International Journal of Safety and Security Engineering
Vol. 14, No. 5, October, 2024, pp. 1357-1369
Journal homepage: http://iieta.org/journals/ijsse

A Survey on the Integration of Cyber Threat Feeds and Blockchain Technology

Ahmed El-Kosairy*, Nashwa AbdelBaki, Heba Aslan

Center for Informatics Science, School of Information Technology and Computer Science, Nile University, Giza 12588, Egypt

Corresponding Author Email: ah.elkosairy@nu.edu.eg

https://doi.org/10.18280/ijsse.140502

Received: 10 June 2024
Revised: 11 September 2024
Accepted: 26 September 2024
Available online: 31 October 2024

Keywords:
blockchain, threat intelligence feeds, Cyber Threat Intelligence, threat sharing, cybersecurity alerting, detection and response

ABSTRACT

Cybersecurity attacks have significantly increased in recent years. Cybersecurity/Alert Threat Intelligence (CTI) has been introduced to ensure systems are secure against these attacks. CTI must be both swift and capable of protecting the sender's identity to mitigate threats immediately. It is crucial because it enhances understanding of attacks. However, a paradox arises between the necessity of generating Cyber Threat Intelligence (CTI) for community sharing and the need to address other challenges not encompassed by CTI, such as privacy concerns This paper aims to explore how blockchain technology can be integrated with CTI to overcome challenges in traditional CTI. This integration has attracted substantial interest in recent years. We evaluate how these studies recently address the relationship between CTI and blockchain integration. Each contribution is scrutinized based on set criteria, highlighting areas where information is lacking, through a comprehensive comparison. We have gathered and compared the latest contributions that employ blockchain to resolve CTI issues. Additionally, we identify gaps in each paper to provide a broad overview of areas requiring further investigation. Additionally, we examine the potential challenges associated with this integration and provide a comparative analysis of recent studies that have investigated the subject. The principal contribution of this paper lies in the integration of all aspects related to both CTI feed sharing and blockchain technology, such as consensus types, CTI sharing mechanisms, mining rewards, CTI standards, and the challenges and limitations of combining these two approaches. This integration could aid in designing a secure system for sharing CTI feeds while preserving privacy and mitigating the threats posed by attackers. In addition, this paper highlights the future research directions, particularly in improving privacy, scalability, and participation incentives in blockchain-based CTI systems.

1. INTRODUCTION

Cybercrime has grown as an increasing number of people have access to the Internet, which has changed how individuals worldwide communicate and get information. With CTI, the community can instantly share alerts and the attack anatomy to limit hacking methods, techniques, and procedures. This is one of the best ways to stop attackers. CTI technology has helped a lot in the struggle against cybercriminals by making it easy to share information quickly. However, the current CTI industry faces challenges and limitations that must be solved to improve privacy, trust and stop the waves of attacks [1].

CTI's IoC (Indicator of Compromise) is evidence found on an endpoint or in a network that strongly suggests a network or endpoint intrusion and can be used to find and track potential cyber threats and where they came from [2]. This artifact could be a newly created file, a modified one, a change in directory permissions, activating a port number to a new registry entry, etc. Besides file hashes, domain names, and IP addresses, signatures might also be included in the CTI report.

Current and conventional CTI that employs structured standards, such as Structured Threat Information exchange (STIX) [3], and Open Indicator of Compromise (OpenIoC), were developed to standardize the exchange of threat intelligence feeds within the CTI community and across platforms [4]. The lack of information sharing and specific details about attacks is currently the biggest challenge facing CTI [5]. Some entities are hesitant to share information as this could compromise their privacy and security. In addition, disclosing attack information could harm their reputation and lead to negative publicity [6]. CTI systems face significant challenges that blockchain technology aims to mitigate. A key issue is the lack of reliable mechanisms to verify the accuracy of threat data, as CTI systems often rely on expensive, centralized services vulnerable to manipulation. Privacy is another concern, with many organizations hesitant to share CTI due to the risk of exposing critical information, which could lead to legal consequences and reputational damage. Moreover, current CTI systems struggle to ensure the credibility and nonrepudiation of shared data, as compromised servers could propagate false information.

Meanwhile, blockchain, built on Peer to Peer (P2P) technology, provides privacy protection, secrecy, and decentralized review and quality. Combining blockchain with CTI will encourage the actors to share attacks' information as the blockchain is an anonymous platform [7].

This will protect the privacy of the parties involved in the sharing process. In addition, blockchain is characterized by being decentralized. Therefore, the use of blockchain will enhance the process of information sharing within the community without using a centralized entity, which could be corrupted. On the other hand, the use of blockchain leads to new challenges that should be considered such as: resource consumption, forking, and sybil attacks.

In this paper, we discuss the CTI model with a concentration on their limitations. One of the main solutions to solve these limitations is incorporating blockchain in CTI systems. We also discuss the challenges of using blockchain with CTI systems with their possible solutions. Furthermore, we present a comprehensive comparative analysis of recent surveys regarding the integration of threat intelligence and blockchain technology. The emphasis is placed on assessing factors such as consensus types, structured threat intelligence sharing language standards, reward models, and the incorporation of CTI sharing. Also, we analyze various studies to determine the depth and comprehensiveness of each contribution and explore how CTI and blockchain could be integrated and work together. The studies we selected were sourced from reputable platforms. This survey presents the benefit of encompassing vital factors pertinent to the merger of blockchain technology and Cyber Threat Intelligence (CTI).

It encompasses considerations such as consensus mechanisms, standards for structured threat intelligence sharing language, reward systems tied to CTI contribution, and an exploration of challenges and limitations as recognized by preceding surveys. We identified noteworthy contributions and emphasized their unique perspectives while identifying areas that require further investigation in integrating blockchain and CTI. The following are the main paper's contributions:

1. Introduce a survey of blockchain based CTI systems.
2. Provide a brief overview of the most demanding problems plaguing the traditional threat intel.
3. Explain how the technology of blockchain can enhance the CTI and provide a new framework to fix the current challenges.
4. Highlight the most recent works that have explored CTI feed sharing and conduct a comparative analysis of these contributions to illustrate the structure and key features of each approach.
5. Describe the difficulties that will arise when using blockchain technology with CTI.

The remainder of this paper is organized as: The purpose and operation of CTI are described in section 2, the issues and difficulties currently facing CTI are discussed in section 3. Section 4 goes on to explain blockchain's origins and functionality. In section 5, We outline how the technology of the blockchain could be applied to threat intel to strengthen the existing CTI framework, and we discuss the potential challenges that may emerge from integrating blockchain with CTI. In section 7, we summarize the findings from the research and conclude them.

2. FEEDS OF CTI

To secure a system, one must have access to relevant data. CTI provides the data needed to secure networks, systems, and infrastructure. Threat intel encompasses details about attackers, their capabilities, and the TTPs they commonly utilize [8]. CTI is a data driven security system that provides deeper insights into risks & threats. In addition, they employed Advanced Persistent Threat (APT), and defenses designed to counter them [9].

A third party, the company, or a third-party provider could gather this data. This shift to intelligence-based defense has historically spawned a plethora of firms providing CTI feeds. Though, these services have typically been priced out of reach for most organizations. These services provide essential data; however, it can be expensive and challenging to be integrated into existing security systems. In addition, numerous open-source alternatives have emerged in recent years. Some of them can be purchased and provided by private security firms. These open-source alternatives have become attractive options for organizations looking to leverage intelligence-based defense since they offer the same level of security at a fraction of the cost compared to commercial offerings [10]. Even though commercial CTI feeds might include unique findings, since they have their own IR and R&D teams and financial income from reselling data, they can develop and create new methods and techniques. However, the open-source feeds provide the potential of community's contribution, which provides more creativity, add-ons, and innovation than the commercial feeds [11]. Cyber Threat Intelligence can collect data on attackers and tactics, allowing for more informed defensive measures. This data can give organizations an idea of the types of attacks they may be vulnerable to, and the skills and resources attackers have at their disposal. The process of gathering Cyber Threat Intelligence looks like this: first, objectives and targets need to be established [12]. Next, information is gathered about the attacks and the process. Then, the collected information is analyzed. Finally, a report is produced that details the findings and the attack anatomy, Figure 1.

