Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing

Yichang Wu
Athlone Institute of Technology
Athlone, Ireland
w.yichang@research.ait.ie

Yuansong Qiao
Athlone IT
Athlone, Ireland
ysqiao@research.ait.ie

Yuhang Ye
Athlone IT
Athlone, Ireland
yye@research.ait.ie

Brian Lee
Athlone IT
Athlone, Ireland
blee@ait.ie

***Abstract*—Threat intelligence sharing is posited as an important aid to help counter cybersecurity attacks and a number of threat intelligence sharing communities exist. There is a general consensus that many challenges remain to be overcome to achieve fully effective sharing, including concerns about privacy, negative publicity, policy/legal issues and expense of sharing, amongst others. One recent trend undertaken to address this is the use of decentralized blockchain based sharing architectures. However while these platforms can help increase sharing effectiveness they do not fully address all of the above challenges. In particular, issues around *trust* are not satisfactorily solved by current approaches. In this paper, we describe a novel trust enhancement framework -TITAN- for decentralized sharing based on the use of P2P reputation systems to address open trust issues. Our design uses blockchain and Trusted Execution Environment technologies to ensure security, integrity and privacy in the operation of the threat intelligence sharing reputation system.**

***Index Terms*—Cyber Security, Threat Intelligence Sharing, Reputation, Blockchain, TEE**

I. Introduction

The incidence of cyber attacks and threats is continually growing, as can be attested by the numerous threat and malware reports on the Internet such as those from the leading security solution vendors. Organizations are being encouraged to share *Threat Intelligence (TI)* i.e. information of received attacks and other cyber security experiences with each other, as a means to counter such threats. Such sharing will give organizations a broader view of the current cybersecurity picture, e.g. at a regional, national or sectoral level, and thus increase their level of cyber situational awareness. This will in turn improve their attack preparedness (security posture) and thus decrease their risk of cyber attack.

Despite the clear benefits to be gained, and the presence of the large number of sharing platforms, there are still substantial barriers remaining to sharing threat intelligence. These include organizations concerns about privacy (confidentiality of information), negative publicity, policy and legal issues and cost amongst others [1]. Furthermore there are fears that not all participants will contribute equally i.e. some parties may 'freeride' and consume more than they contribute [2].

This publication has emanated from research conducted with the financial support of Science Foundation Ireland (SFI) under Grant Number SFI 16/RC/3918, co-funded by the European Regional Development Fund and Government of Ireland - International Education Scholarship (GOI-IES) 2018.

Threat intelligence is normally shared between members of well defined groups or *communities* with varying degrees of openness in sharing. Communities may be *private* i.e. closed with sharing only between the members of the community or *public* i.e. fully open with all information available to anyone; or they may be somewhere in between [3]. Additionally some companies provide information commercially. Recently there is evidence of a move away from the existing semi-static community model towards a more decentralized, dynamic based model - inspired (and enabled) in large part by the increasing trend, in many fields, to share data and information via blockchain based markets. One such example, based on Hyperledger, is TRADE from IBM [4]. Other examples can be found in the number of startups - such as Polyswarm [5] - establishing markets for threat intelligence sharing systems. We fully expect this trend to continue and, furthermore, to see current systems evolve in this direction also. A possible blueprint for how a future hybrid centralized/decentralized threat intelligence sharing environment might play out is the *Knowledge Exchange* concept from Serrano [3].

While this emerging model is expected to improve TI sharing many of the challenges outlined above will still exist. Central to these is, we believe, the issue of *Trust*. Trust is a broad topic with sometimes subtle shades of meaning. We identify three type of trust concerns when considering TI sharing: *Trust between Participants, Trust of TI Quality and Trust in the TI Platform (TIP)*. All of these will be of concern in the emerging decentralized TI sharing environment. Trust between participants is needed for participants to engage in sharing in the first place. Trust in the platform helps provide reassurance about engagement in the community through the provision of Information Technology (IT) security mechanisms to support confidentiality, integrity and privacy. Trust in TI quality helps information receivers more efficiently deal with large volumes of TI by selecting only data with required quality levels.

None of the emerging solutions that we have seen fully addresses all of these issues. TRADE does discuss a reputation management system to help address participant trust but few details are provided and they don't at all mention data quality trust. Nor is this issue addressed satisfactorily by the various startups in the area, many of whom also neglect mechanisms for participant trust management. Al-Ibrahim [6] describes an

architectural approach for assessing TI quality but gives no implementation details and does not at all consider blockchain based systems.

