Security Issues in Cyber Threat Intelligence Exchange: A Review

Moses Olaifa[1(✉)], Joey Jansen van Vuuren[1], Deon Du Plessis[1], and Louise Leenen[2]

[1] Department of Computer Science, Faculty of ICT, Tshwane University of Technology, Pretoria, South Africa
{olaifamo,jansenvanvuurenjc,duplessisdp}@tut.ac.za
[2] Department of Computer Science Programme, Faculty of Natural Science, University of Western Cape, Cape Town, South Africa
lleenen@uwc.ac.za

Abstract. The cost and time required by individual organizations to build an effective cyber defence can become overwhelming with the growing number of cyber attacks. Hence, the introduction of platforms that encourage collaborative effort in the fight against cyber attacks is considered advantageous. However, the acceptability and efficiency of the CTI exchange platforms is massively challenged by lack of trust caused by security issues encountered in such communities. This review examines the security and participation cost issues revolving around the willingness of participants to either join or actively participate in CTI exchange communities and proposed solutions to the security issues from the research perspective.

Keywords: Cyber Threat Intelligence · Cyber Defence · Threat Exchange Platforms · Cyber Attacks

1 Introduction

A major challenge faced by different organizations in this age and time is the security of systems and the information contained on these systems against attacks. There have been an increase in the number of attacks and an advancement in the ways the attacks are carried out. In the event that an attack succeeds, the effect on the operations and productivity of an organization can be severe and recovery after such attacks may be highly challenging. In view of this problem, there is a need for the implementation of measures to prevent or mitigate the effect of such attacks, manage system vulnerabilities and other cyber related incidents [1]. Achieving this will involve the collection and evaluation of information related to the threats or attacks. The threat information require proper analysis in order to produce meaningful information that can be useful for both proactive and reactive defence against future attacks.

However, with the rate of increase in the number of attacks and threats, it may become difficult for a single organization to effectively generate,

K. Arai (Ed.): SAI 2023, LNNS 739, pp. 1308–1319, 2023.
https://doi.org/10.1007/978-3-031-37963-5_89

analyze and manage all the necessary information needed to prevent future attacks. Hence the need for inter-organizational collaboration in the quest to building a powerful and capable system against threats and attacks. This need led to the emergence of different standards and platforms that enable collaborative effort in the collection, analysis and exchange of threat information that can be used by various levels of organizations to tackle cyber-threats. Furthermore, different terms and concepts such as cyber threat intelligence (CTI) sharing, threat intelligence sharing platform (TISP), cyber threat information sharing (CTIS) among others, have emerged from the different inter-organizational activities. These terms generally describe activities involving gathering, analyzing, evaluation and exchange of information related to possible threats and attacks with the intention of using this information to prevent or mitigate future cyber attacks. Generally, the benefits derived from CTI exchange can be summarized into two categories: lower cost of investing in alternative security and stronger resistance to cyber-attacks [2,3]. The cost can be in terms of the price paid or time invested in preventing or recovering from an attack.

In order to enhance the inter-organizational collaboration, a number of infrastructure, platforms and standards are evolving such as Cybersecurity Information Exchange Framework (CYBEX) [4], Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) [1]. This enables a collective approach involving different organizations to identify cyber threat activities and take prompt actions to defend against such activities through the exchange of intelligence on attacks and the perpetrators [5]. Beyond the exchange of CTI, these standards and platforms enables CTI expression, provide tools for analysis and evaluation, provide various services for sharing CTI, flagging of threat signature and real-time security monitoring. However, the suitability of such platforms and standards depend on how well the organizational information needs are satisfied and the practices uphold their values.

As much as many organizations (entities) support the idea of a collaborative effort to cyber defence against these malicious activities, literature has revealed different issues preventing the actual involvement of most organizations in utilizing such existing systems. Some of such issues include the lack of framework for exchange and widely accepted standards for sharing without significant manual intervention [6,7]; the fear of possible damage to organizations reputation in case leakage of sensitive information [8]; trust boundaries among participants among others.