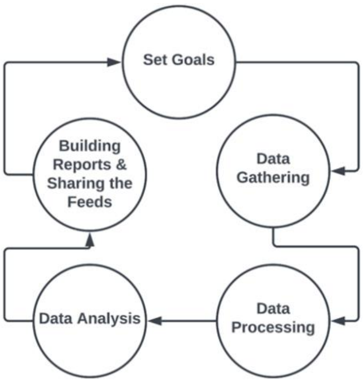


Figure 1. The CTI methodology

2.1 CTI framework & ecosystem

To understand the idea of CTI, we need to understand the CTI anatomy, which is shown in Figure 1, different vendors and service providers could collaborate by sharing threat feeds [13]. Security analysts should structure the shared threat feeds. Only filtered threat feeds can be used as threat intel feeds. Information about the attack anatomy, including TTP and tools used by threat actors, is provided by the most recent CTI feeds.

Cybersecurity enables sufficient security controls with the help of tactical threat intelligence. Security analysts should structure the shared threat feeds so they are filtered and can be used as threat intelligence feeds. Various aspects of the attack are documented in the CTI, including the IP, URL, and domain names; malware hashes; DLL names; registry keys; email attachments; links; and more. This enables security analysts to have an overall understanding of the threat actor's attack anatomy and to gain visibility into their TTPs, as well as the tools they are using endpoint protection, endpoint incident response, security incident event monitoring devices, Intrusion Detection and Prevention systems (IDS/IPS), and firewalls are just some of the technical technologies that make use of the CTI. For organizations to take full advantage of threat intelligence feeds, security analysts must develop an effective system for sharing CTI. These tools identify threats and prevent connection attempts to suspicious IP addresses using the data already present in technical threat intelligence report. However, the intelligence information can only be used and shared with other experts if it follows a standard format. The use of CTI reporting templates is necessary for both technical threat intelligence and tactical threat intelligence.

The community's clients and customers now have access to threat intelligence in a usable format, allowing them to stop attacks before they even begin. Bidirectional feed sharing between CTI platforms is possible. Cyberattacks have become more sophisticated; therefore, identifying and investigating them have become more challenging. Companies and government agencies have had to increase their security budgets to combat cybercriminals, who often use sophisticated techniques such as malware, phishing scams, and data exfiltration.

Attackers are more agile and covert in this new era of attacks than ever before. Automated community wide CTI is being developed more frequently by Cyber Emergency Response Teams (CERTs). CERTs are also responsible for providing community-wide protection against attacks, such as preventing known attacks from occurring again or helping other organizations to identify and defend against new threats.

2.2 History of standardization

Automation and the use of a standardized structured language are crucial for delaying or halting attackers. Automation can help speed up the detection of malicious behavior, allowing organizations to act before any harm is done as a result; numerous contributions have been made throughout the global collaboration of the cyber security industries. By creating a common language, security professionals can quickly communicate the nature of threats and the actions needed to protect against them to help the network and make sure they are prepared to prevent these techniques; these formats distribute CTI feeds about attacks. These guidelines, which specify how information is stored, are referred to as threat reporting formats or cyber threat information structures.

For sharing threats, a standard structure and an exchange protocol that specifies data transmission are both necessary [14]. The nonprofit organization is currently developing STIX, TAXII, and other information sharing standards created by MITRE. These standards have been designed to foster trust and interoperability among public & private sector organizations and to promote the sharing of Cyber Threat Intelligence. The Internet Engineering Task Force (IETF) has also created several standards. In 2007, the Internet Engineering Task Force (IETF) developed a standard for incident objects called Incident Object Description Format (IODF) [15]. It was a technique like TAXII but is no longer supported. TAXII was introduced by The Trusted Automated Exchange of Intelligence Information as an exchange protocol for incident data and RID. Cybersecurity vendors are also developing proprietary threat-sharing standards formats such as OpenIOC and Mandiant, but these standards usually have limited use on other platforms. Also, standards are used with more tools, such as format converters, tool plugins, and APIs for CTI. Therefore, the availability of these extra tools increases the standards' and protocols' efficiency.

2.3 Sharing formats for CTI

When dealing with an Incident Response (IR), information security researchers use a variety of IR data types. For the IR management process, and to comprehend the attack anatomy and root cause, the standard language is essential. As a result, the entities can now exchange CTI data to cooperate in preventing the attack from happening in the first place. By using standard data types, information security researchers can quickly and effectively detect, analyze, respond to, and investigate incidents. The fact that the standard format supports the current security tools is yet another benefit of using it. CTI formats have been created by several research organizations.

The category types shown below can be used to organize the formats offered by CTI. These are fundamental incident indicators, also referred to as actionable data (artifacts; file hash, IP address, registry key information, etc.), incident/threat reporting data, low level raw data (network traffic), vulnerability/weakness, and attack pattern data (vulnerability ID, vulnerability score). Once there are formats that describe incident or threat events, both humans and computers can read them more easily [16]. We rank the most pertinent CTI reporting formats based on how well they support other CTI sharing formats as shown in Table 1, which focuses on threat reporting data formats [17]. Pcap, NetFlow, IPFIX (IP Flow Information Export), and CEF (Common Event Format) are examples of low-level data forms that describe network level data gathered by security tools.

Table 1. STIX support for varied data formats

Format	Format Structures	Cyber Threat Intelligence (CTI)
		STIX
Scan and IR	Open_IOC YARA_Rule IPS_Rule -Cybox -MAEC -MMDEF	Covered
Low level	-CEF Net-Flow IP_FIX -Pcap	Covered
Vulnerability	-CVE -CAPEC	Covered
	-CWSS -CVSS	Not covered
	-CPE -CWE	Covered

Many networks' security tools use the Pcap format to send captured network traffic and provide a level of detail that allows investigators to observe every process step. It was developed by the Tcpdump group and is open source. The libraries that can analyze Pcap files and data include Tcpdump, Wireshark, Snort, Network Miner, and Libecap [17]. NetFlow enabled network devices to export traffic statistics as IP flow records to analyze network traffic by source. To share event feeds between vendors and clients, Security Information and Event Management (SIEM) uses the Common Event Format (CEF) event structure based on Syslog [18]. The antivirus sector uses MMDEF to facilitate the exchange of malware intelligence. Malware can be described using MMDEF in the XML version of MAEC. Cuckoo Sandbox used MMDEF in earlier iterations. Additional formats are also available, including CVE (Common Vulnerabilities and Exposures) [19], CWE [20], CPE [21], CVSS, CWSS. CVE list known security vulnerabilities and disclosures, each entry in the list includes an identification number, description, and at least one public reference. CVE list is supported by MITRE and feeds the U.S. National Vulnerability Database [22]. Common Attack Pattern Enumeration and Classification (CAPEC) is a product that contains attack patterns. CAPEC data is available in CSV and XML format. STIX is used to exchange information about cyber threats [23, 24].

3. DIFFICULTIES WITH THE EXITING CTI METHODOLOGY

This section explains the primary difficulties with the current CTI approach. Cybercriminals use various techniques to attack a victim: they can either steal the victim's private, critical info such as financial info or gain access to and take over the victim's computer to carry out other malicious acts. Examples of these malicious actions include locking or encrypting the victim's computer or distributing malware (in the case of a botnet or a ransomware attack) [25]. Despite using various infection techniques, all cyberattacks follow a similar life cycle, starting with a victim survey and ending with malicious activity on the target's endpoint or network. In addition to the traditional techniques that have always been employed to trick victims (such as phishing) into taking the actions that the attackers want, attackers have recently used more sophisticated and creative techniques for attacking victims. Exploiting zero-day vulnerabilities is one of these methods. Another technique is sending malicious software to the victim's computer in an unexpected format, such as Word files [26]. Some examples of such sophisticated attacks are new families of ransomware that behave like worms and have infected tens of thousands of people, organizations, and crucial systems. The development of attack techniques makes it extremely difficult to identify the attacker and the attack's point of origin. As previously mentioned, the best way to spread these attack descriptions and anatomy throughout the community is to use threat intelligence feeds. The current difficulties and problems in CTI are explained in the subsequent sub-sections.

