Blockchain and Self-Sovereign Identity Empowered Cyber Threat Information Sharing Platform

Eranga Bandara*, Xueping Liang†, Peter Foytik*, Sachin Shetty*,
* {cmedawer, PFoytik, sshetty, rmukkama}@odu.edu
Old Dominion University, Norfolk, VA, USA
† {x_liang}@uncg.edu
University of North Carolina at Greensboro, NC, USA

***Abstract*—Cyber threat information (CTI) sharing involves processes of the collection, analysis and sharing of cyber threat information among multiple organizations. CTI is highly sensitive and inadvertent access can harm an organisation's reputation. Moreover, CTI sharing may also inadvertently advertise a vulnerability that may be present in the organisation's infrastructure. Therefore, preserving the privacy and anonymity of the CTI participants is critical. This paper proposes "Siddhi", a blockchain and Self-Sovereign Identity(SSI) enabled CTI platform that will realize traceability, anonymization and data provenance in a scalable fashion. Siddhi is equipped with SSI-enabled mobile wallet to ensure anonymous reporting of threat information and supports TAXII and STIX standards for exchanging the threat information between participants in the blockchain network.**

***Index Terms*—Blockchain; Self-Sovereign Identity; Cyber Thread Information Sharing; Cloud Computing**

1. Introduction

Cyberthreat information (CT) is shared to assist organizations in identifying, assessing, monitoring, and responding to cyberthreats [1]. The collecting and analysis of attack patterns, IDs, malware, attackers, and tactic-technique-procedures are all part of CTI sharing (TTP). The most widely used CTIdata expression language is STIX [2], [3], and the data communication protocol for exchanging data expressed as STIX is TAXII. The STIX language is used to express the analyzed CTI data, which is subsequently exchanged using the TAXII protocol [4]. To proactively minimize cyber dangers, data must be shared quickly and efficiently.

Due to its sensitive nature and the participants' participation in various trust boundaries, sharing CTI is difficult [5]. The unintentional release of CTI could result in further exploitation by attackers, as well as reputation damage and potential economic loss [6]. Effectively constructing a collaborative information-sharing network will have a detrimental impact. For entities engaging in a CTI sharing network, privacy is still a major problem. Anonymization of the participant providing the information has also been proposed; however, this generates a case in which the trustworthiness of the data is questioned if the data source cannot be verified [7].

In this paper, we proposed Siddhi, a blockchain and self-sovereign identity [8] empowered CTI sharing platform. Siddhi is built on top of our Rahasak scalable permissioned blockchain framework [9], [10]. The cyber threat information and data provenance information is stored in peer to peer blockchain system. Siddhi is integrated with self-sovereign identity (SSI) capability to realize the anonymity of the participants in the cyber threat sharing platform. Siddhi is integrated with TAXII and SITX to ensure standardization of content and exchange among organizations.

1) Blockchain and SSI empowered cyber threat information sharing platform.
2) TAXII and STIX message standard supported on Siddhi platform.
3) Android/IOS based mobile identity wallet in Siddhi has been used to anonymously upload the cyber threat information data into the blockchain.
4) Blockchain-enabled web application has been introduced to post, search and get alerts about the new cyber threat information.

The paper is divided into six sections. Section 2 discusses the architecture of the Siddhi platform and Section 3 presents the functionality of Siddhi. Performance evaluation is given in Section 4. Section 5 summarizes the related work. Finally, the last section of the paper presents the concluding remarks with suggestions for future research directions.