Therefore in this paper we introduce a novel trust framework -TITAN (TI sharing Trust enhANcement) based on P2P reputation systems to address the trust issues outlined above. The approach is based on the fact that members of a TI sharing community are logically connected to each other in a P2P manner. Our design uses blockchain and Trusted Execution Environment (TEE) to ensure the security, integrity and confidentiality of the operation of the trust framework. We report herein on the progress of the design to-date and outline the remaining challenges and work to be done.

The structure of the paper is as follows: In Section 2 we provide background information on trust, blockchain and trusted computing technologies. In Section 3 we elaborate on the core issue of TI sharing and identify requirements to ensure trust in emerging platforms. We describe our approach and design in Section 4 while we outline related work in Section 5. Finally we conclude the paper and indicate future research direction in Section 6.

II. Background

A. Notions of Trust

Trust is, in general, a complex and multi-faceted notion. According to Josang [7] it "is a directional relationship between two parties that can be called trustor and trustee" where the former is considered a "thinking entity" capable to assess facts and form judgments and the latter is a person, organization or physical entity. He identifies two main interpretations of trust, viz:

- *Reliability trust* - the perceived reliability of something or somebody; the "subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends".
- *Decision trust* - to view trust as a decision to enter into a situation of dependence.

Josang also considers *Reputation* in the context of relationships between Trustor/Trustee. He notes that trust is a personal judgment about another entity based on various factor whereas "Reputation can be considered as a collective measure of trustworthiness (in the sense of reliability) based on the referrals or ratings from members in a community". Thus a *Trust System* produces a rating that reflects one party's subjective view of another entity's trustworthiness whereas a *Reputation System* rates an entity's trustworthiness (via a reputation score) as seen by the whole community. In this context trustworthiness can be equated to *reliability*.

Trust as a concept is also related to IT security where it can take a variety of meanings. IT computer system security mechanisms provide protection (confidentiality, availability, integrity) to data and compute resources against attacks. Bishop defines a computer system as trustworthy if there is sufficient evidence that it meets specified security requirements [8]. A number of technologies have also been identified as key enablers of system trustworthiness. Two particular such technologies that are significant in this regard are *trusted computing* and *blockchain*. These are discussed later in this section.

Another issue to consider is reputation in P2P systems. Individual peers rate transactions with other peers (trust) and these individual scores can be collected and weighted to produce a reputation score by the reputation system [9]. The amount of information collected from peers can vary according to the needs of the particular P2P system. In a small system a peer may use only its own trust ratings to rank other peers whereas in a larger system a peer may employ a *transitive trust* chain i.e. ask its "friends" (one-hop trusted peers) or "friends of a friend" (multi-hop trusted peers) right up to a *global history* reputation system that collects transaction history for all peers from all peers. Reputation scores can be calculated by centralized entities or in a decentralized manner by all the peers e.g by using an algorithm such as EigenTrust [9]. P2P reputation systems can also take actions to incentivise sharing or punish bad behaviour.

An important issue that relates to P2P trust and reputation is *anonymity*. A P2P system can typically provide various levels of anonymity from no anonymity, through some form of pseudo anonymity to full anonymity that disconnects a user's actions from his real world identity and his other actions [9]. Full anonymity however precludes the use of a reputation system.

B. Trust Technology Enablers

1) Blockchain: Blockchain is a composition of technologies used in decentralized networks to maintain consistency and transparency of a series of transactions between members of a community i.e. a so called digital ledger. Blockchains are widely used for applications in many different domains including data sharing [10]. Key blockchain characteristics include:

- *Immutability.* Each block contains the hash link of the previous block. Due to the feature of hash algorithms, every transaction or data recorded in the blockchain is protected by subsequent blocks, therefore it can never be changed.
- *Decentralization.* A common solution to verify transactions is introducing a trusted central authority. Blockchain offers a consistent public ledger to replace the central agency. To reach a consensus view of the ledger among distribute users, blockchain employ various distributed consensus algorithms.
- *Anonymity.* Peers interact with the blockchain network through generated addresses. Addresses are not directly connected to real-world identities. Furthermore, Users can possess many addresses to avoid identity exposure.
- *Auditability.* Since data stored in a public tamper-proof ledger, each transaction can be easily traced to previous transactions giving a high level of transparency to the network.