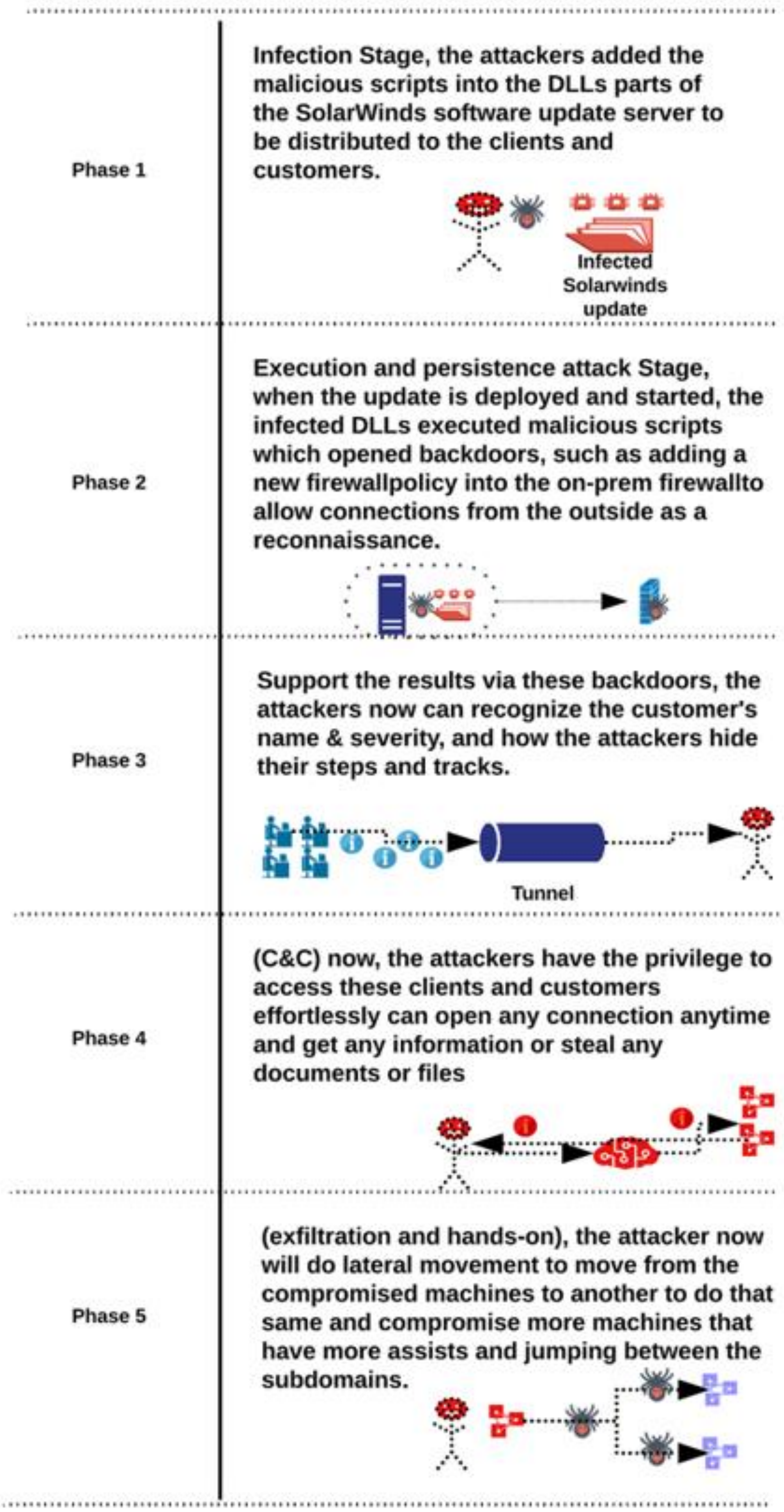
3.1 Accuracy of threat data

The current threat Intel approach fails to deliver test criteria for the received reports and feeds. The quality measurements are the only methods used to prevent disqualified feeds. One must use the commercial threat intelligence feeds company with a high subscription cost to obtain accurate and high-quality information. On the other hand, the threat data quality could be hacked, which creates trust and a central point of failure. If a hacker can access the CTI's backend servers, they can alter the feeds' content and manipulate the records to include fictitious information. The attack may even instruct the target to run a script that gives the perpetrator access to the client's computers and networks as in the SolarWinds supply chain attack that has taken place. Solar-Winds Corporation in 2021 was targeted of a cyberattack. An American company called SolarWinds creates software for businesses to manage their networks, systems, and IT infrastructure. The American government, Microsoft, and cybersecurity companies like CrowdStrike and FireEye have been affected by that attack. The attack contains five phases, as illustrated in Figure 2 [27].

In phase 1 (infection), the attackers added the malicious scripts into the DLL parts of the SolarWinds software update server to be distributed to the clients and customers. When the update was applied, phase 2 (execution and persistence attacks) began, infected DLLs executed malicious scripts that opened backdoors, such as adding a new firewall policy to the on-premises firewall to allow connections from the outside as reconnaissance. In phase 3 (supporting the results), via these backdoors, the attackers can now identify the customer's name and priority level. Then, the attackers hid their steps and tracks. In phase 4 (C&C), the attackers have the privilege to access these clients, can open any connection anytime, and get any information or steal any documents or files. In phase 5 (exfiltration and hands-on), the attacker now will do lateral movement to move from the compromised machines to another to do the same steps and compromise more machines [28]. The same technique could be used with any private CTI, and the consequences would be dangerous. On the other hand, the current CTI approach cannot provide quality either through the private CTI vendors or the public and accessible sources, which will lead to the same method being used to compromise any private CTI, with potentially disastrous results. However, the current CTI approach will lead to an overwhelming amount of CTI traffic and reports with low-quality content as it relies on private CTI vendors rather than publicly available sources. Also, it should be shown that an outside entity can effectively deny and regulate these occurrences. Each party acknowledges its responsibility to check the accuracy and completeness of the CTI's reports. The third-party may be compromised or corrupted for various reasons. Therefore, it is necessary to demonstrate another entity to review and audit the third party, and so on, in an infinite regress. Finding an alternate method to audit and review the content's quality to avoid these risks is crucial. Also, a third party should be proven to reduce and control low quality or corrupted feeds. Everyone agrees to audit and review the CTI's reports' content and quality. Sometimes, the third party could be corrupted for any reason or compromised. That means another party should be proven to review and audit the third party, which will lead to an infinite chain of entities and parties. Thus, one of the keys to overriding this issue is finding an alternative way to audit and review the quality of the content to avoid these types of risks.

3.2 Privacy and legal issue

In the current CTI setup, privacy is not an option, which is one of its major flaws. Most organizations and network members would prefer to collect feeds and updates with no covering for any personally identifiable information to protect their privacy and avoid potential legal repercussions. The main drivers of the attack's spread are review and filtering. A predetermined IR plan can be implemented within seconds to hours and reduce risk and bring the situation under control if an entity is compromised. One of the most important metrics in cyber security is the Mean Time to Response (MTTR), which gauges how quickly an incident response team can implement a plan for recovering from an incident. When the IR team gets started on the plan, they will keep meticulous notes, to produce a comprehensive report detailing everything they did and found during the maintenance window. That is why five phases must [29] exist in any IR plan, as shown in Figure 3. The final IR report will contain details related to the attack anatomy, which should be shared with the community to stop this attack wave from propagating. In addition, this report will contain sensitive and confidential information and details such as the customer's name, severity degree, any stolen accounts, fiscal impact, etc. Therefore, this report must be reviewed before being shared to avoid any legal liability. This procedure will take time and effort to filter these details from the report. That is why the identity of the compromised client should be hidden which is not applicable in the current CTI, especially the free ones.



Infection Stage, the attackers added the malicious scripts into the DLLs parts of the SolarWinds software update server to be distributed to the clients and customers.

Execution and persistence attack Stage, when the update is deployed and started, the infected DLLs executed malicious scripts which opened backdoors, such as adding a new firewallpolicy into the on-prem firewallto allow connections from the outside as a reconnaissance.

Support the results via these backdoors, the attackers now can recognize the customer's name & severity, and how the attackers hide their steps and tracks.

(C&C) now, the attackers have the privilege to access these clients and customers effortlessly can open any connection anytime and get any information or steal any documents or files

(exfiltration and hands-on), the attacker now will do lateral movement to move from the compromised machines to another to do that same and compromise more machines that have more assists and jumping between the subdomains.

Figure 2. Phases of SolarWinds attack

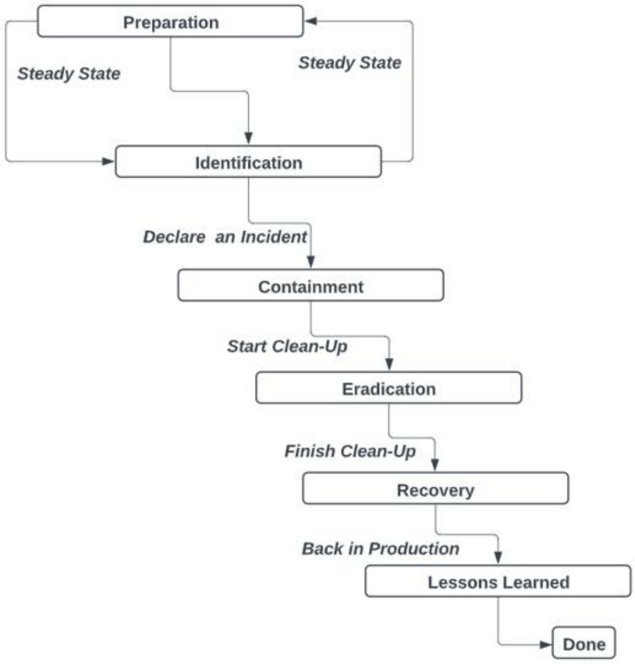


Figure 3. Incident response process

3.3 Credibility and non-repudiation issues

Gaining trust and credibility when receiving any CTI feeds means there should be a third party to review and audit the content and guarantee the inability of the sender to deny sending the message (non-repudiation). Since the attacker could bypass the security controls of any entity to gain access inside it, there is a high chance of compromising the CTI server to push fake CTI feeds and reports to the community [30]. This will lead to making a lot of noise in the community.