2. Siddhi Platform Architecture

2.1. Overview

The Siddhi platform hosts three main types of stakeholders, namely the Service provider, Incident reporters and Incident viewers. Service providers are the host of the Siddhi platform and hold the admin role. There could be multiple admin privilege entities in the Siddhi. All of them have equal permissions. Their main function is to onboard incident reporters and viewers into the platform. Incident reporters and viewers represent different organizations in the Siddhi. Before reporting incidents they need to register their identities on the Siddhi platform. Their identities managed with an anonymous approach as self-sovereign identity. In this way, they can report the incidents anonymously. The cyber incident information published in the blockchain will be publicly available to any party. Incident viewers can view the reported cyber threat incident information's published on the Siddhi platform. They can subscribe to incident types they are interested in. When a new incident came with the relevant type they will automatically get notification about the attack to their web/mobile applications. Siddhi comes with an Android/IOS based mobile wallet application and web application. The mobile wallet application is the identity registration and incident reporting application(which use by the incident reporters). The incident reporters and viewers need to register on the Siddhi platform by using the mobile wallet application. It uses the self-severing identity approach to register the identities of the users. Unlike centralized identity systems, the actual identities of the users stored in the customers' mobile application. The proof of these identities stored in the blockchain-based decentralized storage as a self-sovereign identity proof. Then the admin can verify the identities by directly fetching them from the users mobile wallet application. The registered users(incident reporters) in the platform can report cyber attack information's anonymously by using the mobile wallet application. There is a Siddhi web admin portal for Service providers. By using this admin portal they can verify the identities of the registered users in the Siddhi platform. The publicly available Siddhi web can be accessible by any part to view the Cyberattack information. Incident viewers can use this web application to find the attack information. The Siddhi platform contains three main components, 1) Distributed ledger, 2) Stakeholders, 3) Peer-to-Peer channels.

2.2. Blockchain Ledger

Blockchain ledger maintains all users' digital identity proofs or the decentralized identity proof [8], and the cyber threat information on the Siddhi platform. The user identity proof and consent stored in one node will be synced with all other nodes by the underlying consensus algorithms supported by the blockchain platform. The DID proof is generated by the credential owner and stored in the blockchain ledger. Then admin/verifiers of the Siddhi platform approve it and update the status of the DID proof. The registered users then post the cyber threat information into the blockchain. The blockchain ledger can be deployed among multiple organizations in the Siddhi platform. Each organization in the network can run its own blockchain node.

The functionalities in the Siddhi platform are implemented with blockchain smart contracts. The users in the platform(e.g credential owner, verifier) interact with these smart contracts functions. There are three main smart contracts a) Identity contract, b) Incident contract c) Notification contract. The self-sovereign identity functions implemented with the identity contract. The Incident contract facilitates the create/search functions of cyber attack information on the blockchain. It mainly has functions to create cyber attacks and search cyber attacks data from the blockchain. There are various notification scenarios in Siddhi, for example when a credential verifier needs to access the credential of a customer, a customer needs to be notified about it. These kinds of notifications are handled with the Notification contract.

2.3. Stakeholders

There are three main types of Stakeholders (e.g users) in the Siddhi platform, incident reporters, incident viewers and admin. Incident reporters and viewers are identified as credential owners in SSI terms. Credential owners register their DID proofs on blockchain and enroll in the Siddhi platform with the Siddhi mobile application. Once the user registers DID proof in blockchain, the admin user verifies the users' identities by using the Siddhi web application. To verify the identity admin needs to fetch users actual identity information via connecting to the users mobile wallet application. When performing DID registration and credential verification, credential owners and verifiers interact with each other on top of the underlying blockchain ledger through the Identity smart contract to put and fetch credentials. Siddhi mobile application and Web application interact with Identity smart contract. Once the user identity verified by the admin, users can report cyber attack information on behalf of their organizations by using Siddhi mobile wallet application. In this step, the Siddhi mobile wallet application interacts with the Incident smart contract in the blockchain.

2.4. Peer-To-Peer Channels

The peer-to-peer channels are used to exchange the credential information between the credential owners(e.g incident reporters, incident viewers) and verifiers(e.g admin). When verifying the credentials of a user, the credential verifier first fetches the users' DID proof(cryptographic proof of the credentials) from the blockchain. Then request consent from the user to access the credentials(e.g email, mobile phone number, photo, company etc). Once consent is given by the users, the verifier directly fetches the credentials from the users' mobile wallet application via a peer to peer channel.

3. Siddhi Platform Functionality

3.1. User Registration Process

First, the incident reporters and viewers on the platform need to register their identities on the Siddhi platform anonymously. They can do the identity registration via Siddhi mobile wallet application. Assume User1 from Organization1 register his/her identity in the Siddhi platform by using the

