applied sciences

MDPI

Article

Blockchain-Based Model for Incentivized Cyber Threat Intelligence Sharing

Algimantas Venčkauskas [1], Vacius Jusas [1,*], Dominykas Barisas [1] and Boriss Misnevs [2]

[1] Department of Computer Science, Kaunas University of Technology, LT-51390 Kaunas, Lithuania; algimantas.venckauskas@ktu.lt (A.V.); dominykas.barisas@ktu.lt (D.B.)
[2] Department of Software Engineering, Transport and Telecommunication Institute, LV-1019 Riga, Latvia; misnevs.b@tsi.lv
* Correspondence: vacius.jusas@ktu.lt

Abstract: Sharing cyber threat intelligence (CTI) can significantly improve the security of information technology (IT) in organizations. However, stakeholders and practitioners are not keen on sharing CTI data due to the risk of exposing their private data and possibly losing value as an organization on the market. We present a model for CTI data sharing that maintains trust and confidentiality and incentivizes the sharing process. The novelty of the proposed model is that it combines two incentive mechanisms: money and reputation. The reputation incentive is important for ensuring trust in the shared CTI data. The monetary incentive is important for motivating the sharing and consumption of CTI data. The incentives are based on a subscription fee and a reward score for activities performed by a user. User activities are considered in the following three fields: producing CTI data, consuming CTI data, and reviewing CTI data. Each instance of user activity is rewarded with a score, and this score generates some value for reputation. An algorithm is proposed for assigning reward scores and for recording the accumulated reputation of the user. This model is implemented on the Hyperledger Fabric blockchain and the Interplanetary File System for storing data off-chain. The implemented prototype demonstrates the feasibility of the proposed model. The provided simulation shows that the selected values and the proposed algorithm used to calculate the reward scores are in accordance with economic laws.

Keywords: blockchain; cyber threat intelligence; Hyperledger Fabric; incentive system; IPFS

check for updates

Citation: Venčkauskas, A.; Jusas, V.; Barisas, D.; Misnevs, B. Blockchain-Based Model for Incentivized Cyber Threat Intelligence Sharing. *Appl. Sci.* **2024**, *14*, 6872. https://doi.org/10.3390/app14166872

Academic Editors: Ivo Pereira, Christophe Soares, Rui Humberto Pereira, Ana M. Madureira and Filipe Sá

Received: 12 June 2024
Revised: 4 July 2024
Accepted: 9 July 2024
Published: 6 August 2024

1. Introduction

Cyberattacks are constantly expanding to new domains of the public and private sectors. No organization with access to the internet is safe from cyberattacks. In the SANS annual report of the 2023 CTI survey [1], a notable increase was observed in the diversity of fields that contributed to the CTI survey. These fields included civil engineering, construction, agriculture, mining, health, law, and gaming. Such a diversity of fields means that cyberattacks are expanding their horizons. However, not only are more organizations involved in the reality of the digital world, but new technological artifacts are also coming into use, thus opening up new opportunities for cyberattacks.

A cyber threat analysis must be performed on a constant basis to keep up to date with the changing landscape of cyberattacks. Cyber threat intelligence (CTI) is the result of cyber threat analyses. CTI can be divided into four levels in decreasing hierarchical order: strategic, tactical, technical, and operational [2,3]. A CTI data-sharing system plays an important role, as organizations cannot defend themselves in isolation from emerging threats [4]. Stakeholders and practitioners are not keen on sharing CTI data due to the risk of exposing their private data and potentially losing value on the market. Trust is one of the main factors in sharing CTI. In their systematic review on using blockchain for sharing CTI, Chatziamanetoglou and Rantos [4] found that trust and privacy are predominant themes in this research field. However, the privacy of information and trust are not the only hurdles encountered when sharing CTI; other attributes of intelligence also play an important role, [5], including accuracy, timeliness, usability, completeness, precision, and dependability. These attributes characterize various aspects of the quality of CTI data. Achieving all of these attributes together is usually impossible due to competing demands. Therefore, the trust and quality of shared CTI are essential factors in persuading stakeholders and practitioners to allow their private data to be made available to the interested parties. Thus, CTI data sharing raises a tremendous necessity to create a trusted system that would possess the characteristics of validity, security, privacy, and traceability [6]. With a system that possesses the aforementioned characteristics, CTI users can produce automated and meaningful reports detailing existing threats. Analyzing such reports and proactively implementing appropriate measures can help to reduce the risk of potential cyber threats.

Traditional network systems for information sharing often follow a centralized approach and, thus, have a single point of failure that can be targeted by malicious actors. Meanwhile, a decentralized system is able to prevent the problems of a centralized system. Blockchain is a prominent representative of decentralized systems. Blockchains can operate in permissioned/permissionless and public/private modes [4]. A permissioned blockchain restricts access to the network to a predefined set of participants, who are known and trustworthy participants. Permissioned blockchains are appropriate applications when higher levels of control and confidentiality are required. Such a blockchain possesses the following attractive features for CTI data sharing: immutability, transparency, and traceability. These features are not related to the operation mode of the blockchain. However, the blockchain possesses features that are not attractive for CTI data sharing: a lack of scalability, latency, privacy issues, and limited data storage. The problem of limited data storage is usually solved using an Interplanetary File System (IPFS), when the storage of data is accomplished off-chain [7]. IPFS contributes to improving scalability as well. A private blockchain enables enhanced privacy and trust, as the blockchain grants access to trustworthy participants.

The most important challenge in creating and operating decentralized networks is ensuring the cooperation and contribution of participants of the network [8]. To solve this challenge, most public networks implement incentive mechanisms to keep the network functional and secure [9]. The incentive mechanism not only enhances the motivation of the participants, but also increases the security of the network, as the behavior of the participants is observed and assessed. The incentive mechanism becomes an integral architectural component of the decentralized network. For a decentralized network to be fully decentralized, all subsystems need to be decentralized, including the incentive mechanism. Smart contracts [10] in combination with distributed ledgers establish the decentralized computation of incentives.

The incentive mechanisms are divided into three categories: money, reputation, and service [7]. The monetary incentive mechanism motivates participants by distributing monetary credits. The reputation reward is a digital asset or value that is used to predict participants' future behavior. The service incentive mechanism motivates participants through either allowing direct access to or excluding a user from computational services. Regardless of the incentive mechanism used, if the mechanism is not set properly, the users of the network may be discouraged from participating and may seek cheaper alternatives.

The distinguishable contributions of this paper are as follows:

- Creating a new model for incentivized cyber threat intelligence sharing on permissioned blockchain technology for trustworthy threat intelligence sharing.
- Choosing quality metrics for CTI data evaluation.
- Creating an algorithm for reward score calculation.
- Providing simulation experiments to establish the ratio of monetary rewards to reputation scores.
- Implementing a prototype of the proposed solution on the Hyperledger Fabric blockchain to verify the feasibility of the solution.

- Developing smart contracts for enabling a series of services, including posting, sharing, and reviewing CTI data, and maintaining the rating scores of blockchain users.

The remainder of this paper is organized in the following way: A discussion of the existing CTI data-sharing solutions using incentives is provided in Section 2. Section 3 details the proposed solution, providing a reward score calculation, the model structure, and the model processes. Section 4 considers its implementation by providing the results of the experiment and discussing the results. Finally, Section 5 draws the conclusions.

2. Related Work

We consider various incentive approaches for CTI data sharing on decentralized platforms. The scope of our investigation is limited to the scientific literature, excluding gray literature given that the situation is changing as many established projects on decentralized platforms are becoming part of the academic community and the results are published in journals and conference proceedings. The papers are discussed in chronological order of their appearance.

Wu et al. [11] proposed a trust enhancement framework, TITAN, for threat intelligence (TI) sharing. However, the keyword “cyber” was not used. Nevertheless, the provided definition of TI corresponds to CTI. Trust is established using a shared reputation system. The main component of reputation is the quality of the information provided, which is assessed by a third-party assessor. The other components for representing reputation can be used as well, and the reputation value is stored with every peer. Ethereum blockchain was used to implement the framework. The type of blockchain, either permissioned or permissionless, was not defined. The use of a third-party assessor is the main drawback of the presented approach, since a centralized entry is introduced into a decentralized network, and this centralized entry is a target for attacks as it creates a single point of failure.

Riesco et al. [12] presented an incentivized model for CTI exchange based on tokens. The goal of the model was to enhance motivation for sharing CTI data. With this purpose in mind, three new roles were introduced in addition to the traditional roles of CTI data provider and CTI data consumer, namely investor, owner, and donor. Token-based incentives were proposed to motivate the participants of the network, implemented on the public Ethereum blockchain. However, trading sensitive CTI data is risky and, as the reputation of CTI data producers is not considered, there is no trust in the CTI data provided. Moreover, Riesco et al. [12] recognized that public Ethereum blockchain provides no privacy.

Gong and Lee [13] proposed an incentivized framework, BLOCIS, for CTI data sharing. The goal of the framework was to improve trust in the contents of CTI data. Three types of participants are involved in the network: contributors, consumers, and feeds. Feeds are intermediaries between contributors and consumers and govern the process of CTI data sharing. Feeds collect CTI data from contributors, assess their validity, and then either assign a reward value or penalty term to contributors depending on the provided CTI data before distributing the data to the requesting consumers. The contributor, through providing CTI data, pays a deposit, and the accumulated reward value indicates the reliability of the data. Consumers pay for access to CTI data. The proposed framework has several similarities to the one presented by Wu et al. [11]. Both frameworks use a centralized entry to assess the validity of the provided CTI data and are implemented on the public Ethereum blockchain.