3.4 Negative publicity

Companies [31] are often hesitant to share cyberattacks, particularly breaches. This is due to concerns that regulatory and negative feedback will reflect their reputation in the stock market. Since the attackers now could reach the CTI back-end server using any zero-day exploitations, it will propagate fake CTI reports and details, resulting in lowering the company's reputation. The current CTI approaches did not provide countermeasures to avoid or eliminate that threat.

4. BLOCKCHAIN

The distributed database technology used by blockchain allows for an infinitely growing number of records (known as a "ledger"). Each new record in the ledger must be validated by most network participants to ensure its legitimacy. Additionally, blockchain uses a decentralized peer_2_peer network that authenticates users via public and private key cryptography. Each group contributes to the record by providing new information, and everyone in the system always has access to the most recent and accurate version [32]. One other key aspect of a blockchain network is the motivation it provides for participants to take part in the network. Participation in public networks is incentivized, especially in the case of a cryptocurrency network.

A private blockchain network presents a different incentive structure for users to take part. By this logic, blockchain networks can only function if their participants do not trust one another. The major party's impartiality may be contested by many participants. Limits on people's involvement are thus obligatory. When dealing with fewer entities or fewer standards, the problem of the cost when supporting a one center system could also be a challenge. Each participant in a blockchain has an ownership and responsible for only the costs associated with provisioning their own node in the network. Thus, everyone has an interest in the network. Open source blockchain implementations provide a solution to the problem of deciding who has authority over the network's rules [33]. Every network node in each community can demonstrate some minimum level of trust through its actions. Second, an agreement can be reached regarding the consensus protocol to be used. In this part, we give a wide view on how the business network should deal with fault tolerance and malicious activity. Several sectors around the world are showing serious interest in blockchain technology, and some academics have even compared it to the Internet in terms of its potential utility. Applications of blockchain technology can be found in digital identity, finance, cyber security, and other domains. There are currently 3 kinds of blockchain systems: public, private, and consortium. A public blockchain provides a distributed ledger that anyone can read, write, and mine on [34]. The other two types, on the other hand, limit who can mine blocks and add data to the blockchain.

4.1 Blockchain consensus proof types

Each blockchain has different application scenarios such as: PoW, PoS, and PoA which are considered the most famous consensus algorithms [35]. The PoW consensus applies a set of mechanisms that cause a huge effort when applying the network processing, for example mining blocks [36]. The goal is to protect the blockchain against computing power-based attacks such as DoS attacks. More computing power nodes mean more potential to perform the mining and similar processes on the blockchain network, thus achieving the rewards [37]. The PoS consensus algorithm applies processes that decide the validator node for the following blocks. The purpose is to distribute network tasks among the network's parties since the reward for the network process is not limited to the most computational power participants. Hence, PoS could protect the network against 51% of attacks given the fair distribution of tasks in the network [38]. In PoA based networks, validators confirm transactions and blocks, which are approved accounts. Validators run applications allowing them to put transactions in blocks. The auto-mated process does not require validators to scan their computers regularly. It, regardless, does require keeping the computer (the authority node) uncompromised. With PoA, individuals gain the right to become validators, so there is encouragement to keep the position that they have gained. This means that incentives can be unstable. The PoA is protecting the network from DoS attacks and 51% attacks to some extent [39]. The mechanism includes the normal distributed consistency algo for both BFT and PBFT. Table 2 presents the main comparisons among the consensus algorithms mentioned above. On the other hand, Table 3 shows a comparison of the consensus types [40] from the performance perspective, fault tolerance and compliance review.

From Tables 2 and 3, we conclude that adopting either the PoW or PoS consensus mechanisms would be beneficial, as both have been extensively tested and widely implemented across various industries and technologies. They have demonstrated robustness and ease of application. However, each method has its limitations: PoW requires significant energy and computational resources, while PoS risks centralizing control among large stakeholders, potentially undermining the network's decentralization. Therefore, selecting the appropriate consensus mechanism is crucial. In situations where power consumption is not an issue, PoW can be chosen for its higher security compared to other algorithms. Conversely, in trusted systems, PoS is the preferable option.

Table 2. Comparison between the consensus types of proofs

Type of Proof	Security Case	Pros	Cons
PoS	Use protection against the 51% attack	Saving for power and resources	The high rank stakeholder controls the network
PoA	Use protection against the 51% attack	Increases performance and saves resources	It is not well-suited for most nonenterprise applications, as it requires users to rely on validators and authorizers, whereas public Blockchains are designed to operate in a trustless environment
PoW	Open to 51% attacks	Test over time and easy to apply and implement	Power and resources consumption

Table 3. Comparison between the consensus mechanisms

Evaluation Factor	PoS	PoA	PoW	PBFT
Performance level	Low	High	Low	High
Fault tolerance	50%	51%	50%	33%
Compliance review	Weak	Weak	Weak	Strong

5. CTI AND BLOCKCHAIN INTEGRATION

This section explains how blockchain technology could be applied to CTI to improve existing methods and address some of the most pressing problems plaguing conventional CTI implementations. Integrating the CTI with the blockchain is depicted in Figure 4. Threat intel feeds, sourced from public or private vendors, can be distributed across the blockchain after review by the threat intelligence team, ensuring privacy by concealing the source's identity [13]. To collect their rewards, the miners (also known as validators) must now verify the accuracy and validity of the submitted content. In the following subsection, we detailed some blockchain-based CTI framework.

5.1 CTI consensus proof types

This section aims to examine the discrepancy among the latest research that have investigated the integration of CTI with blockchain technology. The selected contributions are based on the following criteria: The kinds of consensus employed, the structured threat intel sharing language formats utilized, the nature of the reward system, and whether the contribution is focused on CTI sharing. These contributions represent recent studies that discuss the integration of blockchain and CTI. We have chosen these contributions as they discuss the abovementioned factors and are selected from reputable sources, given that the integration of blockchain and CTI is a new concept and has only recently been discussed in academic community. In study of Riesco et al. [41], the authors identified the importance of blockchain technology to solve the CTI problems. Authors did not mention which Blockchain Consensus Type of Proof or reward had been used or Type of Reward, therefore, we represented the value as "-" in Table 4 since there was no value mentioned.

Otherwise, anything matched with our factors is represented in Table 4 as a "✔" such as in study of Riesco et al. [41], the authors identified the Structured Threat Intelligence Sharing Language Standards. On the other hand, in study [42], the authors highlighted the history of the blockchain without mentioning the type of proof and rewards they used. Cha et al. [43] proposed a blockchain-based Cyber Threat Intelligence system architecture for sustainable computing to ad-dress reliability, privacy, scalability, and sustainability for networks and IoT. They mentioned the blockchain in detail, and the reward idea, however, they did not mention the type of proof. In study of Gong and Lee [44], the paper uses blockchain technology to build blocks of CTI feeds. It also proposes to use the smart contract for threat intelligence sharing and rating.

In study of Dunnett et al. [45], they assess the potential of blockchain technology in addressing the limitations of the current platforms for sharing Cyber Threat Intelligence (CTI). The authors identify various challenges faced by CTI sharing systems and discuss how blockchain can offer secure and efficient solutions to these challenges. Additionally, they review some relevant works and high light unique research questions that require further attention in the future. In study of Khalil et al. [46], the authors present an updated literature review of authentication schemes proposed for the IoT in smart cities. The review covers many authentication schemes, highlighting several requirements and open issues researchers should consider when developing lightweight and robust schemes. The paper presents a descriptive approach to decentralized IoT architectures for smart assets in intelligent cities, which pose security threats that must be addressed. Given the resource-constrained nature of low powered IoT enabled smart assets, blockchain based solutions and distributed algorithms must be explored, as most intelligent city deployments are centralized. This centralization creates a single point of failure and a single point of contact for device authentication and overall system security. However, the use of blockchain-based solutions raises concerns about data storage. Decentralized storage platforms, such as IPFS, Swarm, and S3, may be explored to store data generated by intelligent assets. This integration can facilitate the storage of data hashes, helping to prevent storage exhaustion issues.