Some of the review works in the area of cyber threat intelligence are focused on software vendors, general issues and challenges, information sharing, benefits and barriers, standards, threat concepts [9–14]. However, to the best of our knowledge, no review has delved into the aspect of security issues associated with CTI sharing and efforts made within the research community to address these issues.

In this study, we conduct a review of literature with a focus on different security issues related to cyber threat intelligence exchange platforms and the solutions proffered from the research perspective. This study to some extent presents the categories of these security issues and the level of research carried

out to address the issues so far. Thereby providing a solid ground for further research in the area of security in CTI exchange platforms. The remainder of this paper are organized as follows: Sect. 2 discusses the three broad categories of CTI exchange security issues and proposed solutions. Section 3 examines the issue around participation costs and incentives as a motivation for participation. The final section concludes the study.

2 CTI Security Issues

This section examines the different security issues identified in literature and categorized them into three major parts of source protection, secure exchange and malicious participants issues. Furthermore, efforts made to address the identified issues in literature will be examined from a research perspective.

2.1 Privacy Preservation Issues

Organizations can benefit immensely when gathered threat data are transformed into useful intelligence through CTIs are used to make informed security decisions [15]. However, different CTI producers still have reservations about CTI communities due to the possibility of associating shared information with the source. This in many ways can be exploited and maliciously used to the detriment of such sources. As a result, consideration of privacy preservation of CTI sources is of utmost importance in the development of intelligence exchange platforms. Granting access to shared intelligence through the use of access control techniques does not only restrict access to trusted parties but also control access to different part of an intelligence. In an earlier attempt, the Cybersecurity and Infrastructure Security Agency (CISA) created the Traffic Light Protocol (TLP) that assign designations to determine the sensitivity of intelligence shared within communities [16]. Using four different colours; red, amber, green and white, the protocol defines four different levels of information disclosure for different receiving audience.

Through the use of cryptographic approach, [17] proposed two complementary solutions to address the privacy issue in sharing and sightings. Initially, the sensitive content of shared Intelligence are hidden by using a cryptographic hash function. To strengthen the protection of the sensitive contents, a randomly selected non-secret salt can be applied for each of the intelligence. Sharing a similar view on honest-but-curious participants, [18] presented a solution called TATIS, to protect APIs for CTI exchange platforms. This solution is based on User Managed Access (UMA) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE).

Access control methods can be effective in fully trusted sharing servers. In semi-trusted sharing environments however, there may be need for tighter security protocols for privacy preservation. To provide a more effective approach in semi-trusted environments, [19] addressed access control problem in Cybersecurity Information Exchange (CYBEX). The study modeled an attribute based

access control using simple multi-authority cipher-text policy attribute encryption (CP-ABE). Attribute authorities present users with their attributes that is to determine decryption keys that will be provided by the key generation centre. Recipients can only decrypt the cypertext if the assigned attributes satisfy the cypertext attributes.

Signing of Non-Disclosure Agreement by parties involved in a sharing community enforces a level of privacy preservation within the community. This is considered effective in communities with known and trusted members. This is far fetched in a CTI exchange environment with a realistic number of non-cooperating or rival parties. An aggregatable blind signature utilizing BBS+ signature scheme to address privacy issue is presented in [20]. This approach provides a group private key to every participant who registered with the system. The participant shares a CTI with the community via a server after sanitizing and appending signature to the message using the group private key. The message is anonymously published after the server has verified both the signature and validity of the intelligence. This prevents exposure of intelligence sources in the community.

In [21], an anonymity supported CTI exchange platform to preserve the privacy of intelligence sources is designed. Using regular expressions in Java, sensitive details in the submitted intelligence are masked. Masking intelligence valuable information in the message is avoided by implementing exceptions to Java regular expressions. To strengthen intelligence source anonymity, the connection is tunneled through a TOR network to hide the path.

CTI exchange activities sometimes include collaborative use of learning tools in addition to sharing of intelligence. Such collaborative activities should be possible without divulging or leaking identity and other sensitive information about involved parties. The study [22] proposed a privacy preserving framework that supports collaborative CTI exchange and learning activities for organizations to learn and strengthen their cyber defense. This framework is based on homomorphic encryption using the ElGamal crypto system for privacy preservation and decision tree that enables organizations to learn the universal decision tree while privacy is preserved.