Gonçalo et al. [14] proposed an architecture for sharing CTI to increase trust in the provided data. Trust is achieved using five reputation levels. The reputation level is used for both the sharing of CTI data and for the validation of the data shared by other users. By sharing CTI data, users can obtain a certain reputation level. The validation of CTI data is performed by trusted peers. Through sharing more reliable CTI data, the users move up the reputation levels. The proposed architecture was implemented on Hyperledger Fabric blockchain. Initially, a single control channel was implemented, which was used for communication among all users. New channels corresponding to particular topics could then be opened, and the CTI data would be submitted to these specific channels.

Menges et al. [15] suggested a protocol based on verifiers and token-based incentives to induce the fair sharing of CTI data. The authors emphasize the use of the term "fair" throughout the paper. The term "verifiers" is introduced, which is new in this context. However, the same function was performed by feeds in [13]. The use of token-based incentives is not new, as they were proposed by Riesco et al. [12] one year earlier. Moreover, the use of token-based incentives was more elaborated in [12], since new roles of investors, donors, and owners were introduced there. The protocol is implemented on the public EOS blockchain. The CTI data are stored off-chain using an Interplanetary File System (IPFS). The EOS blockchain enables much higher performance, in comparison to the Ethereum blockchain; however, the EOS blockchain is public, and sensitive CTI data cannot be shared on this platform.

Huff and Li [16] introduced a decentralized platform to allow participants to share CTI data anonymously, such that the shared data would not be attributable to the CTI data producer. The platform was implemented on a permissioned Hyperledger Fabric blockchain. A cryptocurrency incentive was proposed in order to improve the quantity and quality of the CTI data. In this approach, human analysts are incentivized to work with the CTI data provided. The work of human analysts includes not only validation of the provided CTI data, but also the annotation or attribution of certain knowledge. However, very little is mentioned regarding cryptocurrency incentives, and the mechanism of functioning of such incentives is not defined. All of the attention is concentrated on techniques to provide non-attributable CTI data. Unconditional anonymity can undermine trust in CTI data, but techniques to manage trust are not considered.

Chatziamanetoglou and Rantos [17] proposed a reputation-based model for CTI data sharing. The model includes three roles: CTI feeds; validators, whose selection is based on their previous reputation; and consumers. The validators evaluate the sources supplied by CTI feeds using a proposed Proof-of-Quality consensus algorithm. This evaluation is used to rate the CTI feeds. The reputation of validators is evaluated according to their performance, and this reputation plays an important role in the whole process. The model should be implemented on a permissionless blockchain. An extension of the work was presented in [18], although only a simulation of the proposed model was provided.

Nguyen et al. [19] introduced an incentivized framework for CTI data sharing in industrial control systems. The goal of this framework is to motivate better engagement for CTI data sharing. The framework involves the following user roles: CTI Consumer, CTI Contributor, Authority, Insurer, Industry CERTs, CTI Verifier, and Analytics. However, the increased number of roles adds a considerable amount of complexity to the organizational processes of the network. Registration and periodic subscription fees are used to monetize the incentives. A discount is given to verifiers and contributors for their next subscription. The use of the Traffic Light Protocol (TLP) was also introduced, as suggested in [20]. The concept of the TLP [20] was enhanced through adding a white channel, where data were made freely available to entities outside the network. The plan was that the implementation of the framework would consist of three main components: (1) the IPFS for off-chain storage, (2) the Hyperledger Fabric network, and (3) an application based on Node.JS. However, the proposed framework was not implemented, and only use-case scenarios were considered.

Zhang et al. [21] introduced a CTI data-sharing model that combines consortium blockchain and distributed reputation management to solve the issues of trust. Furthermore, a new consensus algorithm, "Proof-of Reputation", was proposed to increase the transaction rate in comparison with the Practical Byzantine Fault Tolerance (PBFT) algorithm. The peer nodes of the network can be in one of four states: leader, candidate, follower, and supervisor. The states of the node are dependent on the reputation score of the node. The supervisor node assesses the validity of the shared CTI data. In the case of success, the reputation score of the node is increased; in the opposite case, the reputation score of the node is decreased. The node is declared unfaithful if its reputation score is less than a predefined threshold.

Jesus et al. [22] thoroughly reviewed the state and challenges of CTI data sharing with a focus on the perceived barriers. An analysis of almost ten years' worth of open CTI data was also performed. Based on the findings, Jesus et al. [22] raised the requirements for a CTI data-sharing architecture. These requirements are as follows: identity, bidirectionality, collaboration model, actionability, and safety. The collaboration model is an essential part of the architecture, and it is mapped to four sub-requirements. First, it must focus on decentralized networks. Second, data analytics must be possible. Third, it must include economic incentives. Finally, the model must be able to maintain reputation management.

Ma et al. [23] proposed a blockchain-based incentive CTI data-sharing mechanism to solve the problems of lack of trust and free riding. Evolutionary game theory was used to model the incentive mechanism. Two assumptions form the basis of the incentive mechanism: rewards are needed for sharing CTI data, and penalties are needed for not sharing CTI data within a designated time frame. These assumptions form the basis for the calculation of ratings of members. The rating of members is the basis for the trust in shared CTI. However, the reward given is not based on the quality of the CTI data, as it is not evaluated. The whole incentive mechanism is oriented towards the goal of "sharing as much as possible and within a designated time frame". There is no motivation to consume CTI data. The simulation of the obtained incentive mechanism was performed in MATLAB. The blockchain chosen for the implementation was Ethereum.

A summary of the reviewed works is provided in Table 1.

Table 1. Summary of the reviewed works introducing incentives.

Reference	Incentive	Blockchain	Enhanced CTI Feature	User Roles	Storage
Wu et al. [11]	reputation	Ethereum	trust	not defined	on-chain
Riesco et al. [12]	tokens	public Ethereum	motivation	CTI data provider, CTI data consumer, investor, owner, and donor	on-chain
Gong and Lee [13]	reputation	public Ethereum	trust	contributor, consumer, and feed	on-chain
Gonçalo et al. [14]	reputation	Hyperledger Fabric	trust	not defined	on-chain
Menges et al. [15]	tokens	public EOS blockchain	motivation	CTI data provider, CTI data consumer, and verifier	off-chain
Huff and Li [16]	tokens	Hyperledger Fabric	quantity and quality, anonymity	not defined	on-chain
Chatziamanetoglou and Rantos [17,18]	reputation	permissionless	trust	CTI feed, validator, and consumer	on-chain
Nguyen et al. [19]	fees	Hyperledger Fabric	motivation	CTI consumer, CTI contributor, authority, insurer, industry CERTs, CTI verifier, analytics	off-chain
Zhang et al. [21]	reputation	consortium blockchain	trust	leader, candidate, follower, and supervisor	on-chain
Ma et al. [23]	reputation	public Ethereum	trust	not defined	on-chain

Thus, we can make the following conclusions:

1. Many authors have used incentives to either enhance trust in CTI data or motivate sharing of CTI data, but never pursued both goals together. However, Jesus et al. [22] noticed that a CTI data-sharing model must include both economic incentives and the ability to maintain reputation management.

2. Sensitive CTI data can only be shared on private blockchains [14,16,19,21].
3. CTI data can be large in volume; therefore, they must be stored off-chain [15,19].
4. The sharing of sensitive CTI data must be in accordance with the Traffic Light Protocol, which defines four levels for sharing CTI data [19,20].

These conclusions will guide the construction of the proposed model.

3. Proposed Solution

3.1. Model Structure

The model is built on five pillars (Figure 1): private blockchain, clients, off-chain storage, motivation, and trust. The first three pillars are physical, while the last pillars—motivation and trust—are virtual.

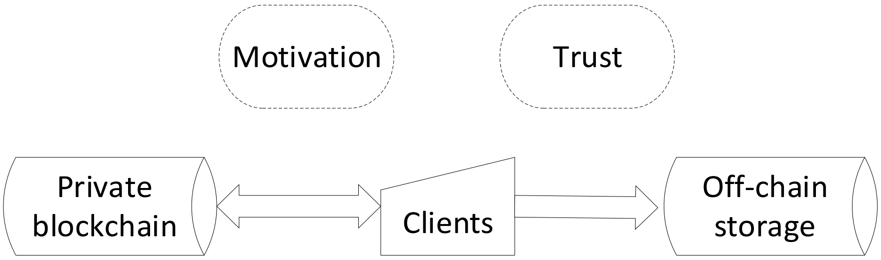


Figure 1. Pillars of the model.

The building of motivation and trust is discussed in Section 3.2. For the private blockchain network, our design uses Hyperledger Fabric, a permissioned blockchain which specializes in protecting information from unauthorized access through segmenting the visibility of the public ledger based on user credentials. Such techniques enable achievement of the goals of confidentiality and privacy. Privacy by design is promoted within Hyperledger Fabric, due to its inherent focus on channel-based privacy. We use this unique feature of Hyperledger Fabric and present an approach to share sensitive information, which is presented in Section 3.3. Finally, the implementation of the proposed technique is discussed in Section 3.4.