In study of Jiang et al. [47], the paper explains a new approach to threat intelligence sharing called BFLS, where blockchain based CTI sharing platforms are used for security and privacy. Federated learning technology is adopted for scalable machine learning applications like threat detection. Furthermore, users can obtain a well-trained threat detection model without sending personal data to the central server. Experimental results on the ISCX_IDS_2012 and CIC_DDoS_2019 datasets showed that BFLS could securely share CTI and have high accuracy in threat detection. The accuracies of BFLS are 98.92% and 98.56% on the two datasets, respectively. In study of Chatziamanetoglou and

Rantos [48], a new reputation based system for evaluating CTI feeds has been proposed by the authors. The system is called awareness architecture based on blockchain CTI convergence, and it uses blockchain technology for CTI sharing. The CTI evaluation is the main goal of the system and is based on a set of quality based parameters. Validators, who are part of the CTI-sharing community, are responsible for conducting the evaluation. The quality parameters are considered equally important and can be weighed accordingly on an ad hoc basis in line with the applied methodology and context.

Also, Dunnett et al. [49] presents a sharing framework for CTI using blockchain. The authors discussed a framework that relies on delegates who make trust decisions and evaluate trust in a decentralized manner. To ensure trustless delegation, the framework allows CTI producers to intentionally inject false data periodically to audit the behavior of delegates. In contrast to existing approaches, delegates within the proposed framework facilitate direct sharing of CTI with consumers, ensuring scalable CTI sharing. A qualitative evaluation of the framework's security shows it is resilient to standard privacy and trust concerns. Additionally, a quantitative evaluation of a proof_of_concept prototype using Ethereum demonstrates that the proposed framework is both scalable and cost effective.

Table 4. Comparison between the contributions according to consensus type of proof, structured threat intelligence sharing language standards, type of rewards, covering full CTI system, and covering sharing system but not CTI

	Blockchain Consensus Type of Proof					**Structured Threat Intelligence Sharing Language Standards**		**Type of Reward**	**Covering Full CTI System**	**Covering Sharing System but not CTI**
Contribution	**PoW**	**PoS**	**PoA**	**PBFT**	**PoET or BFT**	**STIX**	**TAXII**			
[41, 50]	-	-	-	-	-	✔	-	-	✔	-
[51]	-	-	✔	-	-	-	-	-	-	✔
[52]	✔	✔	-	-	-	-	-	✔	-	✔
[42, 53-58]	-	-	-	-	-	-	-	-	-	✔
[43]	-	-	-	-	-	✔	✔	✔	✔	-
[59]	-	-	-	-	-	✔	✔	-	✔	-
[40]	✔	✔	-	✔	-	-	-	✔	-	✔
[44]	✔	-	-	-	-	✔	✔	✔	✔	-
[60]	-	-	-	-	✔	-	-	✔	✔	-
[49, 61]	✔	✔	-	-	-	✔	-	-	✔	-
[62]	✔	-	✔	-	-	-	-	-	✔	-
[63]	-	-	-	-	-	✔	✔	-	✔	-
[64]	-	-	-	-	-	✔	✔	✔	✔	-
[65]	✔	-	-	-	-	-	-	-	-	✔
[45]	✔	✔	-	-	-	✔	✔	✔	✔	-
[46]	✔	-	-	-	-	-	-	-	✔	-
[47]	✔	-	-	-	-	✔	✔	✔	✔	-
[48]	✔	-	-	-	-	✔	-	-	✔	-

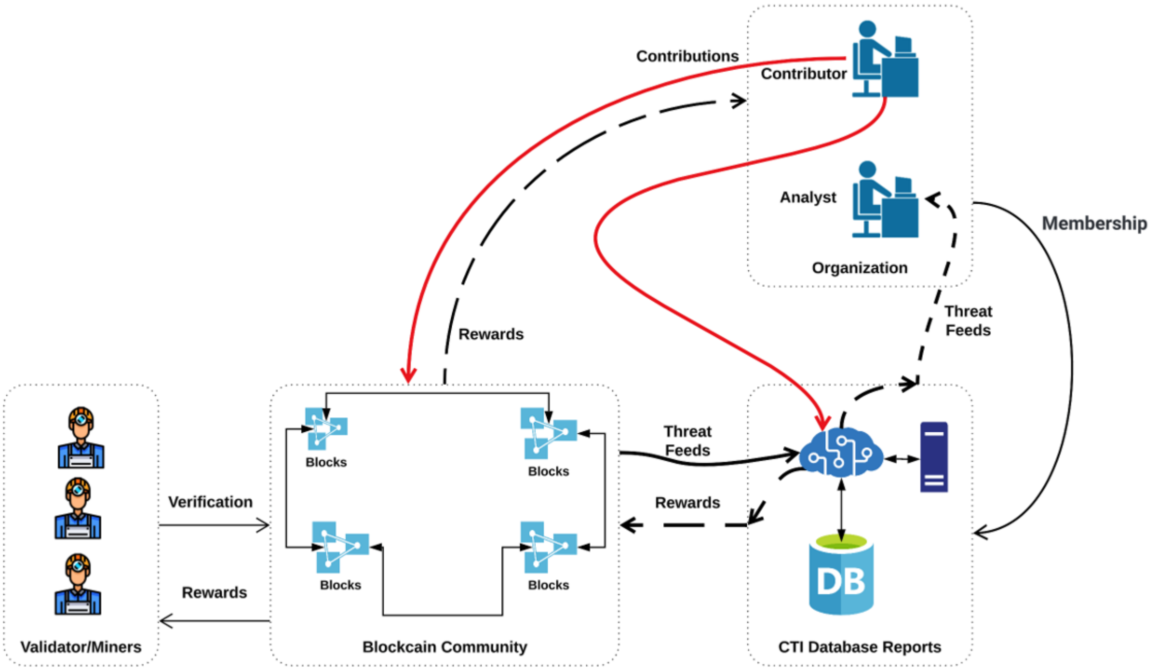


Figure 4. High-level CTI and blockchain diagram

Table 4 summarizes the work done to share attacks' feeds using the blockchain technology. Some of these contributions are based on CTI notification while the others are based on sharing of attacks' feeds without a formal format. As shown in the table, most of the papers mentioned the function of blockchain without describing the methodologies utilized such as: the consensus algorithm, the reward, or the structured threat intelligence sharing language standards. One can conclude from the table that many areas need to be investigated to obtain a solution that could be proposed to incorporate the blockchain into the CTI feeds. Examples of these areas are which consensus algorithm is more suitable for CTI feeds in terms of performance and resources consumption, the way the miners/validators will be rewarded, and which language is more suitable for usage in feeds sharing [50].

5.2 Challenges and limitations

Blockchain is prone to errors and has architectural limitations that may impact threat intel upon integration. Numerous researchers have identified several technical challenges and constraints linked to blockchain, highlighting 5 key challenges associated with its application in CTI [66].

5.2.1 Resources consumption

Consensus protocols like PoW are vital for securing blockchain networks, but they consume significant computing resources, leading to high hardware costs and around $15 million per day in energy expenses [66].

5.2.2 Fork challenges

Forking occurs when a modification needs to be implemented or enforced. There are two types of forks, hard and soft forks. Peers are the main drivers of blockchain. When any modification happens, that modification should be adopted by nodes. Moreover, when nodes are upgraded, they continue to confirm blocks. Although non-upgraded nodes may resume validating blocks, it is called a soft fork, and when non-upgraded nodes cannot resume validating blocks, it is a hard fork. In a hard fork, a crucial issue happens because blockchain is always divided into two different chains and non-upgraded nodes are still on exiting blockchain. Upgraded nodes are transferred to a new blockchain [66].

5.2.3 Sybil attack

A sybil attack targets a blockchain network by undermining its reputation system, where an attacker creates multiple pseudonymous identities to gain disproportionate influence. The term "Sybil" originates from the book Sybil, which details a case of dissociative identity disorder. The concept was introduced by Brian Zill during research at Microsoft [67].

5.2.4 Cost implications

The creation and maintenance of a blockchain system need substantial resources. The financial load could provide significant challenges for enterprises, particularly those of smaller size, because of the necessity for continuous updates and monitoring.

5.2.5 User adoption and education

Users may need to adjust to new procedures and technologies, such as blockchain & CTI systems, which may entail a learning curve. Resistance to change and lack of awareness could hinder widespread adoption.

