepared to fully integrate with the different needs of CTI sharing. For example, RBAC manages user to role mapping for every access to a resource that is not scalable for a large-scale CTI sharing environment. ABAC does not provide a light-weight mechanism for verifying the number of policies to access resources for resource-constrained devices participating in CTI sharing [200].

Moreover, these access control mechanisms (i.e., RBAC and ABAC) do not adequately cover its dynamic and autonomous communications characteristics, which are hugely important in the CTI sharing context. The primary concerns are: (i) to design a light-weight access control mechanism for CTI sharing, in particular for resource-constrained IoT devices that address the uncertainty present in such highly scalable and dynamic systems, (ii) to provide a decentralized intelligence to the edge

IoT devices that is highly efficient for CTI sharing access authorization, (iii) to cluster together various IoT systems that can speed up the access control process and optimize the network's maintenance with meta-heuristics for CTI sharing, and (iv) to develop access control techniques for CTI sharing which are service-oriented and event-driven and are able to manage high volumes of data [201,202].

In the future, to address the above-mentioned issues in CTI sharing, among other, distributed capability-based access control (e.g., [203, 204], and [205]) is beneficial. A capability can be seen as a token of authority that contains the access rights for performing a specific task. These capabilities can store the access rights, which can be validated when the edge IoT devices access CTI information. Capabilities can grant access further based on attributes (e.g., location, date, time, etc.), which may provide a more scalable and robust access control system, tailored for flexible and fine-grained CTI sharing. Further, blockchain-based access control models (e.g., [206,207], and [208]) promise to generate policies based on self-executing smart contracts which can validate an entity and its access rights in run-time. These approaches to CTI sharing would reduce the dependency on a trusted central authority to execute the evidence for authentication and calculate the trust degree to which entities should be authorized to access a resource. At the same time, automate the decision-making with fine-grained access control.

5.7. Seamless cyber-physical interaction

Cyber-Physical System (CPS) is the combination of networked digital systems and analog physical processes that operate in a monitored, controlled, and integrated way [209,210]. CPSs can provide a robust infrastructure for industrial sectors to build and communicate innovative products, smart manufacturing and business models, e.g., smart robots, intelligent buildings, implantable medical devices, just a name of few products [211].

Security of CTI sharing in such infrastructures is paramount because CPS is more likely to be vulnerable to attacks due to its characteristics, e.g., level of automation, interaction with both cyber and physical components, etc. Therefore, an appropriate technique for safe and secure CTI sharing in CPS is the fundamental driver for large-scale industrial sectors, e.g., Industry 5.0 [212]. We argue that the future CTI sharing in CPS must aim to develop the intelligent processes, secure and collaborative networking, and cutting-edge technologies required to seamlessly integrate CPS components that can operate on different spatial and temporal scales across industrial domains [213,214]. This would help develop a flexible and secure platform to share CTI between the organizations, especially when demands or constraints are not amenable to human intervention. Organizations must have a platform that helps share CTI, sensitive business data, and demographic information for seamless interaction between consumers and producers. Towards this, proposal, e.g., [215], could be beneficial to employ. It confirms the data safety and privacy while sharing information in CPS. Another proposal, e.g., [216], can be applied for sharing CTI in CPS that provides an approach to represent and share incident knowledge in different CPSs to enhance security and improve forensic readiness in CPSs. This approach captures the occurring incident patterns in different CPSs. It then allows the various systems to instantiate the incident pattern for assessing the possibility of re-occurrence of the incidents. The approach provides two meta-models for representing (i) incident patterns and (ii) the CPSs themselves. This approach can be used as a basic approach for exchanging CTI in the future, particularly between CPS-connected devices.

Furthermore, we envision that another significant aspect of CTI sharing in CPS in future is the integration of a *digital twin* that connects physical systems to their representations in the virtual world. This connection allows the integration of CPS and technologies, e.g., IoT and other multi-agent systems, to facilitate the development of different processes and industries, including security, smart city, smart manufacturing, agriculture, education, and energy sectors [211,217–219]. For instance, proposal [220] can be used for CTI sharing in CPS that uses a transfer learning technique based on machine learning models. Another proposal, e.g., [221] presents a data exchange model in digital twin that can be used for CTI exchange in future. The proposed model is based on 'AutomationML' (AML) for data exchange between systems connected with the digital twin, including industrial equipment, building automation devices, and medical equipment. The model provides a generic communication mechanism for the connected devices, potentially applicable for future CTI sharing at scale.

5.8. 6G and next-generation communications

It is predicted that by 2030, 6G (sixth-generation wireless communications) will seamlessly integrate the digital and physical world with advanced communication systems, efficient services, and faster signal processing [222]. The 6G uses a higher frequency compared to 5G and is expected to provide increased sustainability, more capacity, and considerably lower latency in communication networks [223]. The speed of 6G networks is anticipated to be a hundred times faster than 5G networks, including enhanced reliability and a broader network coverage [222].

Low latency and high reliability features of 6G networks can address the challenges of communication that are related to lower bandwidth by improving network performance metrics, including: (i) mobility, (ii) throughput, and (iii) energy and spectrum efficiency [224,225]. Therefore, the 6G networks would be able to enhance some current services, e.g., data sharing, intelligence sharing of information, and computing resources and services, with significantly better throughput and higher data rates. To integrate new generation 6G communication technology in CTI sharing, future research must focus on conceptualizing 6G communication systems and standardizing the requirements for the CTI sharing with new CTI sharing models and protocols [223].

It is expected that 6G will shift the network from software and cloud towards intelligence (more likely based on distributed AI) and will revolutionize the wireless networks from 'connected things' to 'connected intelligence' [226]. AI will be the foundation of 6G, and this will make all the components of 6G to be natively and ubiquitously intelligent [222]. Furthermore, this feature will support AI-related services for enhancing CTI sharing systems to take intelligent sharing decisions autonomously to a higher extent using higher frequency bands and agile and cloud-based networking [227].

The integration of 6G and blockchain is another potential solution to overcome the scalability issue of blockchain networks and improve distributed and decentralized CTI sharing. This integration, on another side, will enable the deployment of the blockchain platforms for a large-scale CTI sharing [228]. Furthermore, deploying a decentralized blockchain-based on 6G can address the current IoT requirements of data-intensive applications [229]. Thus, the integration of 6G and blockchain can also address the challenge of combining several data formats distributed across different locations, which helps in blockchain-based approaches for CTI sharing. For example, performance analysis results of 'defense-chain' [114] mechanism for CTI sharing proves that it is two times slower in detection and mitigation of cyber attacks compared to other solutions, as it operates in multiple stages like policy update, attack traffic redirection, etc. Implementing the 'defense-chain' model in IoT with 6G can provide low latency by supporting THz communication at sub-millimeter bands for every component in each stage and increasing their computing power [230].

Edge intelligence powered by AI is predicted to be one of the main enabling elements of the 6G network to support network performance, functions, and services. Deploying edge intelligence in 6G contributes to new ultra-low-latency services performance improvement and traffic optimization [231]. Thus, running services on edge computing can enhance significantly with the help of 6G. Furthermore, it can potentially be an essential advancement for CTI sharing approaches based on edge

intelligence. Integration of 6G and AI will allow edge computational infrastructure to recognize (using the empowered processing ability) the best place for computing to occur, including CTI processing and analysis, sharing, and storage [232].