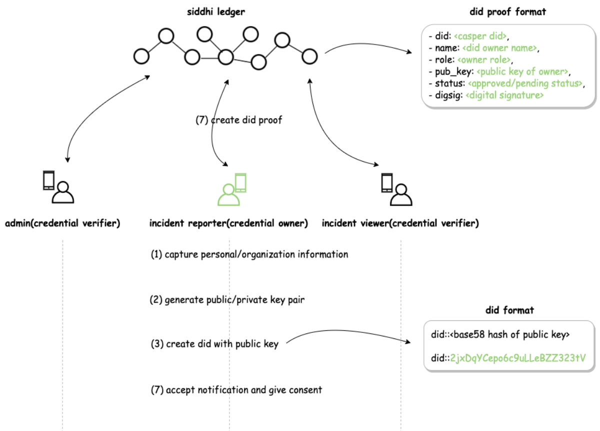
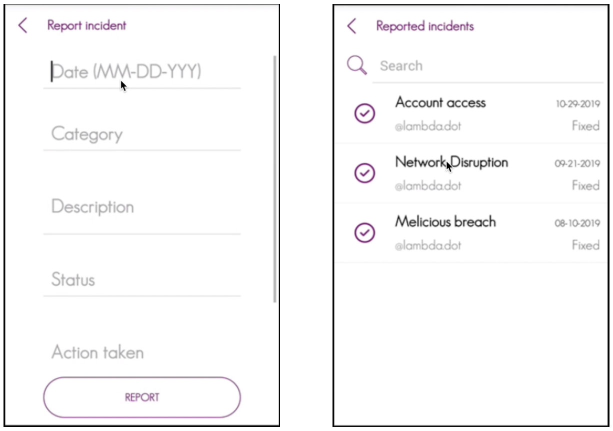

siddhi ledger
did proof format
- did: <casper did>,
- name: <did owner name>,
- role: <owner role>,
- pub_key: <public key of owner>,
- status: <approved/pending status>,
- digsig: <digital signature>
(7) create did proof
admin(credential verifier)
incident reporter(credential owner)
incident viewer(credential verifier)
(1) capture personal/organization information
(2) generate public/private key pair
(3) create did with public key
did format
did::<base58 hash of public key>
did::2jxDqYCepo6c9uLLeBZZ323tV
(7) accept notification and give consent

Figure 1: DID structure in Siddhi platform.



Account access	@lambda.dot	10-29-2019
		Fixed
Network Disruption	@lambda.dot	09-21-2019
		Fixed
Melicious breach	@lambda.dot	08-10-2019
		Fixed

(a) Report incident (b) Incident history

Figure 2: Siddhi mobile application.

mobile wallet. On registration, the user needs to capture his/her identity information, personal information, image, organization information via the Siddhi mobile wallet. The captured information will be stored in a secure storage zone by the mobile application and the proof of this information will be uploaded to the blockchain as self-sovereign identity proof (DID proof). The user DID is generated based on the public key of the user. On registration, the Siddhi mobile wallet will generate a public/private key pair for the user. The private key will be securely stored by the secure Key-store on the mobile application. The DID will be generated with the based58 hash of the public key. The generated DID format is described in Figure 1. It contains a base58 hash of the public key [11]. The user generates the DID proof with the public key, DID and user role. Then the user digitally signs the DID proof with his/her private key and upload it to the blockchain ledger. Figure 1 shows the format of the DID proof on the Siddhi platform.

Once DID proof registered in the blockchain, it needs to be approved by the admin in the Siddhi platform. Admin can approve the identity information via the Siddhi admin web applications. Siddhi admin web application will list all the DID proof information stored in the blockchain ledger. To approve the identity admin required the users' actual identity information which resides on the users' Siddhi mobile wallet. Admin user directly fetches the user identity information from the users' Siddhi mobile wallet by using a peer-to-peer channel(with using Firebase push notification). This identity information includes users personal information, company information etc. The fetched identity information will be displayed in the admin web application. To approve the identity admin needs to check the fetched identity information against the real identity data of the user. If further information required admin can contact the user via email and get the necessary information. If all the identity information is valid the admin will approve the identity registration of the user, by digitally signing the identity proof and mark the status of the identity proof as "Approved". This is the vetting process required in order to approve that the user identity is authentic and verified by a trusted source. Once identity is approved by an authorized administrator, the user can use his/her identity wallet to report the cyber threat information and view them.