3.2. Building of Motivation and Trust

3.2.1. Cost Compensation and Reputation

The cost compensation is the first factor to consider in decentralized data-sharing networks, as the resulting costs can discourage data providers from sharing data. We propose a model for incentivized CTI data sharing, which seeks to provide a profit to both the data provider for sharing CTI data and the CTI data consumer for an acquaintance with the provided data.

The proposed model for incentivized CTI data sharing has three goals: (1) to cover the costs of sharing CTI data incurred by providers; (2) to promote the use of the shared data by CTI data consumers; and (3) to provide some degree of trust in the dependability of the CTI data provider and their shared CTI data. To establish the first two goals, a monetary reward is used. To establish the third goal, a reputation reward, which is expressed in terms of rating scores, is applied. Data providers can benefit twice, receiving a monetary reward to cover the cost of publishing data and receiving recognition from the community. CTI data consumers can also benefit twice, receiving a monetary reward for re-using shared data and receiving recognition for being an active member of the community.

The rating scores show the reputation of the users and are used to predict trust in a presented product. The presented product is either the shared CTI information itself or a review of it. Of course, this prediction is always subjective. No one can ensure that a user with a high rating value will not provide a product of low quality. However, reputation schemes promote cooperation and encourage user activity, thereby increasing decentralization. Moreover, the CTI data producer is discouraged from providing low-quality CTI data since they will be punished by receiving a penalty score.

To start CTI data-sharing activities, the interested parties must invest in them. Funds must be raised and shared according to the activities of the interested parties. One of the ways to raise the funds to support the defined goals is a subscription fee. Community members who are interested in sharing CTI data must subscribe to a CTI data-sharing network and pay the subscription fee, which can be either monthly or annual, depending on how long a member of the network requires access to shared CTI data.

The members of a CTI data-sharing network can interchangeably accept the roles of both CTI data producer and CTI data consumer. CTI data producers are encouraged to provide CTI data; therefore, a reward score is assigned to the CTI data producer for just one single act of CTI data provision. The quality of the CTI data is not taken into account yet. Nevertheless, the quality of the CTI data must be evaluated. The community should be self-organized in such a way that the decentralization of the network is increased. We must avoid using a trusted third party, which is a component of centralization, to evaluate the quality of shared CTI data. This work can be carried out by CTI data consumers. Motivation is needed to encourage CTI data consumers to review CTI data. A reward score should be assigned to consumers who express their desire to utilize the produced CTI data and to write a review of it. The CTI data consumer reward score is much lower than that of the CTI data producer.

3.2.2. Choice of Data Quality Metrics for Reviewers

CTI data consumers are encouraged to write a review of the data and present it to the CTI data producer. To guide the reviewers, an investigation was carried out to select the appropriate metrics for CTI quality evaluation. Sakellariou et al. [24] divided CTI quality factors into three groups: quality metrics, quality of the collected data, and quality of the produced intelligence. Sakellariou et al. [25] later categorized the CTI quality factors into three groups again; however, only the quality of collected data and quality of produced intelligence groups remained the same. The quality of collected data group [24,25] is only based on two publications [26,27]. In contrast, Dalziel [27] wrote that the factors of relevance, actionability, and value characterize the produced intelligence. We suppose that Sakellariou et al. [24,25] wrongly attributed these factors to the group of collected data. Moreover, relevance is defined as showing the relation of information to a specific organization's environment and aligning it with the organization's priorities and objectives. Thus, if the reviewer presents a different domain than the CTI data presented, the organization perceives such CTI data as irrelevant. We suppose that such an assessment would not be fair. Therefore, we seek metrics that are unrelated to the specifics of the field of CTI data; in particular, this requirement is fully satisfied by the quality metrics presented by Grispos et al. [26].

Other CTI data quality metrics [28,29] are available as well. Schlette et al. [28] presented a hierarchical quality metric consisting of three levels: report, object, and attribute. These are quite complex and detailed metrics for ordinary reviewers. Moreover, these metrics are STIX-format-oriented. The attribute level is entirely based on the evaluation of the available STIX objects.

Mavzer et al. [29] introduced quality metrics that include the following factors: completeness, freshness, timeliness, extensiveness, and relevance. These metrics are tool-oriented, and the values of all of the factors are calculated automatically. However, Mavzer et al. [29] noticed that the calculation of completeness, freshness, and extensiveness requires improvement.

We reviewed many studies relevant to the topic in this section; however, only Menges et al. [15] and Nguyen et al. [19] considered the use of quality metrics for the verification of CTI data. The metrics of consideration used in [15] were presented by Schlette et al. [28]. However, Nguyen et al. [19] provided neither a reference to specific metrics nor a detailed description of the metrics used. Only the factors of accuracy, usability, and relevance were mentioned. In addition, their future work was to determine which quality metrics are appropriate for CTI data verification. Moreover, a verified security expert evaluated the quality of CTI data in both approaches [15,19]. We suppose that the metric [28] is too complicated for the ordinary reviewer. Therefore, after careful consideration, we decided to present the quality factors introduced by Grispos et al. [26] to the reviewers, as follows: accuracy, timeliness, completeness, and consistency. These factors are common to many data domains [8].

3.2.3. Algorithm for Reward Score Calculation

The CTI data reviewer assigns a numeric rating ranging from 1 (low value) to 10 (great) to CTI data provided for a defined quality criterion. Behind the scenes, this external rating is converted into a scale from −4 to +5. Then, the quality of the CTI data is evaluated as a weighted sum of the quality criteria. If the obtained value is negative, the CTI data producer receives a penalty score related to this value. In addition, the reviewer is encouraged to write a review in a free form and is assigned a reward score for the review provided.

The CTI data producer is encouraged to verify the reviews. The reviews may be emotional, incomprehensive, or lack important details. Therefore, the CTI data producer can reject or accept the reviews after verification. If the review is rejected, the reasons are given to the reviewer to ensure fairness. Valid reviews are included together with the produced CTI data. An additional reward score is assigned to the first three reviewers to supply valid reviews, and a reward score is assigned to the producer for every included review. Future CTI data consumers then have more trust in the data as they can check the producer ratings and CTI data reviews.

The reward scores are converted into a monetary reward. User scores are accumulated for one year of the subscription, and then the total sum is calculated to determine the monetary value. This value depends on the subscription fund collected and the total sum of the reward scores. Then, the subscription fund is distributed to the users according to their reward scores.

The reward scores represent a reputation rating, and the reward scores obtained for various activities are accumulated. The accumulation of reward scores has been kept for the last five years. The pseudocode of the algorithm for reward score calculation is provided in Algorithm 1.

Algorithm 1. Reward score calculation

```
Input parameters:
    Rw1: CTI producer reward score;
    Rw2: CTI consumer reward score;
    Rw3: CTI reviewer reward score;
    Ps: penalty score;
    PID: CTI producer ID;
    CID: CTI consumer ID;
    Prw: PID CTI producer reward score;
    /* Reward score for one year */
    Crw: CID CTI consumer reward score;
    /* Reward score for one year */
    Prs: PID CTI producer rating score;
    /* Reward score for five years */
    Crs: CID CTI consumer rating score;
    /* Reward score for five years */
    Rating: weighted sum of quality factors of metrics.
Result: Reward scores and rating scores calculated for PID and CID.
    If PID provided CTI data
        Prw = Prw + Rw1;
        Prs = Prs + Rw1;
    If CID have requested the CTI data provided
        Crw = Crw + Rw2;
        Crs = Crs + Rw2;
    If CID reviewed CTI data
        Crw = Crw + Rw3;
        Crs = Crs + Rw3;
```

```
If Rating of CTI data < 0
        Prw = Prw + Ps * Rating;
              Prs = Prs + Ps * Rating;
   Else
              Prw = Prw + Rating;
        Prs = Prs + Rating;
        If PID reviewed CID review
              If review is valid
                    Crw = Crw + Rw3;
                    Crs = Crs + Rw3;
              If PID adds the review to CTI data
                    Prw = Prw + Rw3;
                    Prs = Prs + Rw3;
```

The proposed algorithm looks complex; however, the time complexity of this algorithm is negligent for the following reasons:

1. All data for calculation are stored in the data structures of smart contracts, which are directly accessible. The data structures are detailed in Section 3.3.
2. The algorithm has no loops.
3. The algorithm is only executed in the case of specific events, either on the provision of new CTI data or on the provision of new CTI data reviews.

3.3. Sharing of Sensitive Information

A channel support is required to ensure the sharing of sensitive CTI data according to the TLP [30]. A channel in the Hyperledger Fabric network is a private subnet of communication between two or more specific network members. A channel replicates the structure of the whole blockchain: peers, the shared ledger, chaincode applications, and the ordering service node. Each transaction on the network is executed on a channel. Only authenticated and authorized parties to the specific channel are allowed to transact on that channel. Each party joining a channel has their own identity assigned by a membership service provider that is responsible for the authentication of parties to the specific channel and providing the services designed on that channel. Although any party can belong to and take part in multiple channels, the data from one ledger on one channel cannot pass to another. The separation of ledgers, according to the channels, is defined and implemented by the configuration chaincode and membership service provider. This isolation of parties and ledger data ensures the privacy and confidentiality of the transactions.

The TLP [30] has four colors: red, amber, green, and clear (previously known as white). However, the color amber comes in two varieties, TLP:AMBER+STRICT and TLP:AMBER. TLP:AMBER+STRICT restricts the disclosure of information to the participant's organization, while TLP:AMBER restricts the disclosure of information to the participant's organization and its clients. The TLP is implemented at its full scale (Figure 2).