The earliest blockchain technology implementation to capture attention was Bitcoin [11]. Current popular blockchains include Ethereum, a blockchain with a built-in Turing-complete programming language allowing developers to create smart contracts on blockchain [12], and Hyperledger [13].

2) Trusted Computing: It is used to describe the use of computer hardware assisted mechanisms that offer guarantees of confidentiality and integrity of the code and data that they protect. Example mechanisms include the Trusted Platform Module (TPM) [14] and the Intel SGX [15].

According to [14], a TPM is a computer chip that can securely store artifacts used to authenticate the platform. It provides a predefined set of APIs, such as basic security-related functions, primarily involving encryption keys, but it does no provide a secure execution environment. A Trusted Execution Environment (TEE) addresses this shortcoming by ensuring sensitive data is stored, processed and protected in an isolated and trusted environment [16]. Trusted Applications (TA) run inside the TEE with integrity and confidentiality assured.

Intel Software Guard Extensions (Intel SGX) is one of the main TEE technologies. It supports three main activities to establish trust [15]:

1) Measurement - provides an accurate and protected recording which measures and proves the identity and integrity of an enclave.
2) Attestation - allows an enclave to prove its identity and authenticity to another party. Attestation includes both local and remote attestation.
3) Sealing - ensures that the data is only revealed in the trusted environment, and it is encrypted when stored outside this environment.

III. Threat Intelligence Sharing

A. Overview

Threat Intelligence is information to help organizations identify, assess, monitor, and respond to cyber attacks, including indicators, Tactics, Techniques and Procedures (TTPs), security alerts, threat intelligence reports and actionable advice [17]. TI sharing is the exchange of such information within a community to leverage individual information and so collectively improve security postures. It is particularly valuable to security teams when it either contains 'evidence-based knowledge representing threats that can inform decisions' [1] or is 'actionable' [18] i.e. is *timely, relevant, complete, accurate and ingestible*. Real-time sharing of threat information is particularly useful to organizations.

TI sharing has both benefits and challenges:

1) Benefits:

- *Better Situational Awareness.* Participants may collect a great deal of external threat intelligence, which will grant them a better situational awareness of the threat landscape [1, 2, 3, 17].
- *Greater Defensive Agility.* Sharing information will identify changing TTPs faster and can speed identification and detection of threats, which will prevent potential or ongoing attacks [1, 17].
- *Reducing Costs.* Cost-saving may stem from quicker reactions to attacks, sharing information may help members avoid denial of service and other attacks [1, 2, 18, 19].

2) Challenges: Whilst TI sharing has significant advantages, many challenges still remain. These include:

- *Trust issues.* A number of challenges to sharing exist that can be considered as variations of trust. These are considered in more detail in subsection below.
- *Privacy issues.* In terms of sharing information across organizations, privacy information can refer to both Personally Identifiable Information (PII) and organization identities and secrets. Disclosure of this privacy information may cause violation of legal rules and/or lead to financial loss [1, 3, 17, 18]. The provision of privacy protections is also related to trustworthiness.
- *Negative publicity.* Companies are often reluctant to share information on cyber attacks and, particularly, data breaches. This is due to concerns that regulatory sanctions may be levied or ensuing negative publicity could affect organization's market value and stock price or that competitors might use the information to gain commercial advantage [1, 18, 19].

Sharing takes places in communities of interest with varying degrees of openness of sharing. Serrano [3] defines three such sharing models, *private* which support private communities to which membership is established through trusted channels; *public* which share all information with everyone and *community* which are somewhat similar to private but will share information with other communities. All three models exist in practise today.

Recent trends are moving TI sharing towards a more dynamic, decentralized market based model. Startups, such as Polyswarm [5] are experimenting with novel *crowdsourced TI sharing* through the creation of blockchain based marketplaces where organizations can seek advice or remedy- for a fee - on threat or malware artifacts. This decentralized trend is anticipated to increase even for the somewhat static current models. Serrano provides a blueprint for such a scenario through the concept of a *Knowledge Exchange (KE)*. A KE is envisaged as a form of marketplace containing a list of data publishing organizations and their associated data and/or service offerings. Participation rules in a KE may vary as for today's communities but relationships are likely to be much more dynamic and ephemeral.