3.2. Report and View Incidents

The registered users in the Siddhi platform can report cyber-attack information via the Siddhi mobile application. As shown in Figure 2 when reporting an incident it takes 1) incident data, 2) incident category, 3) description, 4) the current status of the attack 5) action taken to resolve the attack, 6) efficient percentage of the action taken details. The incident category defines the type of the incident such as DOS attack, network attack etc. There are predefined types that the admin of the Siddi platform defined. The status of the attack defines the pending, completed like details. When creating a new incident Siddhi mobile wallet application interact with the Incident smart contract on the blockchain. The mobile app connects to its own organizations' blockchain node and creates the incident. Once incidents created in the organizations' blockchain node, they will be available to the other organizations via the underlying blockchain system. These reported incidents can be viewed by any user(incident viewers) in the Siddhi platform. The users can subscribe to their interested incident types and get notifications about the incidents. For example, a user can subscribe for DOS attack incidents. Then this user will get a notification once a new DOC attack incident created in the blockchain. These notification functions handle by the Notification smart contract.

4. Implementation and Evaluation

The production version of the Siddhi platform has been completed. The underlying blockchain ledger of Siddhi is the Rahasak blockchain [9], [10], [12], which is a highly scalable blockchain aimed for big data. To facilitate blockchain tasks, Rahasak comes with a functional programming and actor-based "Aplos" smart contract platform

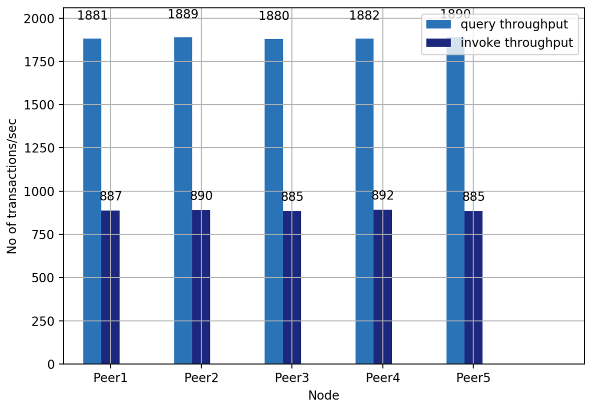


Figure 3: Invoke and Query transaction throughput of Siddhi blockchain platfrom.

[13], [14]. Aplos smart contracts are used to implement all blockchain functions on the Siddhi platform. The TAXII server served as the platform's entry point. The STIX messaging protocol is used by clients to communicate with the TAXII server. Siddhi is a mobile application for Android and iOS devices. The fire-base [15] push notification service has been used to implement peer-to-peer channels in Siddhi. Siddhi's performance evaluation has been completed and is being considered as part of its implementation. The following are the evaluation results, with a changing number of blockchain peers (1 to 7 peers) used in each evaluation.

Transaction throughput – The number of invoke transactions and query transactions that can be completed in each blockchain peer in the Siddhi platform were documented for this evaluation. The invoke transaction alters the status of the assets on the blockchain by creating a record in the ledger. The query looks up the current state of the blockchain ledger. They don't update the asset state or initiate transactions in the ledger. We inundated each peer with concurrent transactions and counted the number of completed outcomes. On the Siddhi platform, we were able to achieve constant throughput in each peer, as seen in Figure 3. Because searches do not update the ledger status, they have a much higher throughput (2 times) than initiate transactions.

Transaction scalability and latency – We calculated the number of transactions that can be processed (per second) divided by the number of peers in the network for this evaluation. We inundated each peer with concurrent transactions and counted the number of transactions that were completed. The findings of transaction scalability are shown in Figure 4. When a node is added to the cluster, the transaction throughput grows roughly linearly. This means that if more blockchain peers are added to the cluster, the latency will be reduced, as seen in Figure 5. There is a declining return when more peers are added, and the performance benefit will deteriorate if too many peers are included.

Transaction execution rate – Following that, we measure the number of submitted and performed transactions in individual blockchain peers while keeping track of the time.

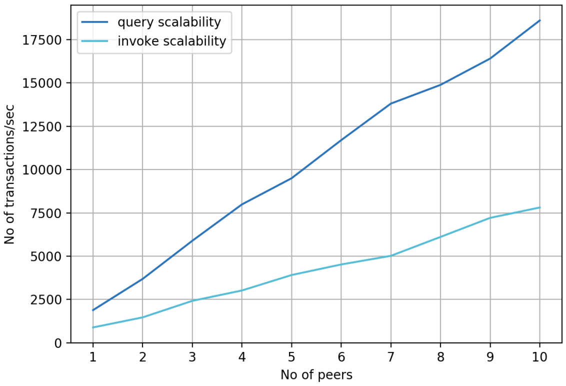


Figure 4: Invoke and Query transaction scalability of Siddhi blockchain platfrom.