5.9. CTI sharing in the metaverse

We envision that CTI sharing can bring benefits to the metaverse cyber defense. Metaverse is the integrated network of 3D virtual worlds [233]. By merging digital virtuality with physical reality, the metaverse creates the post-reality world consisting of a perpetual and persistent multiuser environment [234]. Integration of physical and digital reality in the metaverse is facilitated through the convergence between the Internet and web technologies and extended reality (XR) [235]. Further, digital twin, virtual reality (VR), augmented reality (AR), 6G, wearable sensors and brain–computer interface, AI, blockchain, and non-fungible token (NFT) are some of the key technologies that play important roles in metaverse [236].

However, the development of the metaverse can create a variety of security threats and challenges. Metaverse security challenges are predominantly related to the privacy and security of its users. User profiling, humans in and out of the loop, and integrity and authentication in the metaverse are some reasons for the privacy and security challenges [237,238]. However, the metaverse incorporates diverse technologies in physical and digital reality as its foundation. Therefore, the metaverse may also inherit their underlying weaknesses and vulnerabilities. For example, hackers may use the vulnerabilities of systems and software in the integrated metaverse to exploit the physical layer device (e.g., wearable devices), which is compromised as an entry point to invade critical infrastructures. Moreover, because various technologies are intertwined, the impacts of existing threats can be increased and become more severe in the metaverse [239].

The existing defensive mechanisms can be empowered to be effective in the metaverse. For instance, identity management where the digital identity systems are built on self-sovereign identity (SSI) will be dominantly used in metaverse [239,240]. Moreover, situational awareness will continue to be an effective mechanism for threat monitoring in the metaverse by supporting early warning in the domains and subdomains [239,241]. As a result, in the future, CTI sharing will be an essential proactive defense technique in metaverse by providing situational awareness in such large-scale convoluted systems. We note that future CTI sharing models must be adopted with the metaverse requirements and the threat landscape. Moreover, the metaverse will require massive network bandwidth because it generates a large amount of data, including the sensor's metadata, social activities in virtual space, and high-resolution video streams. As a result, 6G technology will be helpful to address the required scalability of metaverse efficiently, and the data communications in metaverse will rely on the (P2P) communication techniques. From a data storage point of view, blockchain-based CTI sharing can potentially be more successful and generate trust without requiring trusted third parties. The future CTI sharing models in the metaverse must adopt various approaches to the metaverse and its enabling technologies, for example, the vulnerability details of the NFT, which involves the physical world when users purchase and trade assets [242]. As the Metaverse will likely create a more challenging threat landscape, efforts to facilitate CTI sharing between Metaverse-based organizations should be considered.

5.10. Role of quantum computing

Quantum computing is an emerging technology that has the potential to provide a new era in the classical computing paradigm. This technology will affect different areas, e.g., communication, data storage, and security. Subsequently, quantum Internet and quantum machine learning are developed to provide unprecedented capabilities which are impossible in classical computing [243,244]. However, quantum will cause new security threats as well. In the cybersecurity area, quantum computing will jeopardize many security protocols. In addition, malicious actors can create a method to use for malicious purposes. Therefore, quantum computing introduces two significant security challenges: the broken classical security methods and the new quantum attack surface.

The ability of quantum computing to process vast datasets and solve complex algorithms exponentially faster than classical computers could revolutionize cryptography and data encryption, ensuring robust security for shared CTI. Quantum encryption methods provide unbreakable security for sensitive information, while quantum networks enable secure and efficient CTI sharing among trusted parties. As quantum computing continue to advance, they may become essential tools for enhancing the scalability, efficiency, and security of CTI sharing platforms in the future cybersecurity landscape. We argue that the automation of generation and sharing of CTI will be needed to leverage the strengths of quantum computing to create novel approaches. However, analyzing the big data in quantum computing, generation of CTI, and sharing CTI over quantum-based communication links will be challenging due to the transition from cryptography to post-quantum algorithms. We note that in future CTI sharing, AI can play a significant role. AI would also play a vital role in quantum CTI. It can help to automatically collect, analyze and share CTI across various global networks. This helps to combat future advanced quantum attacks. Quantum AI and machine learning will be able to deal with a large amount of information in real-time in quantum networks, analyze raw data and provide quick and reliable CTI [245].

5.11. CTI sharing as a service

We argue that in CTI sharing, organizations may need to provide a wide range of services (in terms of sharing CTI data) to be delivered on-demand to other organizations over the Internet. Therefore, the CTI sharing services must be designed to provide robust infrastructure, platforms, and affordable access to applications and resources in terms of a ready-to-use application platform. In CTI sharing, this service refers to a model that delivers a CTI feed for organizations. The feed may be selected from the collection or discovered information as part of normal business operations.

There are different platforms available on the market for CTI sharing, e.g., zveloCTI [246], and Anomali ThreatStream [247], that provide similar types of content regarding CTI, for example delivering actionable CTI on threat types (e.g., phishing) or transforming relevant, actionable threat intelligence for security teams. However, depending on the operational environment and the usage intention, these products may differ in the application service model. In this model, the organization is the CTI source and can verify the content, accuracy and timeliness of CTI [248]. A potential future direction for CTI sharing 'as a service' can provide a model for an organization to send its CTI to a diverse and large number of CTI consumers. For example, to take CTI from multiple sources and contextualize it to be used by a particular CTI consumer, and to take CTI from multiple CTI sources, normalize it and share it with a diverse and large number of CTI consumers [248].

6. Conclusion

Cyber Threat Intelligence (CTI) sharing is a promising information exchange strategy attracting significant attention and support from organizations, cyber defenders and security professionals to help drive collective action against cyber attacks. However, the CTI sharing landscape still requires further research and exploration to examine CTI sharing challenges and the organization's requirement for exchanging CTI seamlessly. This paper comprehensively surveyed the current approaches and future research directions for CTI sharing using the most representative references from industry, academia, and standardization

bodies. First, we thoroughly explained, CTI, CTI sharing and its fundamentals, including CTI and related requirements for CTI sharing. We also presented the classifications of key CTI-sharing architectures that added a new dimension to how CTI producers and consumers can communicate and collaborate. Next, we identified a comprehensive list of CTI-sharing challenges that must be addressed for effective management and sharing of CTI data. We examined the available approaches to CTI sharing based on various techniques, e.g., blockchain, incentives, machine learning, etc. We noted that emerging technologies have become widespread to address CTI sharing. For example, the use of blockchain for CTI sharing has recently received increased interest due to the inherent features of blockchain, e.g., auditability, transparency, etc. We further critically examine how the various available proposals address the challenges for CTI sharing that we listed in our paper. Finally, we suggested the potential future directions for CTI sharing to address advances in the industrial internet through increased network agility, integrated artificial intelligence, and the capacity to deploy, automate, orchestrate and secure diverse CTI sharing approaches. This survey can guide future innovation and the practical deployment of CTI sharing for many industrial applications.

CRediT authorship contribution statement

Poopak Alaeifar: Investigation, Methodology, Resources, Writing – original draft. **Shantanu Pal:** Conceptualization, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Supervision, Writing – review & editing. **Zahra Jadidi:** Data curation, Investigation, Methodology, Project administration, Supervision, Writing – review & editing. **Mukhtar Hussain:** Writing – review & editing, Resources, Validation. **Ernest Foo:** Project administration, Resources, Writing – review & editing.

Declaration of competing interest

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

Data availability

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

References

[1] Aldauiji F, Batarfi O, Bayousif M. Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. IEEE Access 2022.

[2] statista. Statista-report. 2024, https://www.statista.com/topics/4136/ransomware/#topicOverview. [Online Accessed 14 March 2024].