Some other studies [23–25] proposed the use of blockchain technology in preservation of privacy. While sending intelligence within such blockchain based platforms, sensitive or privacy information is either removed or intelligence is anonymized.

2.2 Data Integrity - Secure Information Exchange Issues

Inor sensitive interception of intelligence by unauthorized parties is another security and privacy issue confronting CTI exchange platforms. In the cause of disseminating CTI, the information can be intercepted and tampered with before it reaches the recipients [26]. Due to the sensitive nature of CTI information, the reputation of an organization can be negatively impacted if such information is intercepted by untrusted parties or leaked to unauthorized parties.

One of the methods adopted in dealing with CTI exchange issues is the blockchain technology. This may not be unconnected with the immutable nature of this technology that

Homan et al [28] proposed a blockchain network model that can help to realize a secure exchange of cybersecurity information in CTI exchange environments. Based on Hyperledger Fabric open-source blockchain specification and tools, the study designed a model for CTI exchange. Using the Fabric's channel features, smaller and trusted communities of entities are created from the larger community and this enables the exchange of highly sensitive intelligence within these smaller communities while still part of the larger community. In addition, Fabric's smart contracts are used to ensure CTI producers are protected from sharing intelligence with unauthorized entities.

In addition to intelligence tampering during exchange, [26] indicates the lack of feedback mechanism as an issue that posses a threat to the quality of intelligence exchanged. The study presented a blockchain based threat intelligence sharing and rating system model, BloTISRST. The model is built into API, function, protocol and resource layers. The resource layer contains entity nodes that define different intelligent providers who are allowed to submit intelligence that is subsequently captured within the blockchain. In terms of quality of intelligence, the credibility and contribution rate of each intelligence producer is computed using an automated process based on smart contracts.

Similar to [26], DEALER [27] presents a decentralized platform for sharing cyber threat intelligence information based on EOS blockchain and IPFS distributed hash table. This model enables the fulfilment of legal reporting obligations and provides incentives to participants involved in CTI exchange. However, both models utilized permissionless blockchain platforms which are not suitable for environment with highly sensitive information exchange. For CTI sharing in sensitive environments like Industrial Control Systems (ICS), [29] proposed a blockchain based intelligence exchange in ICS. Like the BloTISRST and DEALER, this framework provides incentives to willing participants in the exchange of CTI. As opposed to the permissionless platforms used in both, this study adopted the hyperledger Fabric, a permissioned private blockchain platform to ensure authentication and unique identification of participants and smart contract chain codes to facilitate privacy in intelligence dissemination within smaller communities of participants.

PRACIS, a protocol based on Format-preserving and homomorphic technique used to facilitate secure cybersecurity information sharing in insecure infrastructure platforms is proposed in [30]. The protocol leverages on the ability of the homomorphic encryption scheme to prevent parties without the key to retrieve the original plaintext from the initially generated ciphertexts. Moreover, some arithmetic operations can be performed on the ciphertexts to generate various changes to the initial plaintexts. Similar to [34] PRACIS targets semi-trusted message exchange middlewares, however it intended to guarantee the exchange of intelligence without the infrastructure deducing any sensitive content from the shared message.

Using the blockchain model, [31] presented an enhanced approach to secure exchange of CTI within participating entities. In addition, the study indicates that timely access to required intelligence for effective response is a challenge due to the large volume of data feed. The study adopted the Hyperledger Fabric platform of the Distributed Ledger Technology to build a fast and secured CTI exchange platform with a means of verifying the users' configuration and permission to interact with the ledger (send or receive CTI). In addition, a security layer that requires a client's username and password is included. This prevents unauthorized users from modifying the data in the ledger.