As shown in Figure 2, five channels are organized within the Hyperledger Fabric blockchain. The channels are named according to the sensitivity of the information shared on these channels. To obtain access to a specific channel, clients pay a subscription fee, as explained in the previous subsection, except for access to the Clear channel, which has no subscription fee. The fee depends on the sensitivity of information—for more sensitive information, the fee is higher. Clients with access to the channel containing highly sensitive information also have access to those with less sensitive information. Clients with access to the Clear channel have the same possibilities as the clients of other channels, except they do not participate in the distribution of subscription funds.

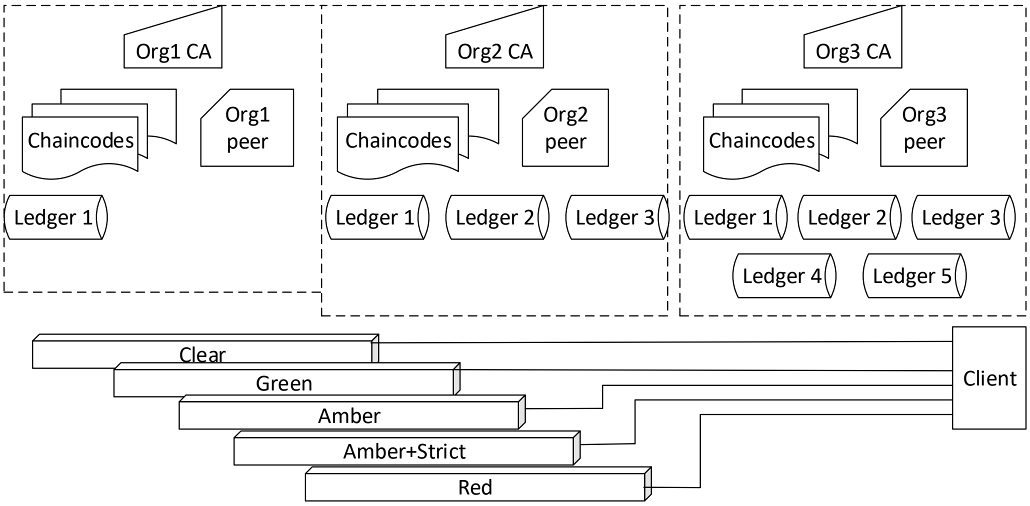


Figure 2. View of Hyperledger Fabric network and client.

As shown in Figure 2, Org1 only has access to the Clear channel. This means that Org1 did not pay a subscription fee. Org2 has access to the Clear, Green, and Amber channels. This means that Org2 has paid the subscription fee required for access to the Amber channel. Org3 has access to all of the available channels, meaning that they paid the highest subscription fee.

For off-chain storage, our design uses the Interplanetary File System (IPFS), which is open-source and provides a distributed file storage system. The IPFS supplies a unique hash for stored files, which has addressed content. The hash, which is 46 bytes long, is updated every time the content of the file is updated [31]. Only this hash is stored in the blockchain; this way, a significant reduction in the amount of storage needed for the blockchain is obtained. In addition, the IPFS enhances scalability, as it enables concurrent access to the stored files.

3.4. Implementation of the Model in the Blockchain

The functionality of the model is implemented using smart contracts. The data structures used in the smart contracts are presented in Figure 3.

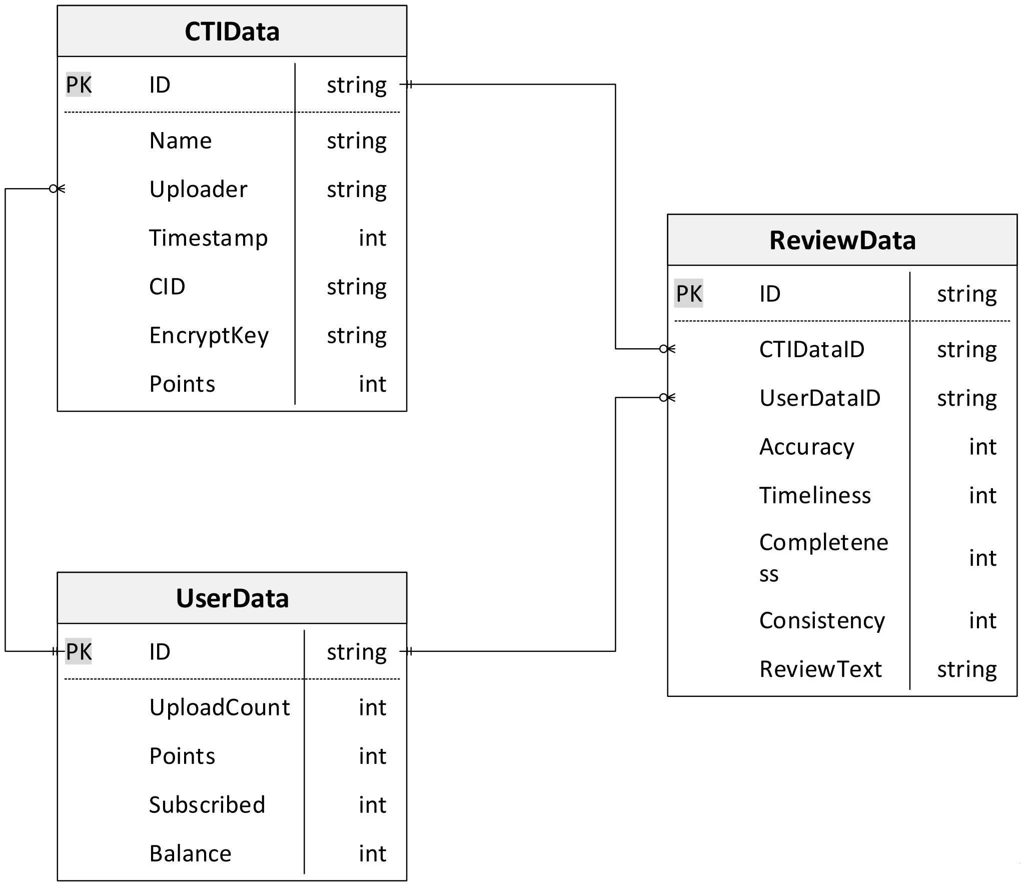
In the figure, “CTIData” represents a single entry, and “Points” denotes a rating score for the CTI data. These points are determined by the reviewers after the entry is uploaded, meaning that the score is not assigned to the CTI data instantly. However, the reward score is assigned instantly to the CTI data producer to encourage them to share the data. The reward score for the CTI data producer can be either increased or decreased, depending on the reviews provided by the CTI data consumers.

“UserData” includes a collected rating score (Points) for user activity and user subscription for CTI data.

“ReviewData” refers to the permission for users to submit reviews for CTI data entries, specifying the user ID and CTI data ID. Predefined quality indicators of CTI data are included in ReviewData. Optional review text can also be provided.

The general process of uploading and retrieving CTI data is depicted in Figure 4.

Figure 4 does not include the operation for client registration with the blockchain, as these operations are generic for any kind of permissioned blockchain. We can observe that the numbers assigned to the operations show their sequence. The process starts by uploading new CTI data into the off-chain file storage IPFS. The operation is accomplished by the CTI data producer. We can also observe that the STIX data format is preferred for CTI data. The operation of uploading CTI data is detailed in Figure 5.



CTIData

PK	ID	string
	Name	string
	Uploader	string
	Timestamp	int
	CID	string
	EncryptKey	string
	Points	int

ReviewData

PK	ID	string
	CTIDataID	string
	UserDataID	string
	Accuracy	int
	Timeliness	int
	Completeness	int
	Consistency	int
	ReviewText	string

UserData

PK	ID	string
	UploadCount	int
	Points	int
	Subscribed	int
	Balance	int

Figure 3. Data structures used in smart contracts.

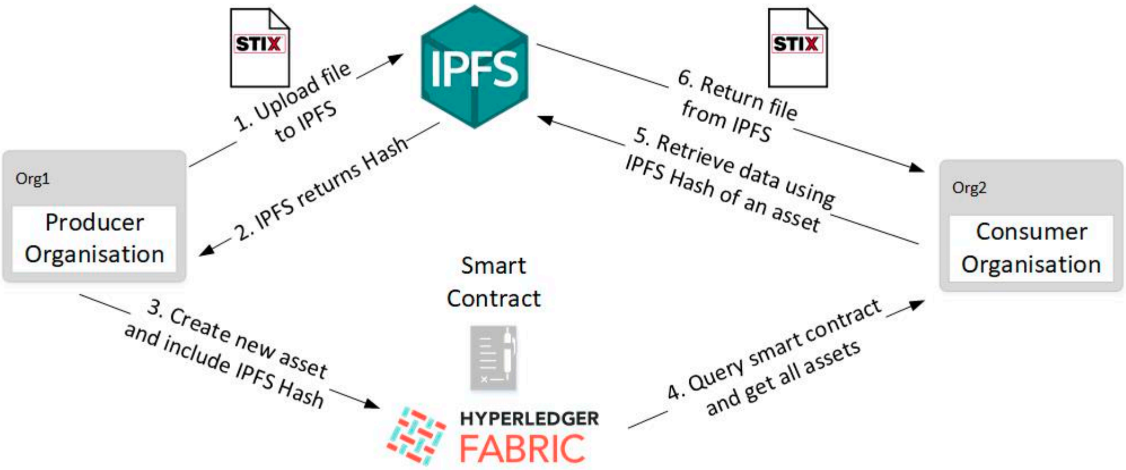


Figure 4. The general process of uploading and retrieving CTI data.