[3] Lutf M. Threat intelligence sharing: a survey. J Appl Sci Comput 2018;8(11):1811–5.

[4] Zrahia A. Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views. J Cybersecur 2018;4(1):tyy008.

[5] Borges Amaro LJ, Percilio Azevedo BW, Lopes de Mendonca FL, Giozza WF, Albuquerque Rd, García Villalba LJ. Methodological framework to collect, process, analyze and visualize cyber threat intelligence data. Appl Sci 2022;12(3):1205.

[6] Gandotra V, Singhal A, Bedi P. Threat-oriented security framework: A proactive approach in threat management. Proc Technol 2012;4:487–94.

[7] Dasgupta D, Akhtar Z, Sen S. Machine learning in cybersecurity: a comprehensive survey. J Def Model Simul 2022;19(1):57–106.

[8] de Melo e Silva A, Costa Gondim JJ, de Oliveira Albuquerque R, García Villalba LJ. A methodology to evaluate standards and platforms within cyber threat intelligence. Future Internet 2020;12(6):108.

[9] Menges F, Putz B, Pernul G. DEALER: decentralized incentives for threat intelligence reporting and exchange. Int J Inf Secur 2021;20(5):741–61.

[10] Pala A, Zhuang J. Information sharing in cybersecurity: A review. Decis Anal 2019;16(3):172–96.

[11] Sigholm J, Bang M. Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats. In: 2013 European intelligence and security informatics conference. IEEE; 2013, p. 166–71.

[12] Schlette D, Caselli M, Pernul G. A comparative study on cyber threat intelligence: the security incident response perspective. IEEE Commun Surv Tutor 2021;23(4):2525–56.

[13] Abu MS, Selamat SR, Ariffin A, Yusof R. Cyber threat intelligence–issue and challenges. Indones J Electr Eng Comput Sci 2018;10(1):371–9.

[14] Fortino G, Savaglio C, Spezzano G, Zhou M. Internet of things as system of systems: A review of methodologies, frameworks, platforms, and tools. IEEE Trans Syst Man Cybern: Syst 2020;51(1):223–36.

[15] Johnson C, Badger L, Waltermire D, Snyder J, Skorupka C, et al. Guide to cyber threat information sharing. NIST Spec Publ 2016;800(150).

[16] Ramsdale A, Shiaeles S, Kolokotronis N. A comparative analysis of cyber-threat intelligence sources, formats and languages. Electronics 2020;9(5):824.

[17] Nweke LO, Wolthusen S. Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection. In: 2020 12th international conference on cyber conflict (cyCon). Vol. 1300, IEEE; 2020, p. 63–78.

[18] Schaberreiter T, Roning J, Quirchmayr G, Kupfersberger V, Wills C, Bregonzio M, Koumpis A, Sales JE, Vasiliu L, Gammelgaard K, et al. A cybersecurity situational awareness and information-sharing solution for local public administrations based on advanced big data analysis: the CS-AWARE project. Chall Cybersecur Priv–Eur Res Landsc 2019;149–80.

[19] Mavroeidis V. Towards automated threat-informed cyberspace defense. 2021.

[20] Pal S, Hitchens M, Varadharajan V. Access control for Internet of Things—Enabled assistive technologies: An architecture, challenges and requirements. In: Assistive technology for the elderly. Elsevier; 2020, p. 1–43.

[21] Griffioen H, Booij T, Doerr C. Quality evaluation of cyber threat intelligence feeds. In: International conference on applied cryptography and network security. Springer; 2020, p. 277–96.

[22] Zibak A, Simpson A. Cyber threat information sharing: Perceived benefits and barriers. In: Proceedings of the 14th international conference on availability, reliability and security. 2019, p. 1–9.

[23] Oosthoek K, Doerr C. Cyber threat intelligence: A product without a process? Int J Intell CounterIntell 2021;34(2):300–15.

[24] Arafune M, Rajalakshmi S, Jaldon L, Jadidi Z, Pal S, Foo E, Venkatachalam N. Design and development of automated threat hunting in industrial control systems. In: 2022 IEEE international conference on pervasive computing and communications workshops and other affiliated events (perCom workshops). IEEE; 2022, p. 618–23.

[25] Czekster RM, Metere R, Morisset C. CyberaCTIve: a STIX-based tool for cyber threat intelligence in complex models. 2022, arXiv preprint arXiv:2204.03676.

[26] Skopik F, Settanni G, Fiedler R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Comput Secur 2016;60:154–76.

[27] Wagner TD, Mahbub K, Palomar E, Abdallah AE. Cyber threat intelligence sharing: Survey and research directions. Comput Secur 2019;87:101589.

[28] Du L, Fan Y, Zhang L, Wang L, Sun T. A summary of the development of cyber security threat intelligence sharing. Int J Digit Crime Forensics (IJDCF) 2020;12(4):54–67.

[29] Sukhabogi S, et al. A theoretical review on the importance of Threat Intelligence Sharing & the challenges intricated. Turk J Comput Math Educ (TURCOMAT) 2021;12(3):3950–6.

[30] Xiaohui Z, Xianghua M. A reputation-based approach using consortium blockchain for cyber threat intelligence sharing. 2021, arXiv preprint arXiv:2107.06662.

[31] McMillan R. Definition: threat intelligence. 2013, Gartner.com.

[32] Montasari R, Carroll F, Macdonald S, Jahankhani H, Hosseinian-Far A, Daneshkhah A. Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence. In: Digital forensic investigation of internet of things (ioT) devices. Springer; 2021, p. 47–64.

[33] Pawlinski P, Jaroszewski P, Kijewski P, Siewierski L, Jacewicz P, Zielony P, Zuber R. Actionable information for security incident response. Heraklion, Greece: European Union Agency for Network and Information Security; 2014.

[34] Doerr C. Cyber threat intelligence standards–a high level overview. TU Delft CTI Labs; 2018.

[35] Crowdstrike-CTI. 2022, https://crowdstrike.com/cybersecurity-101/threat-intelligence/. [Online Accessed 31 May 2022].

[36] Kasperski-CTI. 2022, https://kaspersky.com/resource-center/definitions/threat-intelligence/. [Online Accessed 20 March 2022].

[37] Samtani S, Li W, Benjamin V, Chen H. Informing cyber threat intelligence through dark Web situational awareness: The AZSecure hacker assets portal. Digit. Threats: Res. Pract. (DTRAP) 2021;2(4):1–10.

[38] Bou-Harb E, Debbabi M, Assi C. Cyber scanning: a comprehensive survey. Ieee Commun. Surv. Tutor. 2013;16(3):1496–519.

[39] Pal S, Jadidi Z. Analysis of security issues and countermeasures for the industrial internet of things. Appl Sci 2021;11(20):9393.

[40] Farnham G, Leune K. Tools and standards for cyber threat intelligence projects. SANS Institute; 2013.

[41] van Haastrecht M, Golpur G, Tzismadia G, Kab R, Priboi C, David D, Răcătăian A, Baumgartner L, Fricker S, Ruiz JF, et al. A shared cyber threat intelligence solution for smes. Electronics 2021;10(23):2913.