B. Requirements for Trust in TI Sharing

Although sharing of threat intelligence *is* happening its effectiveness is greatly held back due to trust related issues [1, 2, 3, 17, 18]. In this section we consider further the three trust concerns raised earlier with the goal to identify requirements for the proposed TITAN system. These issues are:

1) Trust between Participants: This type of trust is of paramount importance and is related to the type of TI, degree of sensitivity of the TI data and the purpose for which it is exchanged. Sensitive data that could have a negative impact on a business will be shared only with most trusted partners. Such sharing is often governed through use of the TLP protocol which defines categories of sensitivity and corresponding principles for sharing [20]. Higher TLP category Information is more likely to be of a coarse granularity and very often is shared via email or through direct (either physical or electronic) conversations.

Participant trust also relates more generally to sharing communities. Tounsi reports that trust is lowered when some community members are seen to be under-contributing i.e. freeloading [1]. This is the classic 'selfish' peer in P2P network literature [9]. Furthermore the potential exists for malicious peers in P2P networks who may disseminate false or poor quality information with the aim to disrupt or harm the operation of the community. This aspect of trust is likely to become more critical as TI sharing evolve towards a more market-based model.

Trust as discussed here relates very much to the notion of "Reliability Trust" discussed earlier. The relationships may be subtly different for the two cases described here however. In general, in the case of TLP based sharing the Trustor is *information publishing* entity whereas in the broader community based sharing scenario the Trustor is the *information receiving* entity. In the first case trust is gained over time from ongoing contacts whereas in the second case participants will need a mechanism to estimate the trustworthiness of their counterparty. Reputation systems have been suggested as a means of to achieve trustworthiness and incentivise TI sharing [1], and, more generally, reputation systems are seen as very effective means of incentivising information sharing in P2P systems [9].

2) Trust in the TI Platform: This aspect of trust relates to the notion of IT security trust discussed in the previous Section. In general many different mechanism will be used to ensure that data confidentiality and integrity is maintained including strong access control, encryption of data at rest and in transit, VPN and so on. Platform trust also helps to enable participant trust particularly for communities as many of the policies governing community participation are likely to be directly supported by platform security mechanism such as those mentioned here.

The trust technology enablers discussed in the previous Section are of course also contributors to trust in a sharing platform. To-date these technologies have not been widely deployed and we discuss their role further in our own design in the next section.

3) Trust of TI Quality: The quality of threat intelligence is based on attributes such as relevance, timeliness, accuracy, comparability, coherence and clarity and provenance. Threat intelligence quality (TIQ) trust is becoming evermore critical as the volumes of threat intelligence grow rapidly larger and threaten to swamp cybersecurity teams capability to process incoming information [3, 18, 21, 22]. Having a high degree of trust in the reliability of the information quality is therefore a very important factor in deciding which TI data or data source, or community, to join with.

As TI sharing architectures move toward a more dynamic, decentralized form it will become increasingly more difficult to judge information quality [6, 21]. This will be exacerbated by the problem of assessing quality across different dimensionalities and the fact that threat information can be of many different forms. Furthermore, the mode of delivery is likely to influence assessment of quality e.g. assessing the quality of a synchronous stream of security events versus more asynchronous form of information e.g. incident reports or event data files may require different mechanisms. Sillaber conducted a focus group with security experts to determine the challenges of assessing TIQ [21]. His recommendations for future TI sharing practise include the need

1) to inform users of the TIQ since trust in data is of the utmost importance.
2) to crowdsource TIQ management i.e. to allow a publisher's subjective quality to be ranked by other participants via a reputation system.
3) to automate the TIQ assessment process. This is required due to the sheer volume of information shared.

Al-Ibrahim [6] attempts to measure the effectiveness of TI sharing by assessing the quality of the shared data versus the volume of shared information - the more traditional approach. He introduces the notion of *Quality of Indicators (QoI)* to assess threat intelligence along various quality dimensions. He posits that the concept will help TI improve including amelioration of the free-riding problem.

Future TIPs systems will need to support a variety of data quality assessment forms such as computational trust [23] or machine learning [6]. Furthermore these systems are likely to allow assessment be provided by either publisher, consumer or a third party service [6]. In order to support this flexibility it will be necessary for the TIP to be able to independently verify the integrity of operation of the assessment process in case of dispute. An added complexity for assessment system design will be the need to deal with a variety of TI sharing forms including streaming alerts, security alert files, incident reports and other discrete data.