In [32], the authors introduced data associated risk level approach for the exchange of threat situation awareness information among organizations. CTI contains sensitive information about an organization and if intercepted by unauthorized parties or maliciously used by the consumer, it can threaten the security of the producer's business. To address this issue, the study introduced a model for sharing classified information by defining a minimum risk model for CTI exchange. Using the same scale, each organization is expected to define its risk levels based on the information to be shared and the type of connected organization. Since higher risk level indicates higher security risk, exchange of cyber security information between two organizations requires the discovery of lower risk level organizations through which the exchange will be realized. This problem situation is redefined as a graph problem where the exchange of information between sharing organizations is considered as finding the shortest path problem with the minimum risk exchange path calculated using Dijkstra's algorithm.

Data integrity assurance and appropriateness for event driven architecture (real-time propagation) of TAXII are some of the challenges of CTI platforms address in [33]. The authors indicated the deficiency of TAXII in authenticating CTI data shared on CTI exchange platforms. As presented in the study, the TAXII framework is enhanced to address security and real-time application deficiencies by incorporating the Distributed Ledger Technologies. This is due to the immutable audit trail of the ledger content which ensures a tamper-proof exchange between CTI producers and consumers. The framework is divided into three components responsible for providing TAXII support for both producers and consumers; providing accessibility to end points for the exchange of CTI between producers and consumers; facilitating real-time propagation of CTI data respectively.

2.3 Malicious Versus Legitimate Participants

Majority of the studies reviewed in previous sessions are based on the assumption that all participants in a CTI community are regular participants. They define a more generic abstraction of always rational and benefit-driven organizations [35]. In a realistic setup however, CTI exchanging communities might involve legitimate parties and opposing parties such as competing or rival organizations (malicious participants) with the intention to use the shared intelligence to launch attacks against other participants. There are possibilities that the

producer of a threat information may have other motives than sharing intelligence for collaborative effort to fight against cyber attack. Intelligence received from such devious sources may cause unprecedented damage or harm to the consumers. Thereby, compromising the security of the consumer or all end-points connected with the intelligence community. On the other hand, these malicious participants may provide false intelligence to distract or weaken intelligence build up in the communities. This can negatively impact the regular (legitimate) participating organizations and subsequently discredit the platform.

In an attempt to address some of the mentioned issues, [41] proposes a distributed security framework to address trust issues with cyber threat intelligence sources within the CTI communities. The concerned level is the incident response team. This study focused on addressing issues around the provisioning of malicious intelligence by malicious participants which may compromise or harm the recipients. This work enhances the TATIS security framework using the potentials of MultiChain distributed ledger by scrutinizing the sources of threat intelligence within a sharing community.

The authors in [42] indicated that most existing CTI platforms lack the capacity to adequately exchange incident data with other systems in a standard format and the capability to measure the efficacy of the sources of CTI data. The study proposed an enhanced CTI framework based on a three layered approach that handle input, pre-processing and detailed reporting respectively. In the first layer, malicious and non-malicious threat data are collected from different sources and stored. These data is fed into the second layer for pre-processing, classification and filtering using machine learning techniques in feature engineering, gradient boosting (Xgboost) ensembling and semi-supervised learning. This layer enables the extraction of features that drives the classification of different malicious threats. The third layer is responsible for the management of threats, reporting and threat solutions.

3 Participants' Inducement, Incentives and Participation Cost Issues

A large number of organizations stand to benefit from shared intelligence provided in a CTI exchange community in that, timely access to adequate and accurate intelligence information can foster the development of efficient defence strategies and systems. Determining the commitment of participants may be difficult as some participants consistently disseminate valuable intelligence to the community, while others take advantage by free-riding without any attempt to give anything in return for the shared information. Introducing a participation cost or incentive can be a motivation to active entities and prohibition to entities that would rather utilize than share intelligence. However, if the participation cost and incentives are not properly set, entities may be discouraged from participating but rather seek for cheaper alternatives.

The research [34] argues that it is only worthy to impose a participation cost on participants of a CTI community since such intelligence can be used

to improve the security of the participating organizations. In this study, a 3-way game model is proposed with three players, CYBEX, organizations and attackers. CYBEX determines the right incentives deserved by the organizations based on the intelligence shared with the community, the goal of the attacker is to maximize the effect of the attack, the organization aims to identify an optimal sanitization rate to reduce their privacy cost.