Figure 5 shows that the advanced encryption standard (AES) algorithm is used to encrypt CTI data before uploading it into IPFS. After uploading the CTI data, the CTI data producer registers it with a blockchain. The CTI data consumers are informed, and they start to query the blockchain and download new CTI data.

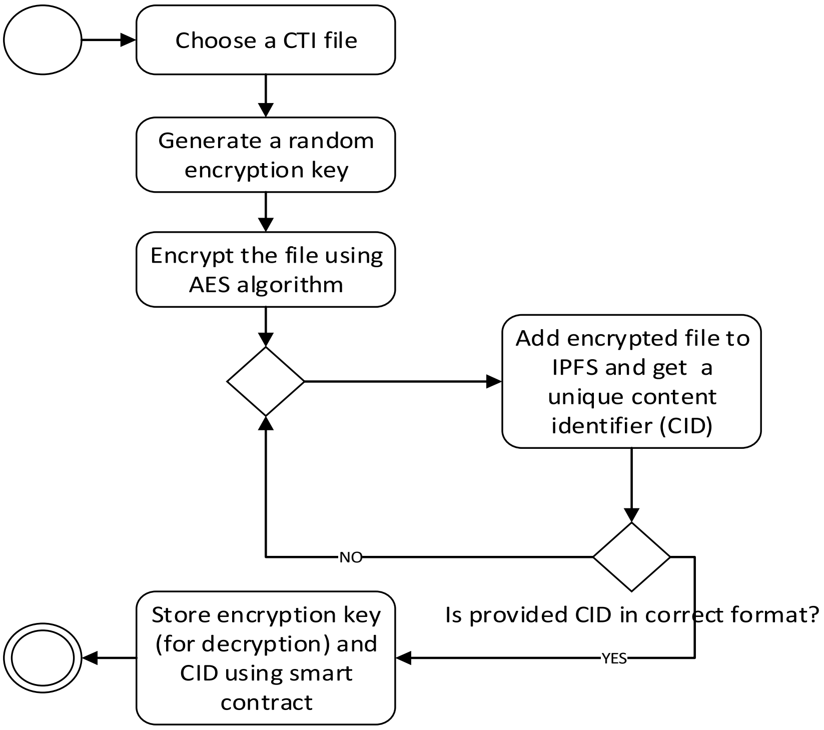

Choose a CTI file
Generate a random encryption key
Encrypt the file using AES algorithm
Add encrypted file to IPFS and get a unique content identifier (CID)
NO
Is provided CID in correct format?
YES
Store encryption key (for decryption) and CID using smart contract

Figure 5. The process of uploading CTI data into IPFS.

Figure 6 presents the activities related to the review of CTI data. These activities are numerated in order of appearance. The labels to be read are as follows:

1. The CTI data consumer submits a review to the Hyperledger Fabric blockchain.
2. The CTI data producer retrieves the review from the Hyperledger Fabric blockchain.
3. The CTI data producer assesses the review. If the review is valid, the producer informs the Hyperledger Fabric blockchain.
4. If the review is valid, the CTI data producer uploads the review next to the CTI data into IPFS.
5. IPFS returns a new hash for the CTI data, since the content of the data has changed.

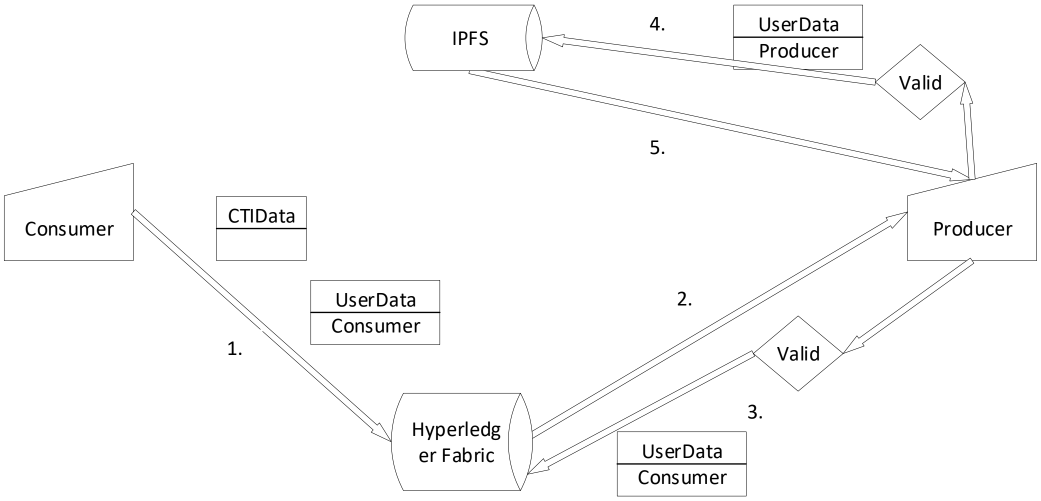


Figure 6. Workflow of review of CTI data.

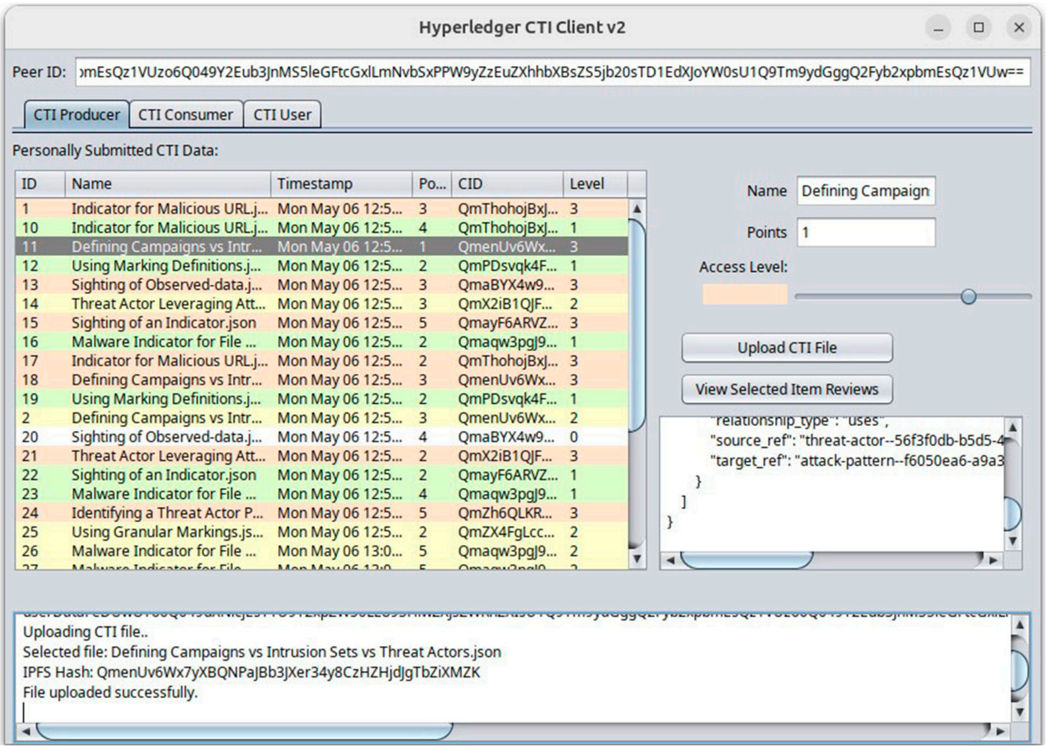
When a CTI data consumer submits a review of CTI data to the blockchain, the CTI data are assigned a score. The CTI data consumer also obtains a score for the provided review. Then, the producer of the CTI data downloads the review from the blockchain and assesses the validity of the review. If the review is valid, the CTI data producer informs the blockchain. The CTI data consumer obtains an additional score for the valid review. Then, the CTI data producer uploads the review next to the CTI data into IPFS. The CTI data producer is awarded a score for this action. Finally, the IPFS returns a new hash for the CTI data, which must be registered with the blockchain.

4. Experimental Evaluation and Discussion

4.1. Experimental Evaluation

Hyperledger Fabric was chosen as a development platform. To configure the Hyperledger Fabric blockchain, the Fabric-SDK-Java toolkit was downloaded, and the Java language was used for the client interface programming, while the Golang language was chosen as the development language for smart contracts. The permissioned blockchain was developed on two virtual machines (VMs). Each VM had two virtual CPU cores, 8 GB of RAM, 10 GB of nonvolatile storage, and a physical machine with an Intel Core i7 and 16 GB of RAM. The Python Web3 Library monitored the behavior of the network. Several Docker containers were used for network entities such as membership service provider (MSP), orderer, peers, and clients. All of the data of the configuration were stored in a Docker compose file.

Figure 7 shows the user interface of the designed application.