[42] Sakellariou G, Fouliras P, Mavridis I, Sarigiannidis P. A reference model for cyber threat intelligence (CTI) systems. Electronics 2022;11(9):1401.
[43] Cybrary. 2022, https://www.cybrary.it/blog/introduction-to-cyber-threat-intelligence/. [Online Accessed 28 May 2022].
[44] Schlette D. Cyber threat intelligence sharing. 2021.
[45] Parmar M, Domingo A. On the use of cyber threat intelligence (CTI) in support of developing the commander's understanding of the adversary. In: MILCOM 2019-2019 IEEE military communications conference. MILCOM, IEEE; 2019, p. 1–6.
[46] Shackleford D. Cyber threat intelligence uses, successes and failures: The sans 2017 cti survey. SANS Institute; 2017.
[47] Shackleford D. CTI in security operations: SANS 2018 cyber threat intelligence survey. SANS Institute; 2018.
[48] Brown R, Lee RM. The evolution of cyber threat intelligence (CTI): 2019 SANS CTI survey. SANS Institute; 2019, Available online: https://www.sans.org/white-papers/38790/. [Accessed on 12 July 2021].
[49] Brown R, Lee RM. 2021 Sans cyber threat intelligence (cti) survey. Tech. rep, SANS Institute; 2021.
[50] TAXII sharing models. 2022, https://taxiiproject.github.io/about/. [Online Accessed 05 March 2022].
[51] van Steen M, Tanenbaum AS. A brief introduction to distributed systems. Computing 2016;98(10):967–1009.
[52] Xi Z. The comparison of decentralized and centralized structure of network communication in different application fields. In: Advances in economics, business and management research, international conference on management science and industrial economy. Vol. 118, 2020.
[53] Ravichandran C, Xavier JL. A survey of data sharing and security issues in P2P networks. Adv Natl Appl Sci 2017;11(7):329–35.
[54] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput Secur 2018;72:212–33.
[55] Sauerwein C, Sillaber C, Mussmann A, Breu R. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. In: Proceedings of the 13th international conference on wirtschaftsinformatik. 2017, p. 837–51.
[56] Connolly J, Davidson M, Schmidt C. The trusted automated exchange of indicator information (taxii). The MITRE Corporation; 2014, p. 1–20.
[57] OpenTPX. 2022, https://www.threat-intelligence.eu/standards/. [Online Accessed 14 May2022].
[58] Tosh DK. Market based models for cybersecurity information exchange (CYBEX). University of Nevada, Reno; 2016.
[59] VERIS. 2022, http://veriscommunity.net. [Online Accessed 14 May 2022].
[60] Takahashi T, Landfield K, Kadobayashi Y. An incident object description exchange format (iodef) extension for structured cybersecurity information. Tech. rep., 2014.
[61] Barnum S. Standardizing cyber threat intelligence information with the structured threat information expression (stix). Vol. 11, Mitre Corporation; 2012, p. 1–22.
[62] TLP. 2022, https://www.incibe-cert.es/en/tlp. [Online Accessed 14 May 2022].
[63] CIF. 2022, https://github-wiki-see.page/m/csirtgadgets/massive-octo-spice/wiki/What-is-the-Collective-Intelligence-Framework. [Online Accessed 10 May 2022].
[64] Moriarty K. Real-time Inter-network defense (RID). Tech. rep., 2012.
[65] OTX. 2022, https://cybersecurity.att.com/open-threat-exchange. [Online Accessed 10 May 2022].
[66] IBM CTI sharing. 2022, https://exchange.xforce.ibmcloud.com/. [Online Accessed 13 May 2022].
[67] AT&T Intellectual Property. USm-anywhere. 2022, https://cdn-cybersecurity.att.com/docs/product-briefs/DS-USM-Anywhere.pdf. [Online Accessed 20-March-2022].
[68] CrowdStrike Products. Falcon. 2022, https://www.crowdstrike.com/products/threat-intelligence/falcon-x-automated-intelligence. [Online Accessed 13 May 2022].
[69] Open CTI. 2022, https://www.opencti.io/en/. [Online Accessed 12 May 2022].
[70] Platforms T. Threat-connect. 2022, https://threatconnect.com. [Online Accessed 12 March 2022].
[71] Brightpoint sentinel. 2022, www.brightpointsecurity.com. [Online Accessed 02 May 2022].
[72] Splunk. 2022, https://www.splunk.com/en_us/software/enterprise-security.html. [Online Accessed 15-March-2022].
[73] Ciscotalos. 2022, https://www.talosintelligence.com/. [Online Accessed 14-May-2022].
[74] Jesus V, Bains B, Chang V. Sharing is caring: Hurdles and prospects of open, crowd-sourced cyber threat intelligence. IEEE Trans Eng Manage 2023;1–20.
[75] Garrido-Pelaz R, González-Manzano L, Pastrana S. Shall we collaborate? A model to analyse the benefits of information sharing. In: Proceedings of the 2016 ACM on workshop on information sharing and collaborative security. 2016, p. 15–24.
[76] Navarrete C, Gil-Garcia JR, Mellouli S, Pardo TA, Scholl J. Multinational e-government collaboration, information sharing, and interoperability: An integrative model. In: 2010 43rd hawaii international conference on system sciences. IEEE; 2010, p. 1–10.
[77] Cha J, Singh SK, Pan Y, Park JH. Blockchain-based cyber threat intelligence system architecture for sustainable computing. Sustainability 2020;12(16):6401.
[78] Tran-Gia P, Binzenhöfer A. On the stochastic scalability of information sharing platforms. In: Distributed cooperative laboratories: networking, instrumentation, and measurements. Springer; 2006, p. 11–27.
[79] Maqsood T, Khalid O, Irfan R, Madani SA, Khan SU. Scalability issues in online social networks. ACM Comput Surv 2016;49(2):1–42.
[80] Wagner TD, Palomar E, Mahbub K, Abdallah AE. Towards an anonymity supported platform for shared cyber threat intelligence. In: International conference on risks and security of internet and systems. Springer; 2017, p. 175–83.
[81] Sauerwein C, Sillaber C, Mussmann A, Breu R. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. 2017.
[82] Mesenbourg TL, Potok NA, Jackson AA, Vitrano FA, Johnson TA, Jost SJ, Little R, Hackbarth DE, McGrath BE, Bostic Jr WG. US Census Bureau statistical quality standards. US Census Bureau; 2013.
[83] Pawliński P. ENISA publication. 2022, https://www.enisa.europa.eu/publications/actionable-information-for-security/at_download/fullReport. [Online Accessed 20 April 2022].
[84] Luiijf E, Klaver M. On the sharing of cyber security information. In: International conference on critical infrastructure protection. Springer; 2015, p. 29–46.
[85] Gong S, Lee C. Blocis: blockchain-based cyber threat intelligence sharing framework for sybil-resistance. Electronics 2020;9(3):521.
[86] Agrawal R, Cheung A, Kailing K, Schonauer S. Towards traceability across sovereign, distributed RFID databases. In: 2006 10th international database engineering and applications symposium. IDEAS'06, IEEE; 2006, p. 174–84.
[87] Solarwinds it glossary. 2022, https://www.solarwinds.com/resources/it-glossary/network-bandwidth. [Online Accessed 10 April 2022].
[88] Wagner TD, Palomar E, Mahbub K, Abdallah AE. A novel trust taxonomy for shared cyber threat intelligence. Secur Commun Netw 2018;2018.
[89] Wu Y, Qiao Y, Ye Y, Lee B. Towards improved trust in threat intelligence sharing using blockchain and trusted computing. In: 2019 sixth international conference on internet of things: systems, management and security. IOTSMS, IEEE; 2019, p. 474–81.
[90] Sadique F, Bakhshaliyev K, Springer J, Sengupta S. A system architecture of cybersecurity information exchange with privacy (cybex-p). In: 2019 IEEE 9th annual computing and communication workshop and conference. CCWC, IEEE; 2019, p. 0493–8.
[91] Fisk G, Ardi C, Pickett N, Heidemann J, Fisk M, Papadopoulos C. Privacy principles for sharing cyber security data. In: 2015 IEEE security and privacy workshops. IEEE; 2015, p. 193–7.
[92] Götz M, Field JG, Murphy KR. Data sharing and data integrity. In: Data, methods and theory in the organizational sciences. Routledge; 2022, p. 49–72.
[93] Gal MS, Rubinfeld DL. Data standardization. NYUL Rev 2019;94:737.
[94] Bromander S, Swimmer M, Muller LP, Jøsang A, Eian M, Skjøtskift G, Borg F. Investigating sharing of cyber threat intelligence and proposing a new data model for enabling automation in knowledge representation and exchange. Digit Threats: Res Pract (DTRAP) 2021;3(1):1–22.
[95] Kowalczyk S, Shankar K. Data sharing in the sciences. Annu Rev. Inf Sci Technol 2011;45(1):247–94.
[96] Pal S. Internet of Things and access control: Sensing, monitoring and controlling access in IoT-enabled healthcare systems, vol. 37, Springer Nature; 2021.
[97] Fabrocini F. Intelligent process automation of industries using artificial intelligence and machine learning. J Comput Natl Sci 2021;45–56.
[98] Rantos K, Spyros A, Papanikolaou A, Kritsas A, Ilioudis C, Katos V. Interoperability challenges in the cybersecurity information sharing ecosystem. Computers 2020;9(1):18.
[99] Pal S, Hitchens M, Rabehaja T, Mukhopadhyay S. Security requirements for the internet of things: A systematic approach. Sensors 2020;20(20):5897.
[100] Takacs G. Integration of CTI into security management. 2019.
[101] Wlosinski LG. Cyberthreat intelligence as a proactive extension to incident response. 2021, https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/cyberthreat-intelligence-as-a-proactive-extension-to-incident-response. [Online Accessed 25 June 2022].
[102] Diaz C, Seys S, Claessens J, Preneel B. Towards measuring anonymity. In: International workshop on privacy enhancing technologies. Springer; 2002, p. 54–68.
[103] Li Z, He Y, Yu H, Kang J, Li X, Xu Z, Niyato D. Data heterogeneity-robust federated learning via group client selection in industrial IoT. IEEE Internet Things J 2022.
[104] Homoliak I, Venugopalan S, Reijsbergen D, Hum Q, Schumi R, Szalachowski P. The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. IEEE Commun Surv Tutor 2020;23(1):341–90.
[105] Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview. 2019, arXiv preprint arXiv:1906.11078.
[106] Badsha S, Vakilinia I, Sengupta S. Blocynfo-share: Blockchain based cybersecurity information sharing with fine grained access control. In: 2020 10th annual computing and communication workshop and conference. CCWC, IEEE; 2020, p. 0317–23.