Even though inter-organizational collaboration in CTI exchange in-arguably positions participants to better create strong cyber defense. However, high cost of participation, lack of trust and other issues deter organizations from participating or rather sharing valuable intelligence information. Hence, a form of inducement can effectively motivate the participation of reluctant organizations. In their study, [35] indicate the need for devising a mechanism to motivate organizations to participate and share valuable CTI in a highly competitive and non-cooperating environment. To achieve this, non-cooperative CTI sharing game is formulated to motivate participants and also generate revenue to maintain the platform. Using the evolutionary game theoretic strategy, the game is analyzed to determine what conditions a player's self-motivated evolutionary stability can be realized. For different possible conditions, a distributed learning heuristic is presented to determine appropriate evolutionary stable strategy (ESS).

Sharing a view similar to [35,36] presents a distributed non-cooperative game is formulated for participating organizations to maximize their average reward by determining appropriate information to share and readiness to invest. A quadratic function is utilized to compute amount of benefit an organization derives from intelligence shared by other organizations and the total utility gain of that organization is determined using the logarithmic gain function

In [37] and [38] an approach that computes incentive and participation fee based on coalitional game theory for cyberthreat exchange participants is proposed. The authors identified the need to induce participants to provide valuable information by creating a system where participants receive incentives for provided information based on the summation of the benefits of all participants utilizing such information. Furthermore, the imposed participation fee for participating organizations should be proportional to the values such participants derives from the CTI. All these are in contrast to the traditional fixed incentives and participation fee. To realize a dynamic and fair participation fees and incentives, the study proposed the Shapley Value and Nucleolus solution concepts to a CTI exchange environment defined as a coalition game problem.

Similar to the concern raised in [37,39] identified the challenges of motivating reluctant participants to share CTI and determining fairer incentives for participants in threat exchange. When determining the reward for each participating organization, it is important to also consider the risk factors and its impact on the organization providing intelligence. To address the participants reluctance to share CTI, the study proposed a multi-stage CTI exchange based on cooperative game model and a modified Shapley value with the concept of risk coefficient for a fair reward distribution.

As opposed to realizing dynamic reward proportional to an organization's level of participation, some other exchange environment aims at maintaining higher payoff or profitability of some participants over others. This in essence will demotivate lower rewarded participants for a more secured exchange environment. The study [40] formulates the coexistence of malicious and regular participants problem as an incomplete information game with the assumption that whenever a CTI platform receives an intelligence, an anomaly detection based on machine learning is carried out on this intelligence to detect if such intelligence is malicious or not. Afterwards, a mixed strategy Nash equilibrium is derived and subsequently simulated. Analysis of the simulation is performed to determine best response strategy that returns higher payoffs. This is utilized by the exchange platform and regular participants to ensure higher profitability over malicious participants.

In general, active participation level within different CTIs may increase with the right participation fee and incentive computation model.

4 Conclusion

The wide adoption of Cyber Threat Intelligence is facing some challenges of which security is considered to be major. In this study, a body of literature that identified and addressed security issues associated with different cyber threat intelligence exchange platforms were reviewed. Identified issues are categorized into three major aspect of source protection, secure exchange and malicious participation issues. It is of great importance to examine what has been done in order to identify the knowledge gaps and possible ways of improvement. In addition, the study considered participation costs related issues as another important factor that demotivates CTI exchange participation. The review carried out in this study has the potential to help identify and understand the various security related issues evident in threat intelligent exchange and thereby give direction to interested parties for future work in this area.

References

1. Dandurand, L., Serrano, O.S.: Towards improved cyber security information sharing. In: 2013 5th International Conference on Cyber Conflick (CYCON 2013), pp. 1–16. IEEE (2013)
2. Locasto, M.E., Parekh, J.J., Keromytis, A.D., Stolfo, S.J.: Towards collaborative security and P2P intrusion detection. In: Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, pp. 333–339. IEEE (2005)
3. Pala, A., Zhuang, J.: Information sharing in cybersecurity: a review. Decis. Anal. **16**(3), 172–196 (2019)
4. Rutkowski, A., et al.: CYBEX-the cybersecurity information exchange framework (X.1500). ACM SIGCOMM Comput. Commun. Rev. **40**(5), 59–64 (2010)
5. Riesco, R., Larriva-Novo, X., Villagra, V.A.: Cybersecurity threat intelligence knowledge exchange based on blockchain. Telecommun. Syst. **73**(2), 259–288 (2020)