Peer ID: ›mEsQz1VUzo6Q049Y2Eub3JnMS5leGFtcGxlLmNvbSxPPW9yZzEuZXhhbXBsZS5jb20sTD1EdXJoYW0sU1Q9Tm9ydGggQ2Fyb2xpbmEsQz1VUw==

Personally Submitted CTI Data:

ID	Name	Timestamp	Po...	CID	Level
1	Indicator for Malicious URL.j...	Mon May 06 12:5...	3	QmThohojBxJ...	3
10	Indicator for Malicious URL.j...	Mon May 06 12:5...	4	QmThohojBxJ...	1
11	Defining Campaigns vs Intr...	Mon May 06 12:5...	1	QmenUv6Wx...	3
12	Using Marking Definitions.j...	Mon May 06 12:5...	2	QmPDsvqk4F...	1
13	Sighting of Observed-data.j...	Mon May 06 12:5...	3	QmaBYX4w9...	3
14	Threat Actor Leveraging Att...	Mon May 06 12:5...	3	QmX2iB1QJF...	2
15	Sighting of an Indicator.json	Mon May 06 12:5...	5	QmayF6ARVZ...	3
16	Malware Indicator for File ...	Mon May 06 12:5...	2	Qmaqw3pgJ9...	1
17	Indicator for Malicious URL.j...	Mon May 06 12:5...	2	QmThohojBxJ...	3
18	Defining Campaigns vs Intr...	Mon May 06 12:5...	3	QmenUv6Wx...	3
19	Using Marking Definitions.j...	Mon May 06 12:5...	2	QmPDsvqk4F...	1
2	Defining Campaigns vs Intr...	Mon May 06 12:5...	3	QmenUv6Wx...	2
20	Sighting of Observed-data.j...	Mon May 06 12:5...	4	QmaBYX4w9...	0
21	Threat Actor Leveraging Att...	Mon May 06 12:5...	2	QmX2iB1QJF...	3
22	Sighting of an Indicator.json	Mon May 06 12:5...	2	QmayF6ARVZ...	1
23	Malware Indicator for File ...	Mon May 06 12:5...	4	Qmaqw3pgJ9...	1
24	Identifying a Threat Actor P...	Mon May 06 12:5...	5	QmZh6QLKR...	3
25	Using Granular Markings.js...	Mon May 06 12:5...	2	QmZX4FgLcc...	2
26	Malware Indicator for File ...	Mon May 06 13:0...	5	Qmaqw3pgJ9...	2
27	Malware Indicator for File	Mon May 06 13:0...	5	Qmaqw3pgJ9...	2

Name: Defining Campaign

Points: 1

Access Level:

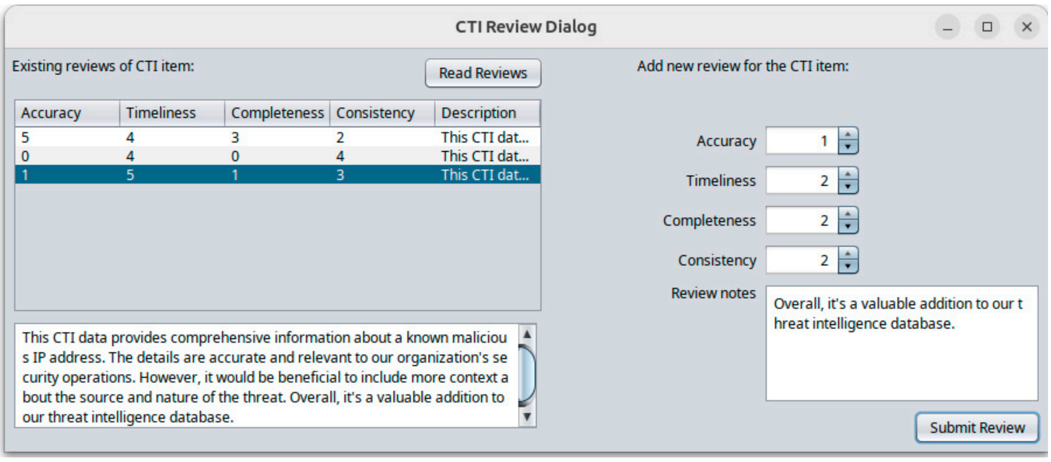
```
            "relationship_type": "uses",
            "source_ref": "threat-actor--56f3f0db-b5d5-4
            "target_ref": "attack-pattern--f6050ea6-a9a3
        }
    ]
}
```

```
Uploading CTI file..
Selected file: Defining Campaigns vs Intrusion Sets vs Threat Actors.json
IPFS Hash: QmenUv6Wx7yXBQNPaJBb3JXer34y8CzHZHjdJgTbZiXMZK
File uploaded successfully.
```

Figure 7. The user interface of the designed application.

The application's user interface is divided into three areas: CTI data producer, CTI data consumer, and CTI data user. These areas are implemented in separate panels. The view of the CTI data producer is presented in Figure 7. The interface of the CTI data producer enables the CTI file to be uploaded into IPFS, as well as the viewing and reading of a review of the uploaded file submitted by a CTI data consumer, and adding the review to the uploaded CTI file. This panel also includes a list of CTI data submitted by the current CTI data producer. The characteristics of the CTI data are shown in this list.

The CTI data consumer panel enables the CTI file to be downloaded and the writing of a review for the downloaded file (Figure 8). The CTI data user panel presents a reputation score for the current year, a reputation score for a five-year period, and the level of the CTI data user.



Existing reviews of CTI item:

Accuracy	Timeliness	Completeness	Consistency	Description
5	4	3	2	This CTI dat...
0	4	0	4	This CTI dat...
1	5	1	3	This CTI dat...

This CTI data provides comprehensive information about a known malicious IP address. The details are accurate and relevant to our organization's security operations. However, it would be beneficial to include more context about the source and nature of the threat. Overall, it's a valuable addition to our threat intelligence database.

Add new review for the CTI item:

Accuracy 1
Timeliness 2
Completeness 2
Consistency 2
Review notes Overall, it's a valuable addition to our t hreat intelligence database.

Figure 8. The user interface for the reviewer.

The reviewer's user interface (Figure 8) is divided into two areas: the left side for reading reviews, and the right side for writing and submitting reviews.

To evaluate the ratio of subscription fees and reward scores for a one-year period, a simulation was performed. The goal of the simulation was to establish whether the algorithm for reward score calculation assigns the rewards in such a way that the CTI data producers and consumers are motivated to take part in the network to share CTI. The simulation was conducted in MATLAB. The initial values of the simulation parameters are provided in Table 2.

Table 2. Initial values of simulation parameters.

Parameter Definition	Value
Reward of CTI data producer	100
Reward of CTI data consumer	10
Reward of CTI data reviewer	10
Subscription fee	EUR 500
Number of produced CTI data	2
Weight coefficients of quality factors (all are equal)	0.5
All CTI data consumers download and read provided CTI data	-

Based on the initial values of the parameters, we conducted an evolutionary simulation [23] of the reward score values and the potential benefits of being an active participant in the CTI data-sharing process. During the evolutionary simulation, only the number of participants changed, as this is the most variable value and is not controlled by the proposed approach. We simulated the worst-case scenario for the process, as all of the rewards will be consumed:

1. All participants demonstrate maximum activity.
2. All of the CTI data provided are of high quality.
3. All of the reviews are valid.

A similar worst-case scenario for simulation was chosen in [12]. The simulation values are provided in Table 3. We chose EUR 500 as the basic value for the subscription fee. This value is only a small fraction, compared to the average ransom of USD 812,380 paid in 2022, according to a SOPHOS report [32]. Moreover, the value of ransom payments almost doubled to USD 1,542,333 in 2023. The global average cost of a data breach is even higher, according to an IBM report [33], which was USD 4.45 million in 2023 and demonstrated a 15% increase over the last 3 years. The value of the subscription fee is very important for the monetary reward of participants in the network. However, we cannot set the subscription fee too high, as it must be an attractive and affordable investment for the participants. For simulation purposes, the absolute value of the subscription fee is not very important, as the relationship between the subscription fee and the reward score in euros is straightforward. For example, if we double the value of the subscription fee, the value of the reward score in euros will also be doubled. The most interesting relationship is between the number of participants in the network and the value of the reward score in euros. This relationship is depicted in Figure 9.

Table 3. Simulation of reward scores.

Subscription Fee is EUR 500, CTI Data Producer Reward Score is 130			
Number of Participants	**Reviewer Reward Score**	**Ordinary CTI Data Consumer Reward Score**	**Value of Score in Euros**
10 10	30 × 3 = 90 30 × 3 = 90	6 × 10 = 60 6 × 10 = 60	EUR 8.92
20 20	30 × 3 = 90 30 × 3 = 90	16 × 10 = 160 16 × 10 = 160	EUR 13.15
30 30	30 × 3 = 90 30 × 3 = 90	26 × 10 = 260 26 × 10 = 260	EUR 15.62
40 40	30 × 3 = 90 30 × 3 = 90	36 × 10 = 360 36 × 10 = 360	EUR 17.24
50 50	30 × 3 = 90 30 × 3 = 90	46 × 10 = 460 46 × 10 = 460	EUR 18.38
60 60	30 × 3 = 90 30 × 3 = 90	56 × 10 = 560 56 × 10 = 560	EUR 19.23
70 70	30 × 3 = 90 30 × 3 = 90	66 × 10 = 660 66 × 10 = 660	EUR 19.88
80 80	30 × 3 = 90 30 × 3 = 90	76 × 10 = 760 76 × 10 = 760	EUR 20.40
90 90	30 × 3 = 90 30 × 3 = 90	86 × 10 = 860 86 × 10 = 860	EUR 20.83
100 100	30 × 3 = 90 30 × 3 = 90	96 × 10 = 960 96 × 10 = 960	EUR 21.18

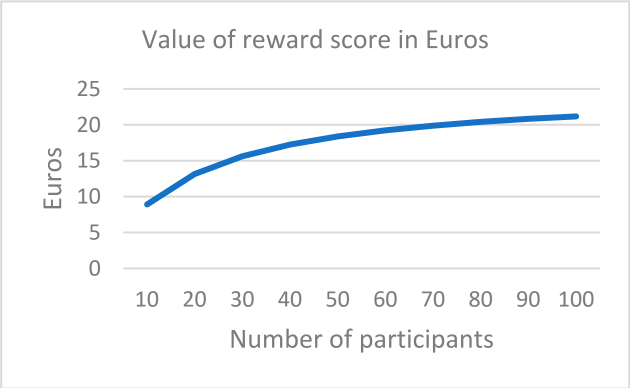


Figure 9. Value of reward score based on the number of participants.