5.3 Discussion & comparison with other related surveys

In this subsection, we discuss and compare our survey with others in literature. We have selected these surveys based on whether the following factors are mentioned or not: type of consensus, type of structured threat intelligence sharing language standards, type of reward, whether it is based on CTI sharing, and whether previous surveys identified challenges and limitations. References from [68-74] represent recent surveys that discuss the integration of blockchain and CTI. We have chosen these surveys as they discuss the abovementioned factors and are selected from reputable sources such as: Elsevier, Springer, ACM, MDPI, IEEE, and more.

We selected the most recent papers published from the years 2019 to 2023, given that the integration of blockchain and CTI is a new concept and has only recently been discussed in academic community.

In several surveys, including [68-74], the authors discussed CTI sharing using Structured Threat Intelligence Sharing Language Standards. However, they did not specify the type of consensus or reward involved. The surveys [73, 74] discussed consensus and reward in CTI sharing but did not mention the Structured Threat Intelligence Sharing Language Standards. Table 5 shows a comparison between our surveys and references [68-74]. The table demonstrates that our survey encompasses the essential parameters for integrating blockchain and CTI.

Table 5. Comparison with other related surveys

Ref.	Type of Consensus	CTI Sharing	Reward	Structured Threat Intelligence Sharing Language Standards	Challenges and Limitations Identified	Year
[50, 68, 71, 72]	X	✔	X	✔	✔	2023-2024
[75]	✔	✔	✔	X	X	2023
[69]	X	✔	X	✔	X	2019
[76]	✔	✔	✔	X	✔	2020
[70]	X	✔	X	✔	X	2022
[73, 74]	X	✔	X	✔	✔	2021
Our Contribution	✔	✔	✔	✔	✔	2023

From the analysis of Table 5, it is evident that our survey offers a more comprehensive approach to integrating blockchain with CTI compared to previous studies. While many surveys address key components such as CTI sharing and threat intelligence standards, they often overlook essential aspects like consensus mechanisms and reward systems, which are critical for ensuring security, scalability, and participant engagement. Our contribution fills these gaps by examining both PoW and PoS mechanisms, incorporating token-based incentives, and identifying challenges such as privacy and centralization. This comprehensive evaluation establishes our survey as a valuable resource for both future research and practical implementations within the field of blockchain based threat intel.

In contrast, many prior works [68, 69], fail to explore this dimension, leaving a critical gap in understanding how participation in blockchain-based CTI systems can be sustained over time. Moreover, while several earlier surveys mention structured threat intelligence sharing standards like STIX and TAXII, they often do not integrate these standards with consensus mechanisms or reward models. Our contribution is unique in its holistic approach, covering all essential elements: Consensus, rewards, CTI sharing standards, and identified challenges. By addressing these gaps, our work provides a more comprehensive framework for integrating blockchain with CTI, making it an important resource for practitioners.

In conclusion, our survey not only covers the technical aspects neglected in previous works but also identifies future research directions, particularly in improving privacy, scalability, and participation incentives in blockchain-based CTI systems.

6. CONCLUSIONS AND FUTURE WORK

There has been a rise in cybercrime as mobile devices have become increasingly central to daily life. Since cybercriminals frequently alter their practices to circumvent security measures, relying on traditional methods of defense is futile. Since most of these assaults are highly sophisticated, their anatomy and details must be shared once uncovered. CTI is the main method used to share the aforementioned information. There are restrictions with the current threat intel, such as the lack of quality_control, privacy, integrity, non_repudiation, etc. To avoid negative publicity, most organizations would rather receive CTI notifications anonymously. Alternatively, blockchain provides a working example of a distributed database that does not rely on any authority [77]. Blockchain's main advantage is its ability to conceal users' identities and locations. The distributed nature of the blockchain allows records to be replicated across all endpoints. Since every endpoint has a copy of every record in the past, updating them is a tedious process. Given these circumstances, blockchain is the most suitable to use and integrate with the CTI to address and fixing the existing issues. The identity concealment feature of blockchain makes it an ideal solution for privacy issues. Thus, confidentiality is maintained while all members of the CTI network exchange data [78].

For the conventional threat intel method, the organization must examine the report (threat intel notifications). Everything that could compromise privacy, such as names, addresses, and phone numbers, is scrubbed from the database. On the other hand, blockchain shields the entity's identity by keeping it hidden in the distributed ledger; therefore, the systems' repudiation is maintained. A digital signature ensures that the information in the CTI feed has not been tampered with and cannot be disputed. The blockchain's rewards system will ensure its continued high quality by incentivizing its participants to share and review the reports of their counterparts.

In this paper, one of the key challenges addressed in this paper is the practical implementation of the integration between blockchain technology and CTI. While many contributions have explored the conceptual aspects, few have delved into the methods and practical applications. As illustrated in the paper, there is a notable lack of comprehensive studies and research specifically addressing the integration of blockchain with CTI. None of the surveyed literature provides a detailed framework or model that thoroughly discusses this integration. We conclude that merging these two fields is inherently difficult due to the distinct technologies. Moreover, applying this integration across various sectors presents additional challenges. A blockchain design tailored for the education sector will differ significantly from one used in health insurance or finance. Critical blockchain components, such as reward systems and consensus mechanisms, must be established before designing the network. The reward system incentivizes consistent, high quality information sharing, while the consensus mechanism affects both network efficiency and energy consumption. Furthermore, the consensus type determines the validation approach used within the system. Although blockchain resolves many of the issues that have historically affected traditional CTI systems, integrating both technologies introduce new challenges, including forking and latency issues. The resource consumption required for mining or validation, coupled with the numerous hash calculations, poses a significant problem for both the CTI network and blockchain nodes. Additionally, Sybil attacks could compromise the quality of CTI feeds by manipulating the blockchain's reward system. Hence, future research should prioritize the development of countermeasures to effectively tackle these emerging challenges. Our survey proposed strategy aim to bridge this gap by offering a more detailed discussion of blockchain's integration with CTI, proposing a framework that addresses these challenges comprehensively.

Future research in blockchain based CTI systems must prioritize developing methods to address the current challenges, such as: sybil attacks, 51% attack, double spending, and resource consumption. The researchers could investigate the use of hybrid consensus algorithm to solve the abovementioned problems. Also, using AI over the CTI and blockchain integration will help detect threats and write the report correctly.

REFERENCES

[1] Alam, M.T., Bhusal, D., Park, Y., Rastogi, N. (2023). Looking beyond IoCs: Automatically extracting attack patterns from external CTI. In Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses, Hong Kong, China, pp. 92-108. https://doi.org/10.1145/3607199.3607208

[2] Kure, H.I., Islam, S., Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 34(18): 15241-15271. https://doi.org/10.1007/s00521-022-06959-2

[3] Marchiori, F., Conti, M., Verde, N.V. (2023). Stixnet: A novel and modular solution for extracting all stix objects in CTI reports. In Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy, pp. 1-11.

https://doi.org/10.48550/arXiv.2303.09999

[4] Couretas, J.M. (2022). Cyber analysis and targeting. In An Introduction to Cyber Analysis and Targeting, Springer International Publishing, 1-12. https://doi.org/10.1007/978-3-030-88559-5_1

[5] Kotsias, J., Ahmad, A., Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems, 32(1): 35-51. https://doi.org/10.1080/0960085X.2022.2088414

[6] Mallikarjunaradhya, V., Pothukuchi, A.S., Kota, L.V. (2023). An overview of the strategic advantages of AI-powered threat intelligence in the cloud. Journal of Science & Technology, 4(4): 1-12. https://doi.org/10.55662/JST.2023.4401

[7] Papanikolaou, A., Alevizopoulos, A., Ilioudis, C., Demertzis, K., Rantos, K. (2023). A blockchained automl network traffic analyzer to industrial cyber defense and protection. Electronics, 12(6): 1484. https://doi.org/10.3390/electronics12061484

[8] Li, Z.X., Li, Y.J., Liu, Y.W., Liu, C., Zhou, N.X. (2023). K-CTIAA: Automatic analysis of Cyber Threat Intelligence based on a knowledge graph. Symmetry, 15(2): 337. https://doi.org/10.3390/sym15020337

[9] Coulter, R., Zhang, J., Pan, L., Xiang, Y. (2022). Domain adaptation for windows advanced persistent threat detection. Computers & Security, 112: 102496. https://doi.org/10.1016/j.cose.2021.102496