6. Vazquez, D.F., Acosta, O.P., Spirito, C., Brown, S., Reid, E.: Conceptual framework for cyber defense information sharing within trust relationships. In: 2012 4th International Conference on Cyber Conflict (CYCON 2012), pp. 1–17. IEEE (2012)
7. Rahman, N.H., Kessler, G.C., Choo, K.K.: Implications of emerging technologies to incident handling and digital forensic strategies: a routine activity theory. In: Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, pp. 131–146. Syngress (2017)
8. Clifton, C., et al.: Privacy-preserving data integration and sharing. In: Proceedings of the 9th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery, pp. 19–26 (2004)
9. Sauerwein, C., Sillaber, C., Mussmann, A., Breu, R.: Threat intelligence sharing platforms: an exploratory study of software vendors and research perspective (2017)
10. Abu, M.S., Selamat, S.R., Ariffin, A., Yusof, R.: Cyber threat intelligence - issues and challenges. Indones. J. Electr. Eng. Comput. Sci. **10**(1), 371–9 (2018)
11. Zibak, A., Simpson, A.: Cyber threat information sharing perceived benefits and barriers. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, pp. 1–9 (2019)
12. Mkuzangwe, N.N., Khan, Z.C.: Cyber-threat information sharing standards: a review of evaluation literature. Afr. J. Inf. Commun. **25**, 1–12 (2020)
13. Cascavilla, G., Tamburri, D.A., Van Den Heuvel, W.J.: Cybercrime threat intelligence: a systematic multi-vocal literature review. Comput. Secur. **105**, 102258 (2021)
14. Saxena, R., Gayathri, E.: Cyber threat intelligence challenges: leveraging blockchain intelligence with possible solution. Mater. Today Proc. **51**, 682–689 (2022)
15. Voutilainen, J., Kari, M.: Strategic cyber threat intelligence: buidling the situational picture with emerging technologies. In: Proceedings of the European Conference on Information Warfare and Security, Academic Conference International (2020)
16. Traffic Light Protocol (TLP) definitions and usage. https://www.cisa.gov/tlp
17. van de Kamp, T., Peter, A., Everts, MH., Jonker, W.: Private sharing of IOCs and sightings. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, pp. 35–38 (2016)
18. Preuveneers, D., Joosen, W.: TATIS: trustworthy APIs for threat intelligence sharing with UMA and CP-ABE. In: Benzekri, A., Barbeau, M., Gong, G., Laborde, R., Garcia-Alfaro, J. (eds.) FPS 2019. LNCS, vol. 12056, pp. 172–188. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45371-8_11
19. Vakilinia, I., Tosh, D.K., Sengupta, S.: Attribute based sharing in cybersecurity information exchange framework. In: 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), pp. 1–6. IEEE (2017)
20. Vakilinia, I., Tosh, D.K., Sengupta, S.: Privacy-preserving cybersecurity information exchange mechanism. In: 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), pp. 1–7 (2017)
21. Wagner, T.D., Palomar, E., Mahbub, K., Abdallah, A.E.: Towards an anonymity supported platform for shared cyber threat intelligence. In: Cuppens, N., Cuppens, F., Lanet, J.-L., Legay, A., Garcia-Alfaro, J. (eds.) CRiSIS 2017. LNCS, vol. 10694, pp. 175–183. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76687-4_12