[107] Sarmah SS. Understanding blockchain technology. Comput Sci Eng 2018;8(2):23–9.
[108] Dorri A, Kanhere SS, Jurdak R. Blockchain in internet of things: challenges and solutions. 2016, arXiv preprint arXiv:1608.05187.
[109] Pal S, Hill A, Rabehaja T, Hitchens M. VeriBlock: A blockchain-based verifiable trust management architecture with provable interactions. 2022, arXiv preprint arXiv:2206.05676.
[110] Maesa DD, Mori P, Ricci L. A blockchain based approach for the definition of auditable access control systems. Comput Secur 2019;84:93–119.
[111] Allouche Y, Tapas N, Longo F, Shabtai A, Wolfsthal Y. TRADE: Trusted anonymous data exchange: Threat sharing using blockchain technology. 2021, arXiv preprint arXiv:2103.13158.
[112] Arvindhan M, Thirunavukarasan M, Daniel A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Handb Green Comput Blockchain Technol 2022;107–18.
[113] Pal S, Jadidi Z, Putra GD, Jurdak R. A democratically anonymous and trusted architecture for CTI sharing using blockchain. In: 12th international workshop on security, privacy, trust for internet of things (ioTSPT 2022). Institute of Electrical and Electronics Engineers Inc.; 2022.
[114] Purohit S, Calyam P, Wang S, Yempalla R, Varghese J. Defensechain: Consortium blockchain for cyber threat intelligence sharing and defense. In: 2020 2nd conference on blockchain research & applications for innovative networks and services. BRAINS, IEEE; 2020, p. 112–9.
[115] Riesco R, Larriva-Novo X, Villagrá VA. Cybersecurity threat intelligence knowledge exchange based on blockchain. Telecommun Syst 2020;73(2):259–88.
[116] Hajizadeh M, Afraz N, Ruffini M, Bauschert T. Collaborative cyber attack defense in SDN networks using blockchain technology. In: 2020 6th IEEE conference on network softwarization (netSoft). IEEE; 2020, p. 487–92.
[117] Mendez Mena D, Yang B. Decentralized actionable cyber threat intelligence for networks and the Internet of Things. IoT 2020;2(1):1–16.
[118] Provatas K, Tzannetos I, Vescoukis V. Standards-based cyber threat intelligence sharing using private blockchains. In: 2023 18th conference on computer science and intelligence systems (fedCSIS). IEEE; 2023, p. 649–56.
[119] Chatziamanetoglou D, Rantos K, et al. Blockchain-based cyber threat intelligence sharing using proof-of-quality consensus. Secur Commun Netw 2023;2023.
[120] Stevens T, Ertan A, Floyd K, Pernik P. Cyber threats and NATO 2030: Horizon scanning and analysis. 2021.
[121] Chadwick DW, Fan W, Costantino G, De Lemos R, Di Cerbo F, Herwono I, Manea M, Mori P, Sajjad A, Wang X-S. A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future Gener Comput Syst 2020;102:710–22.
[122] Xuan S, Zheng L, Chung I, Wang W, Man D, Du X, Yang W, Guizani M. An incentive mechanism for data sharing based on blockchain with smart contracts. Comput Electr Eng 2020;83:106587.
[123] Naghizadeh P, Liu M. Inter-temporal incentives in security information sharing agreements. In: Workshops at the thirtieth AAAI conference on artificial intelligence. 2016.
[124] Nguyen K, Pal S, Jadidi Z, Dorri A, Jurdak R. A blockchain-enabled incentivised framework for cyber threat intelligence sharing in ICS. 2021, arXiv preprint arXiv:2112.00262.
[125] Raja MU, Javaid N. Enhanced Data Sharing Model By Using Blockchain and Incentive Mechanism.
[126] Xiong Q, Chen X. Incentive mechanism design based on repeated game theory in security information sharing. In: 2nd international conference on science and social research (ICSSR 2013). atlantis press. 2013.
[127] Jordan MI, Mitchell TM. Machine learning: Trends, perspectives, and prospects. Science 2015;349(6245):255–60.
[128] Srinivas M, Sucharitha G, Matta A, Chatterjee P, editors. Machine learning algorithms and applications. Wiley; 2021.
[129] Durrant A, Markovic M, Matthews D, May D, Enright J, Leontidis G. The role of cross-silo federated learning in facilitating data sharing in the agri-food sector. Comput Electron Agric 2022;193(April 2021):106648.
[130] Suryotrisongko H, Musashi Y, Tsuneda A, Sugitani K. Robust botnet DGA detection: Blending XAI and OSINT for cyber threat intelligence sharing. IEEE Access 2022;10:34613–24.
[131] Ghazi Y, Anwar Z, Mumtaz R, Saleem S, Tahir A. A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources. In: Proceedings - 2018 international conference on frontiers of information technology, FIT 2018. IEEE; 2019, p. 129–34.
[132] Koloveas P, Chantzios T, Alevizopoulou S, Skiadopoulos S, Tryfonopoulos C. InTIME: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. Electronics (Switzerland) 2021;10(7).
[133] Preuveneers D, Joosen W. Sharing machine learning models as indicators of compromise for cyber threat intelligence. J Cybersecur Priv 2021;1(1):140–63.
[134] Sarhan M, Layeghy S, Moustafa N, Portmann M. A cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. 2021, p. 1–15.
[135] Shahid WB, Aslam B, Abbas H, Khalid SB, Afzal H. An enhanced deep learning based framework for web attacks detection, mitigation and attacker profiling. J Netw Comput Appl 2022;198:103270.