IV. Proposed System

In this section we explain the proposed TITAN system. Our approach to address the above requirements is to develop a system to improve participant trust and data quality assessment issues using trusted platform technologies, namely blockchain and TEE.

Specifically we propose:

1) To develop a TIQ assessment framework based on the use of TEE. This will enable trust through verifying the integrity of the information and processing of the assessment process.
2) To develop a reputation system that will allow peers to rate TI sharing transactions based on the quality of

the TI received and also, more generally, to allow user subjective feedback on a range of peer transaction types e.g. to rate the quality of a different services (providers).

TITAN is aimed to be a general solution for trusted TI sharing for use across different TIPs and to incorporate a variety of TIQ assessment and scoring algorithms. The initial development of the tool is based on the use of EigenTrust in the PROTECTIVE [23] sharing TIP.

A. Architecture

The overview of our system architecture is depicted in Figure 1. It consists of three layers:

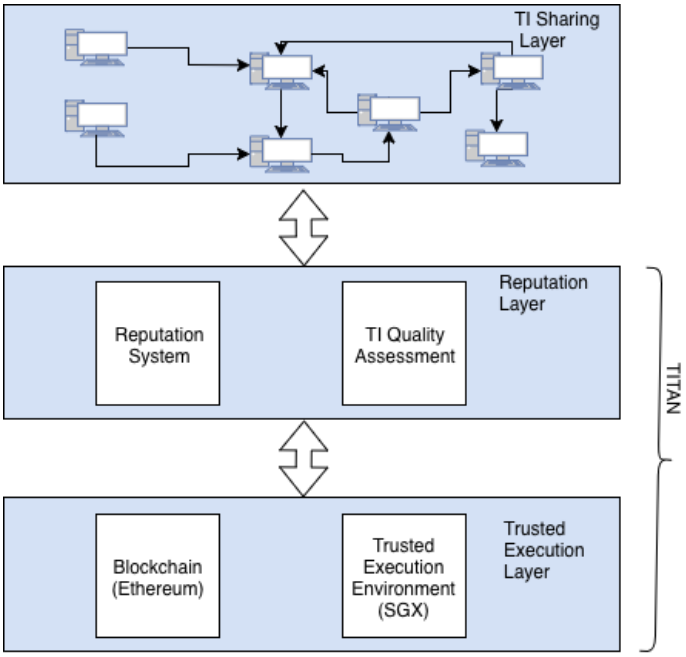

Fig. 1. TITAN Architecture

- *TI Sharing Layer.* This is the (P2P logically connected) threat intelligence sharing community. This layer is in fact outside of our framework and instead consumes the TITAN trust services. The framework is in general agnostic to the details of particular TIP e.g. such as underlying communication distribution models i.e. P2P, hub and spoke or hybrid, but TITAN can be adapted to TI sharing community specific assessment requirements such as TIQ assessment algorithms.
- *Reputation Layer.* The Reputation System is the core functionality of the system. It consists of two principal components the *Reputation System* and *TI Quality Assessment Calculation*.

  The reputation system is based on the use of *global history* P2P reputation algorithms such as EigenTrust. It is primarily implemented in the Trusted Execution layer in both the blockchain and TEE components. The blockchain is composed of the following smart contracts:
  1) *User Administration* - registers and deregister peers to TITAN via *join* and *leave* functions
  2) *TIQAssesment* - responsible for managing the TI quality assessment scores via the *updateQualityScore* and *getQualityScore* functions. This contract automatically invokes the TrustScoring contract to convert TI quality score to local trust score.
  3) *TrustScoring* - the contract updates the reputation score for a single peer interaction or transaction via the *updateTrustScore* function and the score is retrieved using the *getTrustScore* function. The trust score is defined separately from the TI quality assessment as it enables a more general trust scoring scheme. Thus reputation may be based on i) just the TI quality score ii) a combination of TI quality scoring and other parameters or iii) without the TI quality score.
  4) *ReputationScoring* - the reputation algorithm triggers the calculation of the global trust i.e. the reputation score via the *calculateRep* function and the score may be retrieved via the *getTrustScore* function. The actual scoring calculation is offloaded to the TEE for performance reasons.