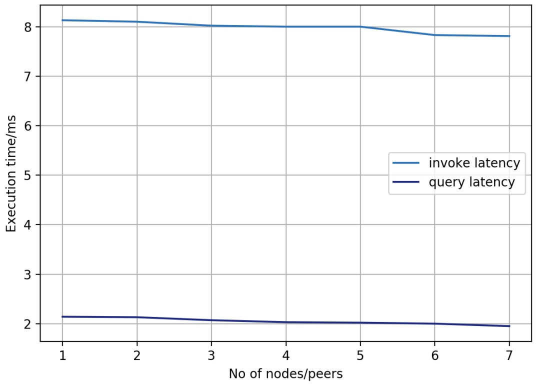


Figure 5: Invoke and Query transaction latency of Siddhi blockchain platfrom.

Figure 6 depicts the total number of completed transactions submitted by a single blockchain peer. Between the rates of submitted transactions and performed transactions, there is a backpressure management operation [16]. In the Siddhi platform, we used an active streaming-based method with Apache Kafka to manage these back pressure activities.

5. Related Works

Research has been conducted in the area of privacy-preserving cyber threat information sharing. **BCTISA** [17] proposes a blockchain-based cyber threat intelligence system architecture for sustainable computing. It addresses the limitation of traditional cyber threat information sharing systems such as reliability, privacy, scalability. **BLOCIS** [18] is a blockchain-based cyber threat intelligence sharing framework for Sybil-resistance. The proposed system can detect inaccurate CTI data which are resistant to Sybil attacks. **BloCyNfo-Share** [19] identified as Blockchain-based Cybersecurity Information Sharing with Fine-Grained Access Control. The proposed system modeled a blockchain-based

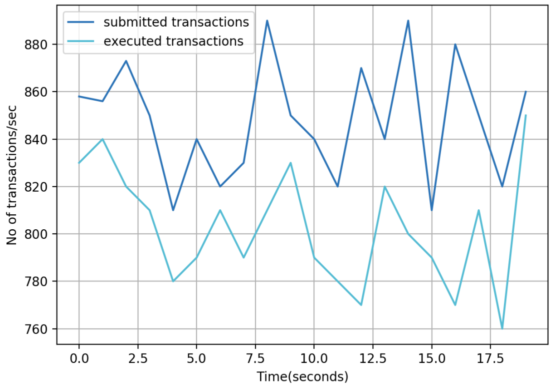


Figure 6: Transaction execution rate and transaction submission rate in a single blockchain peer in Siddhi.

cyber threat information sharing platform using proxy re-encryption and attributed-based encryption.

SDN-CTI [20] work proposes a blockchain-based cyber threat information sharing system for SDN networks. It has reduced the cyber-attack mitigation time by defining fast security policy enforcements via the SDN control plane. **MISP** [21] known as Malware Information Sharing Platform. It allows to collect and share threat information, attacks, vulnerabilities and financial indicators used in fraud cases through a cloud-based system. **CTI-Cloud** [22] proposes a game theory-based cyber-threat information sharing system for cloud computing. The game theory model provides a mechanism for multiple self-interested firms to invest in vulnerability discovery and share their cyber-threat information.

6. Conclusions and Future Work

We propose a blockchain and self-sovereign identity-based cyber threat information sharing platform, Siddhi, which is compatible with TAXII and STIX standers for data sharing between parties in the network. All the cyber threat information and their data provenance information are stored in peer to peer blockchain system with guaranteed reliability. Siddhi platform incorporates with Self-Soverine identity based anonymous mobile wallet application. Therefore, the responsible entity in the organization can register in Siddhi without revealing the sensitive data of the company(e.g company name, etc) with third parties. We have built a production version of Siddhi on top of the Rahasak scalable blockchain platform. Siddhi addresses the main issues in cyber threat information sharing such as traceability, reliability, privacy, scalability, anonymisation and data provenance. We prove that the scalability and transaction throughput features of the Siddhi platform with empirical evaluations. Regarding future research, we are interested in implementing a user study involving multiple organizations to find out how sharing the cyber threat information on Siddhi can help increase the efficiency and effectiveness of an organization's cybersecurity maturity and capabilities.