Figure 9 shows that an increase in the number of participants in the network invokes an increase in the value of the reward score in euros. This increase slows down with the increasing number of participants. This tendency is in accordance with economic logic, where a bigger profit is usually related to a larger number of CTI data consumers. Thus, there is no need to regulate the reward score of the CTI data producers and consumers when the number of participants in the network increases.

The parameter value of the amount of provided CTI data was held constant during the simulation. However, when the number of participants in the network increases, the amount of provided CTI data can also increase. In such a case, the value of the reward score in euros will be smaller in comparison with the current situation, as the number of collected rating scores will increase. For example, let us consider a situation whereby 50 participants are available in the network and three cases of different CTI data are provided. In this case, the value of the reward score in euros is 12.25 in comparison with the value for two CTI data, which is 18.38. The obtained value for three pieces of CTI data is much smaller than for two, but is higher than for 10 participants. Hence, the effect of a larger number of participants still holds, and there is no need to regulate the reward score of the CTI data producers and consumers when the amount of produced CTI data increases.

4.2. Results and Discussion

The key features of our innovation that distinguish it from other research in the field of incentivized CTI data sharing are as follows: the Hyperledger Fabric blockchain implementation, off-chain IPFS storage, a new incentive model, an algorithm for calculating reward scores, and the implementation of TLP for sensitive CTI data sharing.

Ethereum and Hyperledger Fabric are two open-access core platforms for developing applications on blockchains [34]. The features of Hyperledger Fabric blockchain, which are consistent with the task solved, are as follows:

- Hyperledger Fabric is a permissioned blockchain that enables the achievement of confidentiality and privacy goals through its design.
- Hyperledger Fabric supports channel-based privacy that is important for the implementation of the TLP. This feature is unique in comparison to Ethereum blockchain.
- Hyperledger Fabric does not require the use of digital currency to operate. This feature is unique in comparison to Ethereum blockchain.
- Smart contracts, called chaincodes in Hyperledger Fabric, are developed using well-known popular programming languages such as Golang, Java, and Node.js. There is no need to learn a specific language, as is the case for Ethereum.
- Hyperledger Fabric enables the low latency of transaction confirmation, as the confirmation can be acknowledged within only a few organizations [35].

The attractive and desirable features of Hyperledger Fabric have also been acknowledged by other researchers [14,16,19,21] in the field of incentivized CTI data sharing.

The next feature of the current innovation is off-chain IPFS storage. Shared CTI data can occupy a large volume; however, blockchains have limited data storage capacity. One of the recognized alternatives to expand blockchain data storage is the use of the IPFS [36]. The IPFS is an open-source data storage system that stores data in a distributed manner using key-value data access. The file is split into chunks after being uploaded into the IPFS. Each chunk is represented by a content-related hash key. The chunks are related to each other, and the hash key of the root chunk is stored in a blockchain ledger. The IPFS is a public-nature network. Therefore, any participant node can download the data from the IPFS. To ensure confidentiality, the data must be encrypted before being uploaded. We used the AES 256 algorithm to encrypt the data. Only two research works [15,19] from those reviewed used the IPFS to store data off-chain. Menges et al. [15] used the AES 256 algorithm to encrypt data, as we did in our case. In addition, AES symmetric keys were encrypted using the RSA public crypto system to share the keys over the network, as the network used was public. Nguyen et al. [19] did not specify a particular encryption algorithm. However, again, the encryption doubled despite the Hyperledger Fabric blockchain being used. The symmetric keys are encrypted using an unspecified public crypto system. This double encryption is related to the CTI data verification process.

The next feature of our innovation is the new incentive model. Many authors [11–19,21,23] have used incentives to either enhance trust in CTI data or motivate sharing, but they never pursued both goals together. However, Jesus et al. [22] noticed that the CTI data-sharing model must include economic incentives and maintain reputation management at the same time. We followed the observation of Jesus et al. [22] and proposed a new incentive model that combines economic incentives and reputation management. The economic incentives are based on a subscription fee. The use of a subscription fee was also proposed by Nguyen et al. [19], although it was used quite differently, as a discount was given to the verifiers and contributors towards the next subscription. First, Nguyen et al. [19] did not elaborate on the amount of the subscription fee. Second, they did not provide details of the amount of discount. Third, they did not offer discounts for CTI data consumers, meaning that CTI data consumers were not motivated to actively participate in the CTI data-sharing process. Our proposed model maintains the reputation of all participants in the network, including CTI data producers and consumers, as both roles are interchangeable. The maintenance of the reputation system increases the users' trust in the CTI data-sharing process.

The next feature of our innovation is the algorithm for calculating reward scores. The proposed algorithm is based on a large number of variables. To explore the relationship between different variables, we conducted an evolutionary simulation for selected values when the number of participants increased. The result of the simulation showed that the selected values and the proposed algorithm are in accordance with economic laws. Hence, we can conclude that the proposed algorithm for reward score calculation motivates users to share CTI data. Simulation was also used as a tool by other researchers in the field [12,13,18,23]. Riesco et al. [12] used a Monte Carlo simulation to check the viability of their proposed incentivized CTI data-sharing model. Gong and Lee [13] verified the influence of malicious contributors using simulation, although the simulation scheme and tools were not discussed. Chatziamanetoglou and Rantos [18] used a probabilistic simulation to check the tolerance of the proposed algorithm against malicious validators. Ma et al. [23] applied an evolutionary simulation in MATLAB to check the impact of the proposed incentive strategy.

The final distinguishing feature of our innovation is the implementation of TLP for CTI data sharing. Of all of the reviewed studies in the field of incentivized CTI data sharing, only Nguyen et al. [19] considered the implementation of the TLP. The authors discussed the implementation of four channels: white, green, amber, and red. Nguyen et al. [19] observed that data can be freely disclosed outside the network in the white channel. However, they did not provide details on how the data can be disclosed outside of the network when a permissioned blockchain is used. We implemented five channels for CTI data disclosure, according to the latest version of the TLP [30], as five colors are now available.

A summary of the discussion is provided in Table 4. The asterisk (*) used means that the feature was implemented.

Table 4. Comparison with other incentive models.

Reference	Features							
	Prototype Implemented	**View of Prototype Presented**	**Incentive Reputation**	**Incentive Monetary**	**Sharing of Sensitive Data**	**Implementation of TLP**	**Sharing of Large Data**	**Simulation Used**
Wu et al. [11]			*					
Riesco et al. [12]	*	*		*				*
Gong and Lee [13]			*					*
Gonçalo et al. [14]	*		*		*			
Menges et al. [15]	*	*		*			*	
Huff and Li [16]	*			*	*			
Chatziamanetoglou and Rantos [18]			*					*
Nguyen et al. [19]				*	*	*	*	
Zhang et al. [21]	*		*					
Ma et al. [23]			*					*
Proposed model	*	*	*	*	*	*	*	*

The summary of implemented features presented in Table 4 clearly indicates the superiority of our proposed model, compared to existing incentive models in the field.

5. Conclusions

A review of the related literature revealed that many authors have used incentives to either increase confidence in CTI data or to motivate the sharing of the data, but they have not pursued both goals together. We presented a model for sharing CTI data that includes both monetary incentives and reputation management. The combination of two incentives into a single model is the main novelty and contribution of our model. The monetary incentive stimulates the participation of the users in the CTI data-sharing process. The reputation incentive is important to ensure trust in the shared CTI data. The model was implemented on a private Hyperledger Fabric blockchain, enabling the sharing of sensitive CTI data. The unique feature of the Hyperledger Fabric blockchain (i.e., channel-based privacy) was utilized to implement the sharing of sensitive CTI data in accordance with the latest version of the Traffic Light Protocol. The CTI data are stored off-chain, as they can be large in volume. The hash of the CTI data is only stored on the chain. The key elements of the model to support the monetary incentive are a subscription fee and a reward score for the activity shown. The network's users play the role of either CTI data producer or CTI data consumer. CTI data consumers are encouraged to write a review for newly submitted CTI data. However, the quality of these reviews is not always satisfactory or manageable. Therefore, reviewing CTI data is a limiting factor in our model. Our next research direction involves the development of a method to automatically assess the quality of CTI data.