  While TITAN will admit flexible placement of the assessment function as described earlier we restrict discussion to the general case of assessment via a third party assessor as described in [6]. Note that the remote attestation features of the TEE means use of a third party to provide the assessment service does not change the decentralized nature of the architecture as any peer may provide the function.
- *Trusted Execution Layer.* This layer comprises the blockchain and the TEE. The blockchain stores the trust and reputation score data and provides security and integrity against manipulation of the scores. The TEE provides security and integrity for the TI quality scoring algorithm and data and prevents manipulation or tampering. The algorithm code is published so that any person can examine it and verify its operation. The input data to the assessment is cached in the TEE layer for some policy defined period to enable remote attestation in case of dispute. The reputation scoring algorithm is similarly protected.

B. Workflow

Figure 2 gives a high level overview of the operation of the TITAN system, shown in the phases A, B and C. The figure depicts two members of the TI sharing community as well as the blockchain and TEE components.

In phase A, members of the TI sharing community register as part of the TITAN TIP via invoking the *join* smart contract function. At this stage member accounts and other related data entities are created in the Ethereum blockchain and elsewhere in the system s required. Participants are now able to take part in the TITAN sharing scheme.

At some later time, in phase B, one participant receives threat intelligence from a peer - how this is done is specific to a particular TIP and is not considered here. The receiving

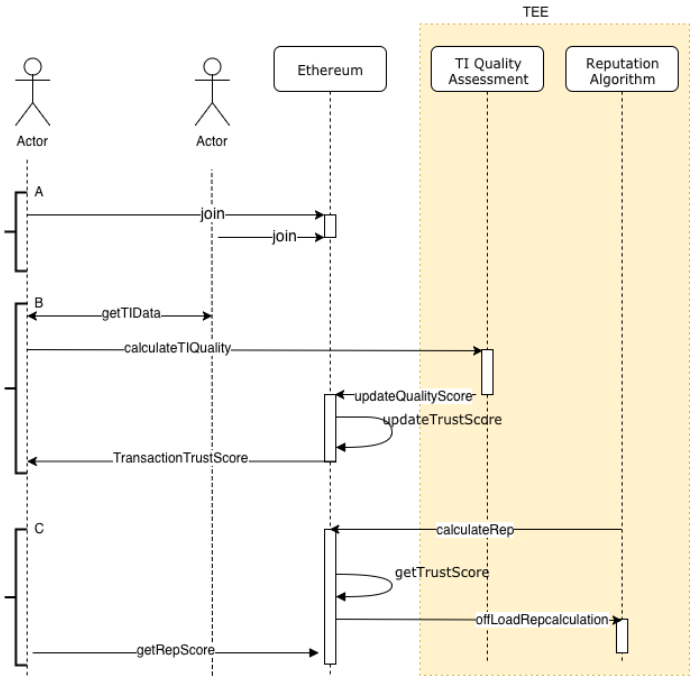

Fig. 2. TITAN Workflow

peer then requests the third party TIQ assessor to assess the quality of the received TI. The result of the assessment is then posted to the blockchain via the *updateQualityScore* smart contract function and this in turn triggers the *updateTrustScore* smart contract function to determine the final trust score for the transaction. The receiving peer is then notified by of the transaction trust score.

In phase C, according to some policy determined schedule time the TITAN system will periodically refresh the reputation scores by calculating the peer global trust values i.e. *calculateRepScore*. This will retrieve all stored trust values via *getTrustScore* and invoke the actual calculation function on the TEE. A peer may then, or at any time, retrieve the reputation score for any other peer via *getRepScore* smart contract function.

Remote attestation of a TIQ assessment score, invoked by any 3rd party to verify the transaction, is also part of the workflow but is not shown on the figure for reasons of space.

C. TITAN prototype

TITAN is using the the H2020 PROTECTIVE project TIP [23] as the TI sharing layer to develop to prototype and validate the approach. PROTECTIVE aims to improve security situational awareness through, amongst other things, TI sharing. The TIP shares network and email indicators of compromise using the Intrusion Detection Extensible Alert (IDEA) schema [24].

1) Quality Assessment: The project has developed a TIQ assessment algorithm based on computational trust [23]. In this approach TIQ is expressed as

$$TIQScore = f(Completeness, Freshness, Relevance) \quad (1)$$

In the equation (1), Completeness, Freshness and Relevance are defined as :

- Completeness - measures how much the the TI complies with IDEA schema definition. Completeness decreases for each missing field.
- Freshness - measures how long the information is shared since it is generated. It decays as time passes.
- Relevance - for each type of alert source, a list of specific keywords is predefined along an associated relevance value. The relevance score is based on the number of keyword occurrences in the alert's field.