22. Badsha, S., Vakilinia, I., Sengupta, S.: Privacy preserving cyber threat information sharing and learning for cyber defense. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 908–714. IEEE (2019)
23. Rawat, D.B., Njilla, L., Kwiat, K., Kamhoua, C.: iShare: blockchain-based privacy-aware multi-agent information sharing games for cyber security. In: 2018 International Conference on Computing Networking and Communications (ICNC), pp. 425–431. IEEE (2018)
24. Cha, J., Singh, S.K., Pan, Y., Park, J.H.: Blockchain-based cyber threat intelligence system architecture for sustainable computing. Sustainability **12**(16), 6401 (2020)
25. Gong, S., Lee, C.: Blocis: blockchain-based cyber threat intelligence sharing framework for sybil-resistance. Electronics **9**(3), 521 (2020)
26. He, S., Fu, J., Jiang, W., Cheng, Y., Chen, J., Guo, Z.: Blotisrt: blockchain-based threat intelligence sharing and rating technology. In: Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies, pp. 524–534 (2020)
27. Menges, F., Putz, B., Pemul, G.: DEALER: decentralized incentives for threat intelligence reporting and exchange. Int. J. Inf. Secur. **20**(5), 741–761 (2021)
28. Homan, D., Shiel, I., Thorpe, C.: 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), pp. 1–6. IEEE (2019)
29. Nguyen, K., Pal, S., Jadidi, Z., Dorri, A., Jurdak, R.: A blockchain enabled incentivised framework for cyber threat intelligence sharing in ICS. arXiv: 2112.00262 (2021)
30. de Fuentes, J.M., Gonzalez-Manzano, L., Tapiador, J., Peris-Lopez, P.: PRACIS: privacy-preserving and aggregatable cybersecurity information sharing. Comput. Secur. **69**, 127–141 (2017)
31. Moubarak, J., Bassil, C., Antoun, J.: On the dissemination of cyber threat intelligence through hyperledger. In: 2021 17th International Conference on the Design of Reliable Communication Networks (DRCN), pp. 1–6 (2021)
32. Kokkonen, T., Hautamaki, J., Siltanen, J., Hamalainen, T.: Model for sharing the information of cyber security situation awareness between organizations. In: 2016 23rd International Conference on Telecommunications (ICT), pp. 1–5. IEEE (2016)
33. Pahlevan, M., Voulkidis, A., Velivassaki, T.H.: Secure exchange of cyber threat intelligence using TAXII and distributed ledger technologies-application for electrical power and energy system. In: The 16th International Conference on Availability, Reliability and Security, pp. 1–8 (2021)
34. Vakilinia, I., Tosh, D.K. Sengupta, S.: 3-way game model for privacy-preserving cybersecurity information exchange framework. In: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), pp. 829–834. IEEE (2017)
35. Tosh, D., Sengupta, S., Kamhoua, C., Kwiat, K., Martin, A.: An evolutionary game theoretic framework for cyber threat information sharing. In: 2015 IEEE International Conference on Communications (ICC), pp. 7341–7346. IEEE (2015)
36. Tosh, D.K., Sengupta, S., Mukhopadhyay, S., Kamhoua, C.A., Kwiat, K.A.: Game theoretic modeling to enforce security information sharing among firms. In: 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing 2015, pp. 7–12. IEEE (2015)
37. Vakilinia, I., Sengupta, S.: A coalitional game thoery approach for cybersecurity information sharing. In: MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), pp. 237–242. IEEE (2017)
38. Vakilinia, I., Sengupta, S.: Fair and private rewarding in a coalitional game of cybersecurity information sharing. IET Inf. Secur. **13**(6), 530–540 (2019)

39. Xie, W., Yu, X., Zhang, Y., Wang, H.: An improved shapley value benefit distribution mechanism in cooperative game of cyber threat intelligence sharing. In: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workships (INFOCOM WKSHPS), pp. 810–815. IEEE (2020)
40. Thakkar, A., Badsha, S., Sengupta, S.: Game theoretic approach applied in cybersecurity information exchange framework. In: 2020 IEEE 17th Annual Consumer Communication and Networking Conference (CCNC), pp. 1–7. IEEE (2020)
41. Preuveneers, D., Joosen, W., Bernal Bernabe, J., Skarmeta, A.: Distributed security framework for reliable threat intelligence sharing. Secur. Commun. Netw. (2020)
42. Keim, Y., Mohapatra, A.K.: Cyber threat intelligence framework using advanced malware forensics. Int. J. Inf. Technol. 1–10 (2019)