[136] Zhao W, White G. A collaborative information sharing framework for community cyber security. In: 2012 IEEE conference on technologies for homeland security. HST, IEEE; 2012, p. 457–62.
[137] Schlette D, Böhm F, Caselli M, Pernul G. Measuring and visualizing cyber threat intelligence quality. Int J Inf Secur 2021;20(1):21–38.
[138] Vakilinia I. Collaborative analysis of cybersecurity information sharing (Ph.D. thesis), University of Nevada, Reno; 2019.
[139] Pal S. Extending mobile cloud platforms using opportunistic networks: survey, classification and open issues. J UCS 2015;21(12):1594–634.
[140] Krishnan R, Niu J, Sandhu R, Winsborough WH. Group-centric secure information-sharing models for isolated groups. ACM Trans Inf Syst Secur 2011;14(3):1–29.
[141] Arenas E. Cyber threat intelligence information sharing. Australia e. arenas@cqu. edu. au: School of Engineering and Technology CQUniversity.
[142] Zhao W, White G. Designing a formal model facilitating collaborative information sharing for community cyber security. In: 2014 47th hawaii international conference on system sciences. IEEE; 2014, p. 1987–96.
[143] "Nist cloud computing". 2022, https://www.nist.gov/publications/nist-definition-cloud-computing. [Online Accessed 09 June 2022].
[144] Marinescu DC. Cloud computing: theory and practice. Morgan Kaufmann; 2022.
[145] Barik RK, Priyadarshini R, Dubey H, Kumar V, Mankodiya K. FogLearn: leveraging fog-based machine learning for smart system big data analytics. Int J Fog Comput (IJFC) 2018;1(1):15–34.
[146] Bonomi F, Milito R, Zhu J, Addepalli S. Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on mobile cloud computing. 2012, p. 13–6.
[147] Khan WZ, Ahmed E, Hakak S, Yaqoob I, Ahmed A. Edge computing: A survey. Future Gener Comput Syst 2019;97:219–35.
[148] Chen J, Ran X. Deep learning with edge computing: A review. Proc IEEE 2019;107(8):1655–74.
[149] Capra M, Peloso R, Masera G, Ruo Roch M, Martina M. Edge computing: A survey on the hardware requirements in the internet of things world. Future Internet 2019;11(4):100.
[150] Xu D, Li T, Li Y, Su X, Tarkoma S, Jiang T, Crowcroft J, Hui P. Edge intelligence: Architectures, challenges, and applications. 2020, arXiv preprint arXiv:2003.12172.
[151] Hammoud A, Sami H, Mourad A, Otrok H, Mizouni R, Bentahar J. AI, blockchain, and vehicular edge computing for smart and secure IoV: Challenges and directions. IEEE Internet Things Mag 2020;3(2):68–73.
[152] Repetto M, Carrega A, Duzha A. A novel cyber-security framework leveraging programmable capabilities in digital services. In: ITASEC. 2020, p. 201–11.
[153] Ionita M-G, Patriciu V-V. Secure threat information exchange across the Internet of Things for cyber defense in a fog computing environment. Inform Econ 2016;20(3).
[154] Sari A. Context-aware intelligent systems for fog computing environments for cyber-threat intelligence. In: Fog computing. Springer; 2018, p. 205–25.
[155] Pop P, Zarrin B, Barzegaran M, Schulte S, Punnekkat S, Ruh J, Steiner W. The FORA fog computing platform for industrial IoT. Inf Syst 2021;98:101727.
[156] Rashid A, Chaturvedi A. Cloud computing characteristics and services: a brief review. Int J Comput Sci Eng 2019;7(2):421–6.
[157] Varshney P, Simmhan Y. Characterizing application scheduling on edge, fog, and cloud computing resources. Softw: Pract Exp 2020;50(5):558–95.
[158] Zhang X, Wang Y, Lu S, Liu L, Shi W, et al. OpenEI: An open framework for edge intelligence. In: 2019 IEEE 39th international conference on distributed computing systems. ICDCS, IEEE; 2019, p. 1840–51.
[159] Alotaibi A, Barnawi A, Buhari M, et al. Attribute-based secure data sharing with efficient revocation in fog computing. J Inf Secur 2017;8(03):203.
[160] Sun T, Yang P, Li M, Liao S. An automatic generation approach of the cyber threat intelligence records based on multi-source information fusion. Future Internet 2021;13(2):40.
[161] Al-Taleb N, Saqib NA. Towards a hybrid machine learning model for intelligent cyber threat identification in smart city environments. Appl Sci 2022;12(4):1863.
[162] Alexopoulos N, Vasilomanolakis E, Roux SL, Rowe S, Mühlhäuser M. TRIDEnT: building decentralized incentives for collaborative security. 2019, arXiv preprint arXiv:1905.03571.
[163] Samtani S, Abate M, Benjamin V, Li W. Cybersecurity as an industry: A cyber threat intelligence perspective. In: Holt TJ, Bossler AM, editors. The palgrave handbook of international cybercrime and cyberdeviance. Cham: Springer International Publishing; 2020, p. 135–54.
[164] Nacer MI, Prakoonwit S, Alarab I. The combination of AI, blockchain, and the Internet of Things for patient relationship management. Int Ser Oper Res Manage Sci 2021;305:49–65.
[165] Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y. Differentially private asynchronous federated learning for mobile edge computing in urban informatics. IEEE Trans Ind Inf 2020;16(3):2134–43.
[166] Nguyen DC, Ding M, Pathirana PN, Seneviratne A, Li J, Vincent Poor H. Federated learning for Internet of Things: A comprehensive survey. IEEE Commun Surv Tutor 2021;23(3):1622–58.