Author Contributions: Conceptualization, V.J. and A.V.; Methodology, V.J.; Software, D.B.; Validation, V.J., D.B. and B.M.; Formal Analysis, V.J.; Investigation, V.J.; Resources, V.J. and D.B.; Data Curation, V.J. and D.B.; Writing—Original Draft Preparation, V.J.; Writing—Review and Editing, B.M.; Visualization, B.M.; Supervision, A.V.; Project Administration, A.V.; Funding Acquisition, A.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Economic Revitalization and Resilience Enhancement Plan "New Generation Lithuania" as part of the execution of the "Mission-driven Implementation of Science and Innovation Programmes" project (No. 02-002-P-0001).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Brown, R.; Nickels, K. SANS 2023 CTI Survey: Keeping Up with a Changing Threat Landscape. 17 July 2023. Available online: https://www.sans.org/white-papers/2023-cti-survey-keeping-up-changing-threat-landscape/ (accessed on 7 March 2024).
2. Moubarak, J.; Bassil, C.; Antoun, J. On the dissemination of Cyber Threat Intelligence through Hyperledger. In Proceedings of the 2021 17th International Conference on the Design of Reliable Communication Networks (DRCN), Milano, Italy, 19–22 April 2021; pp. 1–6. [CrossRef]
3. Villalón-Huerta, A.; Ripoll-Ripoll, I.; Marco-Gisbert, H. Key Requirements for the Detection and Sharing of Behavioral Indicators of Compromise. *Electronics* **2022**, *11*, 416. [CrossRef]
4. Chatziamanetoglou, D.; Rantos, K. Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. *Computers* **2024**, *13*, 60. [CrossRef]
5. Ainslie, S.; Thompson, D.; Maynard, S.; Ahmad, A. Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Comput. Secur.* **2023**, *132*, 103352. [CrossRef]
6. Dunnett, K.; Pal, S.; Jadidi, Z. Challenges and Opportunities of Blockchain for Cyber Threat Intelligence Sharing. In *Secure and Trusted Cyber Physical Systems. Smart Sensors, Measurement and Instrumentation*; Pal, S., Jadidi, Z., Foo, E., Eds.; Springer: Cham, Switzerland, 2022; Volume 43. [CrossRef]
7. Ihle, C.; Trautwein, D.; Schubotz, M.; Meuschke, N.; Gipp, B. Incentive Mechanisms in Peer-to-Peer Networks—A Systematic Literature Review. ACM Comput. *Surv. July* **2023**, *55*, 308. [CrossRef]

8. Wagner, T.D.; Mahbub, K.; Palomar, E.; Abdallah, A.E. Cyber threat intelligence sharing: Survey and research directions. *Comput. Secur.* **2019**, *87*, 101589. [CrossRef]
9. Olaifa, M.; van Vuuren, J.J.; Du Plessis, D.; Leenen, L. Security Issues in Cyber Threat Intelligence Exchange: A Review. In *Intelligent Computing. SAI 2023. Lecture Notes in Networks and Systems*; Arai, K., Ed.; Springer: Cham, Switzerland, 2023; Volume 739, pp. 1308–1319. [CrossRef]
10. Lin, S.-Y.; Zhang, L.; Li, J.; Ji, L.-L.; Sun, Y. A survey of application research based on blockchain smart contract. *Wireless Netw.* **2022**, *28*, 635–690. [CrossRef]
11. Wu, Y.; Qiao, Y.; Ye, Y.; Lee, B. Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019; pp. 474–481. [CrossRef]
12. Riesco, R.; Larriva-Novo, X.; Villagra, V.A. Cybersecurity threat intelligence knowledge exchange based on blockchain. *Telecommun. Syst.* **2020**, *73*, 259–288. [CrossRef]
13. Gong, S.; Lee, C. BLOCIS: Blockchain-Based Cyber Threat Intelligence Sharing Framework for Sybil-Resistance. *Electronics* **2020**, *9*, 521. [CrossRef]
14. Gonçalo, R.; Pedrosa, T.; Lopes, R.P. An Architecture for Sharing Cyber-Intelligence Based on Blockchain. In *Blockchain and Applications. BLOCKCHAIN 2020. Advances in Intelligent Systems and Computing*; Prieto, J., Pinto, A., Das, A., Ferretti, S., Eds.; Springer: Cham, Switzerland, 2020; Volume 1238. [CrossRef]
15. Menges, F.; Putz, B.; Pernul, G. DEALER: Decentralized incentives for threat intelligence reporting and exchange. *Int. J. Inf. Secur.* **2021**, *20*, 741–761. [CrossRef]
16. Huff, P.; Li, Q. A Distributed Ledger for Non-attributable Cyber Threat Intelligence Exchange. In *Security and Privacy in Communication Networks. SecureComm 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Garcia-Alfaro, J., Li, S., Poovendran, R., Debar, H., Yung, M., Eds.; Springer: Cham, Switzerland, 2021; Volume 398. [CrossRef]
17. Chatziamanetoglou, D.; Rantos, K. CTI Blockchain-Based Sharing using Proof-of-Quality Consensus Algorithm. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021; pp. 331–336. [CrossRef]
18. Chatziamanetoglou, D.; Rantos, K. Blockchain-Based Cyber Threat Intelligence Sharing Using Proof-of-Quality Consensus. *Secur. Commun. Netw.* **2023**, *2023*, 3303122. [CrossRef]
19. Nguyen, K.; Pal, S.; Jadidi, Z.; Dorri, A.; Jurdak, R. A Blockchain-Enabled Incentivised Framework for Cyber Threat Intelligence Sharing in ICS. In Proceedings of the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Pisa, Italy, 21–25 March 2022; pp. 261–266. [CrossRef]
20. Homan, D.; Shiel, I.; Thorpe, C. A New Network Model for Cyber Threat Intelligence Sharing using Blockchain Technology. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; pp. 1–6. [CrossRef]
21. Zhang, X.; Miao, X.; Xue, M. A Reputation-Based Approach Using Consortium Blockchain for Cyber Threat Intelligence Sharing. *Secur. Commun. Netw.* **2022**, *2022*, 7760509. [CrossRef]
22. Jesus, V.; Bains, B.; Chang, V. Sharing Is Caring: Hurdles and Prospects of Open, Crowd-Sourced Cyber Threat Intelligence. *IEEE Trans. Eng. Manag.* **2023**, *71*, 6854–6873. [CrossRef]
23. Ma, X.; Yu, D.; Du, Y.; Li, L.; Ni, L.W.; Lv, H. A Blockchain-Based Incentive Mechanism for Sharing Cyber Threat Intelligence. *Electronics* **2023**, *12*, 2454. [CrossRef]
24. Sakellariou, G.; Fouliras, P.; Mavridis, I.; Sarigiannidis, P. A Reference Model for Cyber Threat Intelligence (CTI) Systems. *Electronics* **2022**, *11*, 1401. [CrossRef]
25. Sakellariou, G.; Fouliras, P.; Mavridis, I. A Methodology for Developing & Assessing CTI Quality Metrics. *IEEE Access* **2024**, *12*, 6225–6238. [CrossRef]
26. Grispos, G.; Glisson, W.B.; Storer, T. How good is your data? Investigating the quality of data generated during security incident response investigations. In Proceedings of the 52nd Hawaii International Conference on System Sciences Scholar Space Hawaii International, Maui, HI, USA, 8–11 April 2019; pp. 7156–7165. Available online: https://hdl.handle.net/10125/60152 (accessed on 4 April 2024).
27. Dalziel, H. A Problem Well-Defined is Half-Solved. In *How to Define and Build an Effective Cyber Threat Intelligence Capability*; Elsevier: London, UK, 2015; pp. 3–6.
28. Schlette, D.; Böhm, F.; Caselli, M.; Pernul, G. Measuring and visualizing cyber threat intelligence quality. *Int. J. Inf. Secur.* **2021**, *20*, 21–38. [CrossRef]
29. Mavzer, K.B.; Konieczna, E.; Alves, H.; Yucel, C.; Chalkias, I.; Mallis, D.; Cetinkaya, D.; Sanchez LA, G. Trust and Quality Computation for Cyber Threat Intelligence Sharing Platforms. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021; pp. 360–365. [CrossRef]
30. America's Cyber Defense Agency, USA. Traffic Light Protocol (TLP) Definitions and Usage. 22 August 2022. Available online: https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage (accessed on 4 April 2024).

31. Kumar, R.; Tripathi, R. Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain. In Proceedings of the 2019 Fifth International Conference on Image Information Processing (ICIIP), Shimla, India, 15–17 November 2019; pp. 246–251. [CrossRef]
32. SOPHOS. The State of Ransom 2023. Available online: https://www.sophos.com/en-us/content/state-of-ransomware (accessed on 4 March 2024).
33. IBM. Cost of a Data Breach Report 2023. Available online: https://www.ibm.com/reports/data-breach (accessed on 7 March 2024).
34. Pahlevan, M.; Ionita, V. Secure and Efficient Exchange of Threat Information Using Blockchain Technology. *Information* **2022**, *13*, 463. [CrossRef]
35. Ali, H.; Ahmad, J.; Jaroucheh, Z.; Papadopoulos, P.; Pitropakis, N.; Lo, O.; Abramson, W.; Buchanan, W.J. Trusted Threat Intelligence Sharing in Practice and Performance Benchmarking through the Hyperledger Fabric Platform. *Entropy* **2022**, *24*, 1379. [CrossRef] [PubMed]
36. Verma, G.; Kanrar, S. Secure document sharing model based on blockchain technology and attribute-based encryption. *Multimed Tools Appl.* **2024**, *83*, 16377–16394. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.