The quality score is calculated for every received security event. In the current, static community structure usage, events are exchanged continually between known community members and trust scores are used primarily as input to an alert prioritization scheme. In the decentralized scenario that we anticipate we envision blocks i.e. files of indicators of compromise being exchanged and the individual event quality scores being aggregated by the TIQ assessment function for such event files.

2) Reputation Assessment: TITAN will use the EigenTrust algorithm to calculate reputation score. EigenTrust takes in peer transaction histories and produces global trust values for all participants [25]. EigenTrust is based on the notion of transitive trust. Each peer calculates a local trust score value v_{ijk} i.e. the information quality value of k^{th} transaction from provider i to consumer j. The reputation that consumer j contributes to provider i is R_{ij}:

$$R_{ij} = \sum_{k} v_{ijk} \quad (2)$$

The aggregated reputation of provider i is R_i:

$$R_i = \sum_{j} R_{ij} \quad (3)$$

TITAN stores the transaction trust scores on Ethereum. The integrity and transparency provided by the blockchain addresses the two main EigenTrust security concerns i.e. i) the current trust value of a peer must not be computed by and reside at the peer itself and ii) the calculation of a global trust score for any peer must not be miscalculated by any other peer. A side effect of storing the local trust values in Ethereum is that the centralized version of the algorithm can be used to calculate the global trust score.

Every peer with the reputation algorithm TEE enclave is capable of processing Eigentrust and can store the result in Ethereum. A reward is provided by Ethereum to peers who calculate the Eigentrust for the community.

V. Related work

Blockchain is increasingly being used as a platform for *sharing of data* often via decentralized marketplaces.

Blockchain can provide security and transparency and rewards individual data producers to engage in data trading. Decentralization also gives user more control of privacy. Zyskind et al. re-purpose a blockchain as an access-control moderator, and design two types of transactions: one is used for access control management; the other is used for data storage and retrieval [26]. Shafagh et al. [27] describe one such IoT data sharing platform. The raw IoT data is stored off-chain and the blockchain system is used to manage the ownership and access permissions of data by transactions. Similarly Ozyilmaz et al. propose a blockchain-based, decentralized and trustless data marketplace, IDMoB, where IoT devices vendors and data consumers may interact and collaborate [28]. In the health sector Peterson et al. [29] utilize blockchain to share patient information, where the terms of data access is strictly controlled by the patient.

Blockchain is also used as a *reputation management system*. Scott [30] proposes a public reputation scoring system for financial professionals to discourage unethical behavior. Dennis and Owen [31] present a blockchain system that stores and verifies the receipts of transaction on the blockchain. Then, the peers can calculate the reputation score based on receipts and their own parameters. The individual and subjective reputation is stored locally instead of on blockchain. Buechler et al. propose a reputation scoring algorithm, net flow convergence reputation algorithm, which is implemented by smart contracts [32], to manage misbehaviour in an electronic payment system. The reputation system is built directly on blockchain. It does not fit into our problem domain.

Storage and computation executed in blockchain is expensive [33]. Trusted computing is emerging a means to integrate off-chain computation with blockchain. The Proof of Elapsed Time (PoET) is a distributed consensus algorithm which adopt TEE in blockchain [34]. Ayoade et al. propose a IoT data management system that utilizes blockchain and TEE [10]. They use smart contracts to enforce data access permission, and store the sealed data in a secure storage using TEE. In their system, blockchain and TEE exist as independent modules. In contrast, our solution use smart contracts to store TEE's outcomes.

VI. Conclusion and Future Work

Threat Intelligence Sharing is one of the most promising approaches to resist ever-growing cyber attacks. Many pressing challenges still exist for effective TI sharing especially around trust. We describe the main trust challenges and identify the shortcoming in existing TIPs. We have designed TITAN, a decentralized TI sharing trust enhancement framework based trusted execution technologies i.e. blockchain and TEE, to address open trust issues. We outline the main features of the platform and give an overview of its operation including its application to a specific case study.

We are currently implementing the TITAN prototype. Future work will validate its effectiveness in operation with the PROTECTIVE TIP. Beyond this TITAN will be generalized to work with a broader set of TIQ and reputation algorithms. It will also be evolved into a more fully featured blockchain based TIP e.g. through the inclusion of the micro-payment incentive system etc.

References

[1] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & security*, 2017.

[2] C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives," 2017.