[167] Conti M, Dargahi T, Dehghantanha A. Cyber threat intelligence: Challenges and opportunities. Adv Inf Secur 2018;70:1–6.

[168] Rassam MA, Maarof MA, Zainal A. Big data analytics adoption for cybersecurity: A review of current solutions, requirements, challenges and trends. J Inf Assur Secur 2017;11:124–45.

[169] Siddiqa A, Hashem IAT, Yaqoob I, Marjani M, Shamshirband S, Gani A, Nasaruddin F. A survey of big data management: Taxonomy and state-of-the-art. J Netw Comput Appl 2016;71:151–66.

[170] Serketzis N, Katos V, Ilioudis C, Baltatzis D, Pangalos G. Improving forensic triage efficiency through Cyber Threat Intelligence. Future Internet 2019;11(7).

[171] Guo J, Huang C, Hou J. A scalable computing resources system for remote sensing big data processing using GeoPySpark based on spark on K8s. Remote Sens 2022;14(3):521.

[172] Dafir Z, Lamari Y, Slaoui SC. A survey on parallel clustering algorithms for Big Data. In: Artificial intelligence review, Vol. 54, Springer Netherlands; 2021, p. 2411–43.

[173] Torres J, Nogueira M, Pujolle G. A survey on identity management for the future network. IEEE Commun Surv Tutor 2013;15(2):787–802.

[174] Pal S, Hitchens M, Varadharajan V. Towards the design of a trust management framework for the Internet of Things. In: 2019 13th international conference on sensing technology. ICST, IEEE; 2019, p. 1–7.

[175] Werner J, Westphall CM, Westphall CB. Cloud identity management: A survey on privacy strategies. Comput Netw 2017;122:29–42.

[176] Liu Y, He D, Obaidat MS, Kumar N, Khan MK, Raymond Choo KK. Blockchain-based identity management systems: A review. J Netw Comput Appl 2020;166(May):102731.

[177] Suguna M, Anusia R, Mercy Shalinie S, Deepti S. Secure identity management in mobile cloud computing. In: 2017 international conference on nextgen electronic technologies: silicon to software, ICNETS2 2017. IEEE; 2017, p. 42–5.

[178] Selvanathan N, Jayakody D, Damjanovic-Behrendt V. Federated identity management and interoperability for heterogeneous cloud platform ecosystems. In: ACM international conference proceeding series. 2019.

[179] Samtani S, Kantarcioglu M, Chen H. Trailblazing the artificial intelligence for cybersecurity discipline. ACM Trans Manage Inf Syst 2020;11(4):1–19.

[180] Sullivan C, Burger E. "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence. Comput Law Secur Rev 2017;33(1):14–29.

[181] Rajendran Keerthana, Jayabalan Manoj RME. A study on k-anonymity, l-diversity, and t-closeness techniques focusing medical data. IJCSNS Int J Comput Sci Netw Secur 2017;17(12):172–7.

[182] Farid F, Elkhodr M, Sabrina F, Ahamed F, Gide E. A smart biometric identity management framework for personalised iot and cloud computing-based healthcare services. Sensors (Switzerland) 2021;21(2):1–18.

[183] Ghimire B, Rawat DB. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. IEEE Internet Things J 2022.

[184] Adewopo V, Gonen B, Adewopo F. Exploring open source information for cyber threat intelligence. In: 2020 IEEE international conference on big data (big data). IEEE; 2020, p. 2232–41.

[185] Albakri A, Boiten E, De Lemos R. Sharing cyber threat intelligence under the general data protection regulation. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). LNCS, vol. 11498, 2019, p. 28–41.

[186] Bu-Pasha S. Cross-border issues under EU data protection law with regards to personal data protection. Inf Commun Technol Law 2017;26(3):213–28.

[187] Magruk A, et al. Uncertainty in the sphere of the industry 4.0–potential areas to research. Bus Manage Educ 2016;14(2):275–91.

[188] Cofta P, Karatzas K, Orłowski C. A conceptual model of measurement uncertainty in IoT sensor networks. Sensors 2021;21(5):1827.

[189] Frederiksen M. Trust in the face of uncertainty: A qualitative study of intersubjective trust and risk. Int Rev Sociol 2014;24(1):130–44.

[190] Ismail S, Shah K, Reza H, Marsh R, Grant E. Toward management of uncertainty in self-adaptive software systems: IoT case study. Computers 2021;10(3):27.

[191] Haseeb K, Saba T, Rehman A, Ahmed I, Lloret J. Efficient data uncertainty management for health industrial internet of things using machine learning. Int J Commun Syst 2021;34(16):e4948.

[192] Saeedi R, Fallahzadeh R, Alinia P, Ghasemzadeh H. An energy-efficient computational model for uncertainty management in dynamically changing networked wearables. In: Proceedings of the 2016 international symposium on low power electronics and design. 2016, p. 46–51.

[193] Nærland K, Müller-Bloch C, Beck R, Palmund S. Blockchain to rule the waves-nascent design principles for reducing risk and uncertainty in decentralized environments. In: ICIS. 2017.

[194] Li Q, Li A, Wang T, Cai Y. Interconnected hybrid AC-DC microgrids security enhancement using blockchain technology considering uncertainty. Int J Electr Power Energy Syst 2021;133:107324.

[195] Wang S, Liu X, Ha J. Optimal IoT-based decision-making of smart grid dispatchable generation units using blockchain technology considering high uncertainty of system. Ad Hoc Netw 2022;127:102751.

[196] Prithi S, Sumathi D, Poongodi T, Suresh P. Trust management framework for handling security issues in multi-cloud environment. In: Operationalizing multi-cloud environments. Springer; 2022, p. 287–306.

[197] Tourani R, Misra S, Mick T, Panwar G. Security, privacy, and access control in information-centric networking: A survey. IEEE Commun Surv Tutor 2017;20(1):566–600.

[198] Pal S, Jadidi Z. Protocol-based and hybrid access control for the IoT: Approaches and research opportunities. Sensors 2021;21(20):6832.

[199] Ravidas S, Lekidis A, Paci F, Zannone N. Access control in Internet-of-Things: A survey. J Netw Comput Appl 2019;144:79–101.

[200] Pal S, Dorri A, Jurdak R. Blockchain for IoT access control: Recent trends and future research directions. J Netw Comput Appl 2022;103371.

[201] Li Q, Zhang Q, Huang H, Zhang W, Chen W, Wang H. Secure, efficient and weighted access control for cloud-assisted industrial IoT. IEEE Internet Things J 2022.

[202] Huo R, Zeng S, Wang Z, Shang J, Chen W, Huang T, Wang S, Yu FR, Liu Y. A comprehensive survey on blockchain in industrial Internet of Things: Motivations, research progresses, and future challenges. IEEE Commun Surv Tutor 2022.

[203] Pal S, Hitchens M, Varadharajan V, Rabehaja T. Policy-based access control for constrained healthcare resources in the context of the Internet of Things. J Netw Comput Appl 2019;139:57–74.

[204] Xu R, Chen Y, Blasch E, Chen G. A federated capability-based access control mechanism for internet of things (iots). In: Sensors and systems for space applications XI. Vol. 10641, International Society for Optics and Photonics; 2018, 106410U.

[205] Hernández-Ramos JL, Jara AJ, Marín L, Skarmeta Gómez AF. DCapBAC: embedding authorization logic into smart things through ECC optimizations. Int J Comput Math 2016;93(2):345–66.

[206] Pal S, Hill A, Rabehaja T, Hitchens M. A blockchain-based trust management framework with verifiable interactions. Comput Netw 2021;200:108506.

[207] Pal S, Rabehaja T, Hitchens M, Varadharajan V, Hill A. On the design of a flexible delegation model for the Internet of Things using blockchain. IEEE Trans Ind Inf 2019;16(5):3521–30.

[208] Agrawal TK, Angelis J, Khilji WA, Kalaiarasan R, Wiktorsson M. Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration. Int J Prod Res 2022;1–20.

[209] Hassan MU, Rehmani MH, Chen J. Differential privacy techniques for cyber physical systems: a survey. IEEE Commun Surv Tutor 2019;22(1):746–89.

[210] Rajkumar R, Lee I, Sha L, Stankovic J. Cyber-physical systems: the next computing revolution. In: Design automation conference. IEEE; 2010, p. 731–6.

[211] Amato A, Quarto A, Di Lecce V. An application of cyber-physical system and multi-agent technology to demand-side management systems. Pattern Recognit Lett 2021;141:23–31.