[10] Caballero, J., Gomez, G., Matic, S., Sánchez, G., Sebastián, S., Villacañas, A. (2023). The rise of GoodFATR: A novel accuracy comparison methodology for indicator extraction tools. Future Generation Computer Systems, 144: 74-89. https://doi.org/10.1016/j.future.2023.02.012

[11] Shi, H., Wang, W., Liu, L., Lin, Y., Liu, P., Xie, W., Zhang, Y. (2022). Threat intelligence sharing model and profit distribution based on blockchain and smart contracts. In Proceedings of the 11th International Conference on Computer Engineering and Networks, 645-654. https://doi.org/10.1007/978-981-16-6554-7_70

[12] Borges Amaro, L.J., Percilio Azevedo, B.W., Lopes de Mendonca, F.L., Giozza, W.F., Albuquerque, R.D.O., García Villalba, L.J. (2022). Methodological framework to collect, process, analyze and visualize Cyber Threat Intelligence data. Applied Sciences, 12(3): 1205. https://doi.org/10.3390/app12031205

[13] El Bekkali, A., Essaaidi, M., Boulmalf, M. (2023). A blockchain-based architecture and framework for cybersecure smart cities. IEEE Access, 11: 76359-76370. https://doi.org/10.1109/ACCESS.2023.3296482

[14] Barnum, S. (2012). Standardizing Cyber Threat Intelligence information with the structured threat information expression (STIX). Mitre Corporation, 11: 1-22.

[15] Danyliw, R., Meijer, J., Demchenko, Y. (2007). The incident object description exchange format (No. rfc5070). https://www.rfc-editor.org/rfc/rfc5070.html.

[16] Abzakh, A., Alkhatib, A.A., Rabayah, O., Elmanaseer, S., Albustanji, R.N., Almadi, N. (2023). A survey: Threat hunting for the OT systems. In 2023 International Conference on Information Technology (ICIT), Amman, Jordan, pp. 130-134. https://doi.org/10.1109/ICIT58056.2023.10225758

[17] Özdemir, A. (2021). Cyber Threat Intelligence sharing technologies and threat sharing model using Blockchain. Master's thesis, Middle East Technical University.

[18] Negi, C.S., Kumari, N., Kumar, P., Sinha, S.K. (2021). An approach for alert correlation using ArcSight SIEM and Open Source NIDS. In Proceeding of Fifth International Conference on Microelectronics, Computing and Communication Systems: MCCS 2020, pp. 29-40. https://doi.org/10.1007/978-981-16-0275-7_3

[19] Blinowski, G.J., Piotrowski, P. (2020). CVE based classification of vulnerable IoT systems. In Theory and Applications of Dependable Computer Systems: Proceedings of the Fifteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, Brunów, Poland, pp. 82-93. https://doi.org/10.1007/978-3-030-48256-5_9

[20] Galhardo, C.C., Mell, P., Bojanova, I., Gueye, A. (2020). Measurements of the most significant software security weaknesses. In Proceedings of the 36th Annual Computer Security Applications Conference, New York, NY, United States, pp. 154-164. https://doi.org/10.1145/3427228.3427257

[21] Schlette, D., Menges, F., Baumer, T., Pernul, G. (2020). Security enumerations for cyber-physical systems. In Data and Applications Security and Privacy XXXIV: 34th Annual IFIP WG 11.3 Conference, DBSec 2020, Regensburg, Germany, pp. 64-76. https://doi.org/10.1007/978-3-030-49669-2_4

[22] Ushakov, R., Doynikova, E., Novikova, E., Kotenko, I. (2021). CPE and CVE based technique for software security risk assessment. In 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, pp. 353-356. https://doi.org/10.1109/IDAACS53288.2021.9660968

[23] Rostami, S., Kleszcz, A., Dimanov, D., Katos, V. (2020). A machine learning approach to dataset imputation for software vulnerabilities. In Multimedia Communications, Services and Security: 10th International Conference, MCSS 2020, Kraków, Poland, pp. 25-36. https://doi.org/10.1007/978-3-030-59000-0_3

[24] Guo, L., Wen, S., Wang, D., Wang, S., Wang, Q., Liu, H. (2021). Overview of Cyber Threat Intelligence description. In International Conference on Applications and Techniques in Cyber Security and Intelligence, pp. 343-350. https://doi.org/10.1007/978-3-030-79200-8_50

[25] Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. Applied Research in Artificial Intelligence and Cloud Computing, 6(8): 1-21.

[26] Prieto, Y., Figueroa, M., Pezoa, J.E. (2021). Maximizing network reliability to 0-day exploits through a heterogeneous node migration strategy. IEEE Access, 9: 97747-97759. https://doi.org/10.1109/ACCESS.2021.3095149

[27] Alkhadra, R., Abuzaid, J., AlShammari, M., Mohammad, N. (2021). Solar winds hack: In-depth analysis and countermeasures. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, pp. 1-7. https://doi.org/10.1109/ICCCNT51525.2021.9579611

[28] Hayes, K. (2021). Ransomware: A growing geopolitical threat. Network Security, 2021(8): 11-13. https://doi.org/10.1016/S1353-4858(21)00089-1

[29] Staves, A., Balderstone, H., Green, B., Gouglidis, A.,

Hutchison, D. (2020). A framework to support ICS cyber incident response and recovery. In ISCRAM, USA, pp. 638-651.

[30] Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review. IEEE Access, 8: 79764-79800. https://doi.org/10.1109/ACCESS.2020.2988579

[31] von Wangenheim, G. (2020). Blockchain-based land registers: A law-and-economics perspective. Disruptive Technology, Legal Innovation, and the Future of Real Estate, pp. 103-122. https://doi.org/10.1007/978-3-030-52387-9_6

[32] Saxena, S., Bhushan, B., Ahad, M.A. (2021). Blockchain based solutions to secure IoT: Background, integration trends and a way forward. Journal of Network and Computer Applications, 181: 103050. https://doi.org/10.1016/j.jnca.2021.103050

[33] Tanrıverdi, M. (2020). A systematic review of privacy-preserving healthcare data sharing on blockchain. International Journal of Information Management, 5(2 SI 1): 31-37. https://doi.org/10.5281/zenodo.4014251

[34] Mollah, M.B., Zhao, J., Niyato, D., Lam, K.Y., Zhang, X., Ghias, A.M., Yang, L. (2020). Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things Journal, 8(1): 18-43. https://doi.org/10.1109/JIOT.2020.2993601

[35] Caceres, C.P.P., Martinez, J.V.B., Pérez, F.M., Fonseca, I.L., Martinez, M.E.A. (2023). Blockchain architecture based on decentralised PoW algorithm. International Journal of Advanced Computer Science and Applications, 14(7): 697-705.

[36] Nazir, A., He, J., Zhu, N., Wajahat, A., Ullah, F., Qureshi, S., Pathan, M.S. (2024). Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration. Journal of King Saud University-Computer and Information Sciences, 36(2): 101939. https://doi.org/10.1016/j.jksuci.2024.101939

[37] Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., Li, Y. (2020). Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digital Communications and Networks, 6(4): 480-485. https://doi.org/10.1016/j.dcan.2019.12.001

[38] Saleh, F. (2021). Blockchain without waste: Proof-of-stake. The Review of Financial Studies, 34(3): 1156-1190. https://doi.org/10.1093/rfs/hhaa075

[39] Chatzigiannis, P., Chalkias, K. (2021). Proof of assets in the diem blockchain. In Applied Cryptography and Network Security Workshops: ACNS 2021 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA, Kamakura, Japan, pp. 27-41. https://doi.org/10.1007/978-3-030-81645-2_3

[40] Si, H., Sun, C., Li, Y., Qiao, H., Shi, L. (2019). IoT information sharing security mechanism based on blockchain technology. Future Generation Computer Systems, 101: 1028-1040.