[3] O. Serrano, L. Dandurand, and S. Brown, "On the design of a cyber security data sharing system," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*. ACM, 2014, pp. 61–69.

[4] Y. Allouche, "Trusted and anonymized threat sharing using blockchain technology," 2019. [Online]. Available: https://www.first.org/resources/papers/telaviv2019/IBM-Dr.-Yair-Allouche-Trusted-and-Anonymized-Threat-Sharing-Using-Blockchain-Technology.pdf

[5] P. Inc., "Polyswarm crowdsourced threat detection." [Online]. Available: https://www.polyswarm.io

[6] O. Al-Ibrahim, A. Mohaisen, C. Kamhoua, K. Kwiat, and L. Njilla, "Beyond free riding: quality of indicators for assessing participation in information sharing for threat intelligence," *arXiv preprint arXiv:1702.00552*, 2017.

[7] A. Jøsang, "Trust and reputation systems," in *Foundations of security analysis and design IV*. Springer, 2007, pp. 209–245.

[8] M. Bishop, *Computer Security*. Addison Wesley, 2018.

[9] S. Marti and H. Garcia-Molina, "Taxonomy of trust: Categorizing p2p reputation systems," *Computer Networks*, vol. 50, no. 4, pp. 472–484, 2006.

[10] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized iot data management using blockchain and trusted execution environment," in *2018 IEEE International Conference on Information Reuse and Integration (IRI)*. IEEE, 2018, pp. 15–22.

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[12] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, 2014. [Online]. Available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[13] Open Source Technology. (2017) Hyperledger architecture, volume 1: Introduction to hyperledger business blockchain design philosophy and consensus. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

[14] Trusted Computing Group. (2008) Trusted platform module (tpm) summary. [Online]. Available: https://trustedcomputinggroup.org/wp-content/uploads/Trusted-Platform-Module-Summary_04292008.pdf

[15] Intel, "Intel software guard extensions developer guide," 2017. [Online]. Available: https://software.intel.com/en-us/documentation/sgx-developer-guide

[16] GlobalPlatform. (2018) Introduction to trusted execution environments. [Online]. Available: https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Trusted-Execution-Environment-15May2018.pdf

[17] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "Guide to cyber threat information sharing," *NIST special publication*, vol. 800, p. 150, 2016.

[18] N. Robinson and E. Disley, "Incentives and challenges for information sharing in the context of network and information security," 2012.

[19] D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat, and A. Martin, "An evolutionary game-theoretic framework for cyber-threat information sharing," in *Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 7341–7346.

[20] FIRST, "Traffic light protocol definitions and usage." [Online]. Available: https://www.first.org/tlp/

[21] C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, "Data quality challenges and future research directions in threat intelligence sharing practice," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*. ACM, 2016, pp. 65–70.

[22] J. Steinberger, B. Kuhnert, A. Sperotto, H. Baier, and A. Pras, "In whom do we trust-sharing security events," in *IFIP International Conference on Autonomous Infrastructure, Management and Security*. Springer, 2016, pp. 111–124.

[23] Protective, "Proactive risk management through improved situational awareness," 2019. [Online]. Available: https://www.protective-h2020.eu

[24] P. Kacha, "Intrusion detection extensible alert," 2016. [Online]. Available: https://idea.cesnet.cz

[25] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th international conference on World Wide Web*. ACM, 2003, pp. 640–651.

[26] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

[27] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in *Proceedings of the 2017 on Cloud Computing Security Workshop*. ACM, 2017, pp. 45–50.

[28] K. R. Özyilmaz, M. Doğan, and A. Yurdakul, "Idmob: Iot data marketplace on blockchain," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 2018, pp. 11–19.

[29] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, 2016, pp. 1–10.

[30] B. Scott, "Blockchain technology for reputation scoring of financial actors," *Ethics in Finance, Robin Cosgrove Prize Global*, vol. 2015, pp. 128–39, 2016.

[31] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2015, pp. 131–138.

[32] M. Buechler, M. Eerabathini, C. Hockenbrocht, and D. Wan, "Decentralized reputation system for transaction networks," Technical report, University of Pennsylvania, Tech. Rep., 2015.

[33] A. M. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and Dapps*. O'Reilly Media, 2018.

[34] Intel, "Poet 1.0 specification introduction," 2017. [Online]. Available: https://sawtooth.hyperledger.org/docs/core/releases/1.0/architecture/poet.html