[212] Sawhney A, Riley M, Irizarry J, Riley M. In: Sawhney A, Riley M, Irizarry J, editors. Construction 4.0. 10, Routledge; 2020, 9780429398100, doi.

[213] Vanderbilt Engineering Graduate Admissions Team. IoT-CPS. 2022, https://blog.engineering.vanderbilt.edu/what-is-the-difference-between-cps-and-iot. [Online Accessed 25 June 2022].

[214] Griffor ER, Greer C, Wollman DA, Burns MJ, et al. Framework for cyber-physical systems: Volume 1, overview. 2017.

[215] Qiu H, Qiu M, Liu M, Memmi G. Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. IEEE J Biomed Health Inform 2020;24(9):2499–505.

[216] Alrimawi F, Pasquale L, Mehta D, Nuseibeh B. I've seen this before: Sharing cyber-physical incident knowledge. In: Proceedings of the 1st international workshop on security awareness from design to deployment. 2018, p. 33–40.

[217] Sikder AK, Petracca G, Aksu H, Jaeger T, Uluagac AS. A survey on sensor-based threats and attacks to smart devices and applications. IEEE Commun Surv Tutor 2021;23(2):1125–59.

[218] Fotiadou K, Velivassaki T-H, Voulkidis A, Railis K, Trakadas P, Zahariadis T. Incidents information sharing platform for distributed attack detection. IEEE Open J Commun Soc 2020;1:593–605.

[219] Alrimawi F, Pasquale L, Mehta D, Yoshioka N, Nuseibeh B. Incidents are meant for learning, not repeating: sharing knowledge about security incidents in cyber-physical systems. IEEE Trans Softw Eng 2020.

[220] Yang C, Li Y, Yang Y, Liu Z, Liao M. Transfer learning-enabled modelling framework for digital twin. In: 2022 IEEE 25th international conference on computer supported cooperative work in design. CSCWD, IEEE; 2022, p. 113–8.

[221] Schroeder GN, Steinmetz C, Pereira CE, Espindola DB. Digital twin data modeling with automationml and a communication methodology for data exchange. IFAC-PapersOnLine 2016;49(30):12–7.

[222] Yeh C, Do Jo G, Ko Y-J, Chung HK. Perspectives on 6G wireless communications. ICT Express 2022.

[223] Chowdhury MZ, Shahjalal M, Hasan M, Jang YM, et al. The role of optical wireless communication technologies in 5G/6G and IoT solutions: Prospects, directions, and challenges. Appl Sci 2019;9(20):4367.

[224] Rajatheva N, Atzeni I, Bjornson E, Bourdoux A, Buzzi S, Dore J-B, Erkucuk S, Fuentes M, Guan K, Hu Y, et al. White paper on broadband connectivity in 6G. 2020, arXiv preprint arXiv:2004.14247.

[225] Shah K, Chadotra S, Tanwar S, Gupta R, Kumar N. Blockchain for IoV in 6G environment: review solutions and challenges. Cluster Comput 2022;1–29.
[226] Siriwardhana Y, Porambage P, Liyanage M, Ylianttila M. AI and 6G security: Opportunities and challenges. In: 2021 joint European conference on networks and communications & 6G summit (euCNC/6G summit). IEEE; 2021, p. 616–21.
[227] Mohsan SAH, Mazinani A, Malik W, Younas I, Othman NQH, Amjad H, Mahmood A. 6G: envisioning the key technologies, applications and challenges. Int J Adv Comput Sci Appl 2020;11(9).
[228] Xu H, Klaine PV, Onireti O, Cao B, Imran M, Zhang L. Blockchain-enabled resource management and sharing for 6G communications. Digit Commun Netw 2020;6(3):261–9.
[229] Jahid A, Alsharif MH, Hall TJ. The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap. 2021, arXiv preprint arXiv:2109.03184.
[230] Wang Z, Du Y, Wei K, Han K, Xu X, Wei G, Tong W, Zhu P, Ma J, Wang J, et al. Vision, application scenarios, and key technology trends for 6G mobile communications. Sci China Inf Sci 2022;65(5):1–27.
[231] Peltonen E, Bennis M, Capobianco M, Debbah M, Ding A, Gil-Castiñeira F, Jurmu M, Karvonen T, Kelanti M, Kliks A, et al. 6G white paper on edge intelligence. 2020, arXiv preprint arXiv:2004.14850.
[232] Ji B, Wang Y, Song K, Li C, Wen H, Menon VG, Mumtaz S. A survey of computational intelligence for 6G: Key technologies, applications and trends. IEEE Trans Ind Inf 2021;17(10):7145–54.
[233] Dionisio JDN, Burns III WG, Gilbert R. 3D virtual worlds and the metaverse: Current status and future possibilities. ACM Comput Surv 2013;45(3):1–38.
[234] Mystakidis S. Metaverse. Encyclopedia 2022;2(1):486–97.
[235] Lee L-H, Braud T, Zhou P, Wang L, Xu D, Lin Z, Kumar A, Bermejo C, Hui P. All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. 2021, arXiv preprint arXiv:2110.05352.
[236] Duan H, Li J, Fan S, Lin Z, Wu X, Cai W. Metaverse for social good: A university campus prototype. In: Proceedings of the 29th ACM international conference on multimedia. 2021, p. 153–61.
[237] Di Pietro R, Cresci S. Metaverse: Security and privacy issues. In: 2021 third IEEE international conference on trust, privacy and security in intelligent systems and applications (TPS-iSA). IEEE; 2021, p. 281–8.
[238] Dunnett K, Pal S, Jadidi Z, Jurdak R. The role of cyber threat intelligence sharing in the metaverse. IEEE Internet Things Mag. 2023;6(1):154–60.
[239] Wang Y, Su Z, Zhang N, Liu D, Xing R, Luan TH, Shen X. A survey on metaverse: Fundamentals, security, and privacy. 2022, arXiv preprint arXiv:2203.02662.
[240] Grider D, MAXIMO M. The metaverse: Web 3.0 virtual cloud economies. Grayscale Res 2021.
[241] Wang T, Okada S. Human relationship advice system in metaverse world: Application propose of CTUP model in future communication. In: 2022 4th global conference on life sciences and technologies. IEEE; 2022, p. 202–3.
[242] Cheng R, Wu N, Chen S, Han B. Will metaverse be nextg internet? vision, hype, and reality. 2022, arXiv preprint arXiv:2201.12894.
[243] Singh A, Dev K, Siljak H, Joshi HD, Magarini M. Quantum Internet—Applications, functionalities, enabling technologies, challenges, and research directions. IEEE Commun Surv Tutor 2021;23(4):2218–47.
[244] Dixit V, Selvarajan R, Aldwairi T, Koshka Y, Novotny MA, Humble TS, Alam MA, Kais S. Training a quantum annealing based restricted boltzmann machine on cybersecurity data. IEEE Trans Emerg Top Comput Intell 2021.
[245] Hechler E, Oberhofer M, Schaeck T. AI and quantum computing. In: Deploying AI in the enterprise. Springer; 2020, p. 273–95.
[246] Zvelocti. 2022, https://zvelo.com/zvelocti-cyber-threat-intelligence. [Online Accessed 22 May 2022].
[247] Thraetstream. 2022, https://www.anomali.com/products/threatstream. [Online Accessed 22 May 2022].
[248] Watson K. CISA-CTI. 2022, https://www.cisa.gov/sites/default/files/publications/Service%20Models%20for%20Cyber%20Threat%20Intelligence_508c.pdf. [Online Accessed 24 March 2022].