[41] Riesco, R., Larriva-Novo, X., Villagrá, V.A. (2020). Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and Smart contracts to foster the cyber threat and risk intelligence exchange of information. Telecommunication Systems, 73(2): 259-288. https://doi.org/10.1007/s11235-019-00613-4

[42] Tanrıverdi, M., Tekerek, A. (2019). Implementation of blockchain based distributed web attack detection application. In 2019 1st International Informatics and Software Engineering Conference (UBMYK), Ankara, Turkey, pp. 1-6. https://doi.org/10.1109/UBMYK48245.2019.8965446

[43] Cha, J., Singh, S.K., Pan, Y., Park, J.H. (2020). Blockchain-based Cyber Threat Intelligence system architecture for sustainable computing. Sustainability, 12(16): 6401. https://doi.org/10.3390/su12166401

[44] Gong, S., Lee, C. (2020). Blocis: Blockchain-based Cyber Threat Intelligence sharing framework for sybil-resistance. Electronics, 9(3): 521. https://doi.org/10.3390/electronics9030521

[45] Dunnett, K., Pal, S., Jadidi, Z. (2022). Challenges and opportunities of blockchain for Cyber Threat Intelligence sharing. Secure and Trusted Cyber Physical Systems: Recent Approaches and Future Directions, 43: 1-24. https://doi.org/10.1007/978-3-031-08270-2_1

[46] Khalil, U., Malik, O.A., Hussain, S. (2022). A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. IEEE Access, 10: 76805-76823. https://doi.org/10.1109/ACCESS.2022.3189998

[47] Jiang, T., Shen, G., Guo, C., Cui, Y., Xie, B. (2023). BFLS: Blockchain and Federated Learning for sharing threat detection models as Cyber Threat Intelligence. Computer Networks, 224: 109604. https://doi.org/10.1016/j.comnet.2023.109604

[48] Chatziamanetoglou, D., Rantos, K. (2023). Blockchain-based Cyber Threat Intelligence sharing using proof-of-quality consensus. Security and Communication Networks, 2023(1): 3303122. https://doi.org/10.1155/2023/3303122

[49] Dunnett, K., Pal, S., Jadidi, Z., Jurdak, R. (2023). A blockchain-based framework for scalable and trustless delegation of Cyber Threat Intelligence. In 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dubai, United Arab Emirates, pp. 1-9. https://doi.org/10.1109/ICBC56567.2023.10174885

[50] Venčkauskas, A., Jusas, V., Barisas, D., Misnevs, B. (2024). Blockchain-based model for Incentivized Cyber Threat Intelligence sharing. Applied Sciences, 14(16): 6872. https://doi.org/10.3390/app14166872

[51] Aljihani, H., Eassa, F., Almarhabi, K., Algarni, A., Attaallah, A. (2021). Standalone behaviour-based attack detection techniques for distributed software systems via Blockchain. Applied Sciences, 11(12): 5685. https://doi.org/10.3390/app11125685

[52] Guha Roy, D., Srirama, S.N. (2021). A blockchain-based cyber attack detection scheme for decentralized internet of things using software-defined network. Software: Practice and Experience, 51(7): 1540-1556. https://doi.org/10.1002/spe.2972

[53] Gadekallu, T.R., Manoj, M.K., Kumar, N., Hakak, S., Bhattacharya, S. (2021). Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications. IEEE Internet of Things Magazine, 4(3): 30-33. https://doi.org/10.1109/IOTM.1021.2000160

[54] Rathore, S., Kwon, B.W., Park, J.H. (2019). BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. Journal of Network and Computer Applications, 143: 167-177.

https://doi.org/10.1016/j.jnca.2019.06.019

[55] Putz, B., Pernul, G. (2020). Detecting blockchain security threats. In 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, pp. 313-320. https://doi.org/10.1109/Blockchain50366.2020.00046

[56] Suhail, S., Jurdak, R. (2021). Towards trusted and intelligent cyber-physical systems: A security-by-design approach. arXiv preprint arXiv:2105.08886.

[57] Banerjee, M., Lee, J., Choo, K.K.R. (2018). A blockchain future for internet of things security: A position paper. Digital Communications and Networks, 4(3): 149-160. https://doi.org/10.1016/j.dcan.2017.10.006

[58] Homayoun, S., Dehghantanha, A., Parizi, R.M., Choo, K.K.R. (2019). A blockchain-based framework for detecting malicious mobile applications in app stores. In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, pp. 1-4. https://doi.org/10.1109/CCECE.2019.8861782

[59] Smys, S., Haoxiang, W. (2021). Data elimination on repetition using a blockchain based Cyber Threat Intelligence. IRO Journal on Sustainable Wireless Systems, 2(4): 149-154. https://doi.org/10.36548/jsws.2020.4.002

[60] Wu, Y., Qiao, Y., Ye, Y., Lee, B. (2019). 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), Granada, Spain, pp. 474-481. https://doi.org/10.1109/IOTSMS48152.2019.8939192

[61] Hajizadeh, M., Afraz, N., Ruffini, M., Bauschert, T. (2020). Collaborative cyber attack defense in SDN networks using blockchain technology. In 2020 6th IEEE Conference on Network Softwarization (NetSoft), pp. 487-492. https://doi.org/10.1109/NetSoft48620.2020.9165396

[62] Mendez Mena, D., Yang, B. (2020). Decentralized actionable Cyber Threat Intelligence for networks and the internet of things. IoT, 2(1): 1-16. https://doi.org/10.3390/iot2010001

[63] Allouche, Y., Tapas, N., Longo, F., Shabtai, A., Wolfsthal, Y. (2021). Trade: Trusted anonymous data exchange: Threat sharing using blockchain technology. arXiv preprint arXiv:2103.13158.

[64] He, S., Fu, J., Jiang, W., Cheng, Y., Chen, J., Guo, Z. (2020). Blotisrt: Blockchain-based threat intelligence sharing and rating technology. In Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies, United States, pp. 524-534. https://doi.org/10.1145/3444370.3444623

[65] Falco, G., Li, C., Fedorov, P., Caldera, C., Arora, R., Jackson, K. (2019). Neuromesh: IoT security enabled by a blockchain powered botnet vaccine. In Proceedings of the International Conference on Omni-Layer Intelligent Systems, Crete Greece, pp. 1-6. https://doi.org/10.1145/3312614.3312615

[66] Khan, F.A., Asif, M., Ahmad, A., Alharbi, M., Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. Sustainable Cities and Society, 55: 102018. https://doi.org/10.1016/j.scs.2020.102018

[67] Douceur, J.R. (2002). The sybil attack. Peer-To-Peer Systems: First International Workshop, Iptps 2002, Cambridge, Ma, USA. https://doi.org/10.1007/3-540-45748-8_24

[68] Arazzi, M., Arikkat, D.R., Nicolazzo, S., Nocera, A., Conti, M. (2023). NLP-based techniques for Cyber Threat Intelligence. arXiv preprint arXiv:2311.08807. https://doi.org/10.48550/arXiv.2311.08807

[69] Homan, D., Shiel, I., Thorpe, C. (2019). A new network model for Cyber Threat Intelligence sharing using blockchain technology. In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, pp. 1-6. https://doi.org/10.1109/NTMS.2019.8763853

[70] Deshmukh, A., Sreenath, N., Tyagi, A.K., Abhichandan, U.V.E. (2022). Blockchain enabled cyber security: A comprehensive survey. In 2022 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, pp. 1-6. https://doi.org/10.1109/ICCCI54379.2022.9740843

[71] Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., Zhang, J. (2023). Cyber Threat Intelligence mining for proactive cybersecurity defense: A survey and new perspectives. IEEE Communications Surveys & Tutorials, 25(3): 1748-1774. https://doi.org/10.1109/COMST.2023.3273282

[72] Rahman, M.R., Hezaveh, R.M., Williams, L. (2023). What are the attackers doing now? Automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey. ACM Computing Surveys, 55(12): 1-36. https://doi.org/10.1145/3571726

[73] Basheer, R., Alkhatib, B. (2021). Threats from the dark: A review over dark web investigation research for Cyber Threat Intelligence. Journal of Computer Networks and Communications, 2021(1): 1302999. https://doi.org/10.1155/2021/1302999

[74] Sauerwein, C., Fischer, D., Rubsamen, M., Rosenberger, G., Stelzer, D., Breu, R. (2021). From threat data to actionable intelligence: An exploratory analysis of the intelligence cycle implementation in Cyber Threat Intelligence sharing platforms. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna Austria, pp. 1-9. https://doi.org/10.1145/3465481.3470048

[75] ElMamy, S.B., Mrabet, H., Gharbi, H., Jemai, A., Trentesaux, D. (2020). A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0. Sustainability, 12(21): 9179. https://doi.org/10.3390/su12219179

[76] Rathore, H., Mohamed, A., Guizani, M. (2020). A survey of blockchain enabled cyber-physical systems. Sensors, 20(1): 282. https://doi.org/10.3390/s20010282

[77] El-Kosairy, A., Abdelbaki, N., Aslan, H. (2023). A survey on Cyber Threat Intelligence sharing based on Blockchain. Advances in Computational Intelligence, 3(3): 10. https://doi.org/10.1007/s43674-023-00057-z

[78] Sharad Mangrulkar, R., Vijay Chavan, P. (2024). Bitcoin. In Blockchain Essentials: Core Concepts and Implementations, Berkeley, CA, 83-121. https://doi.org/10.1007/978-1-4842-9975-3_3