Acknowledgements

This work was supported in part by the DoD Center of Excellence in AI and Machine Learning (CoE-AIML) under Contract Number W911NF-20-2-0277 with the U.S. Army Research Laboratory.

References

[1] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," in *2017 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 2017, pp. 91–98.

[2] M. Apoorva, R. Eswarawaka, and P. V. B. Reddy, "A latest comprehensive study on structured threat information expression (stix) and trusted automated exchange of indicator information (taxii)," in *Proceedings of the 5th international conference on frontiers in intelligent computing: theory and applications*. Springer, 2017, pp. 477–482.

[3] F. Sadique, S. Cheung, I. Vakilinia, S. Badsha, and S. Sengupta, "Automated structured threat information expression (stix) document generation with privacy preservation," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 2018, pp. 847–853.

[4] J. Connolly, M. Davidson, and C. Schmidt, "The trusted automated exchange of indicator information (taxii)," *The MITRE Corporation*, pp. 1–20, 2014.

[5] P. Kampanakis, "Security automation and threat information-sharing options," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 42–51, 2014.

[6] C. Johnson, M. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "Guide to cyber threat information sharing," National Institute of Standards and Technology, Tech. Rep., 2016.

[7] E. W. Burger, M. D. Goodman, P. Kampanakis, and K. A. Zhu, "Taxonomy model for cyber threat intelligence information exchange technologies," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, 2014, pp. 51–60.

[8] D. Baars, "Towards self-sovereign identity using blockchain technology," Master's thesis, University of Twente, 2016.

[9] E. Bandara, X. Liang, P. Foytik, S. Shetty, N. Ranasinghe, and K. De Zoysa, "Rahasak-scalable blockchain architecture for enterprise applications," *Journal of Systems Architecture*, p. 102061, 2021.

[10] E. Bandara, W. K. NG, K. DE Zoysa, N. Fernando, S. Tharaka, P. Maurakirinathan, and N. Jayasuriya, "Mystiko—blockchain meets big data," in *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018, pp. 3024–3032.

[11] J. Fisher and M. H. Sanchez, "Authentication and verification of digital data utilizing blockchain technology," Sep. 29 2016, uS Patent App. 15/083,238.

[12] E. Bandara, D. Tosh, P. Foytik, S. Shetty, N. Ranasinghe, and K. De Zoysa, "Tikiri-towards a lightweight blockchain for iot," *Future Generation Computer Systems*, 2021.

[13] E. Bandara, W. K. NG, K. De Zoysa, and N. Ranasinghe, "Aplos: Smart contracts made smart," *BlockSys'2019*, 2019.

[14] E. Bandara, X. Liang, P. Foytik, S. Shetty, N. Ranasinghe, K. De Zoysa, and W. K. Ng, "Saas-microservices-based scalable smart contract architecture."

[15] C. Khawas and P. Shah, "Application of firebase in android app development-a study," *International Journal of Computer Applications*, vol. 179, no. 46, pp. 49–53, 2018.

[16] A. Destounis, G. S. Paschos, and I. Koutsopoulos, "Streaming big data meets backpressure in distributed network computation," in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 2016, pp. 1–9.

[17] J. Cha, S. K. Singh, Y. Pan, and J. H. Park, "Blockchain-based cyber threat intelligence system architecture for sustainable computing," *Sustainability*, vol. 12, no. 16, p. 6401, 2020.

[18] S. Gong and C. Lee, "Blocis: Blockchain-based cyber threat intelligence sharing framework for sybil-resistance," *Electronics*, vol. 9, no. 3, p. 521, 2020.

[19] S. Badsha, I. Vakilinia, and S. Sengupta, "Blocynfo-share: Blockchain based cybersecurity information sharing with fine grained access control," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2020, pp. 0317–0323.

[20] M. Hajizadeh, N. Afraz, M. Ruffini, and T. Bauschert, "Collaborative cyber attack defense in sdn networks using blockchain technology," in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2020, pp. 487–492.

[21] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "Misp: The design and implementation of a collaborative threat intelligence sharing platform," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, 2016, pp. 49–56.

[22] C. Kamhoua, A. Martin, D. K. Tosh, K. A. Kwiat, C. Heitzenrater, and S. Sengupta, "Cyber-threats information sharing in cloud computing: A game theoretic approach," in *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*. IEEE, 2015, pp. 382–389.