2018 2nd Cyber Security in Networking Conference (CSNet)

Concept for Controlled Business Critical Information Sharing using Smart Contracts

Klaus Zaerens
Department of Military Technology
National Defence University
Helsinki, Finland
Klaus.Zaerens@iki.fi

***Abstract*— Trust management has been a topic of keen interest in recent years. There has been a lot of discussion as to what new opportunities it can bring to markets, what benefits it can offer, and what system development possibilities it enables for software development. In this paper we discuss trust management and business critical information sharing in a definite group of stakeholders called Circle of Trust. We examine the key features of the Circle of Trust in military environments. We address the most essential problems and obstacles to be considered before the benefits of Circle of Trust can be fully enabled therein. As a solution to problems with the information transfer management, we propose a novel conceptual approach which ensures the privacy of the data source and transparency of information sharing utilizing the blockchain technology and modern cryptographic solutions. In addition, the concept presented enables the quantitative information trade and objective control mechanism for contractual liabilities within the consortium. The discussion and views presented in this paper can be adopted in any organization with doubts concerning the sensitive and classified contents of supply chain management or current ICT systems.**

Keywords*— *Trust management, Information Sharing, Security Management, Cryptography, Military

I. INTRODUCTION

Importance of trust management is increasing as the Internet is more open for access, different collaboration environments have become more common and social networking affects our decision making. The relevance of trust management is gradually becoming more significant, but the multilateral nature of the concept, generally trustworthy parties and large data sets with high response time requirements have kept commercial activators and applications away from production use in public authority environments [1].

Public authorities in security field have sought and developed numerous means to improve cooperation by ICT solutions [1]. Different kind of collaboration tools and environments has been deployed and integrations between systems and data storages have developed. It is obvious that concepts like semantic knowledge processing, connectivity and social networking enables improved cooperation between authorities. However, these concepts also cause new challenges. Openness can be hard to manage in highly secured environment. Also processing and sharing the critical operative information increases hostile interest on system environment.

In public authority environment the trust in other stakeholder is unreserved in relation to profession and officiality. In collaboration and cooperation context, participating authorities compose virtual community with only trusted parties [2]. We call this kind of consortium a Circle of Trust. Within the Circle of Trust, the participant shares information in a way that the other participants will improve their success in operations. This enhances the overall performance of the virtual community from which every participant gain benefit.

The special case of information sharing is to delegate operative situational data for improving situational awareness in the Circle of Trust. This kind of collaboration improves the accuracy of the individual awareness in each actor and enriches the awareness of all actors within operation. This cooperation enables better communications, safe procedures and more effective actions in operations throughout participating authority organizations.

In this paper, we will discuss issues and problems to be considered when implementing Circle of Trust concept in core authority systems. We define the key characteristics of such a high security environment. We will narrow our observations to military systems in which the need for computational capacity is high and the reliability of information is always critical. In military environment we must ensure data flow correctness, traceability and survivability. In this paper we discuss on a situation where a trusted node forfeited credibility and we should control the information or knowledge the node receives from our trusted network. As a solution to problems with the adoption of Circle of Trust in high security environments, we propose a novel Enhanced Information Sharing Management approach based on blockchain technology that manages the delivery of information within the closed Circle of Trust and improve the security of overall system by reducing the risk of information being compromised.

II. SITUATIONAL AWARENESS AND TRUST MANAGEMENT IN MILITARY CONTEXT

Improving situation awareness has become more critical in public authority operations and especially in military context. The possibilities and utilizations of situation awareness have increased together with technical evolution. Sensors and mobile devices increase the effectivity of collecting data from locations that traditionally have been difficult to access. More data can be collected and stored than previously, which enables view on situation to be more truthful, accurate and comprehensive.

Most of the severe challenges on improving situation awareness are related to refinement of significant information from huge amount of data, unstable data transfer connections and especially in field operations, limited data capacities [1]. Data correctness, reliability, redundancy and timeliness have also been discussed in several publications [1]. Less discussion has been addressed to trust evaluation of the data source or the security issues on delegating the situational data to recipients with different trust levels. This aspect is relevant in military environment where there is always possibility for a malicious actor receiving confidential information or sending unreliable data to decision making process.

In this paper we adopt the definition of trust presented by Grandison and Sloman because of the simplicity yet complete enough. According to Grandison and Sloman, trust is a quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context [2]. Moreover, in this paper we limit our observation on computative trust management. Widely accepted features on computative trust management include subjectivity, the expected probability and relevance [3, 4].

In military context participants of the trust relation are bound to a role. A participant represents some actor or unit within an organization. Unit has a task and a goal and special expertise specified by the organization. In this environment, two interacting actors from different units trust the represented role of the other not the actor itself. Yet the trustworthiness between two roles can be fixed on process level, the individual actor might have specific preferences, interests or experience which affects to quantitative trust. Similarly, data providers such as sensors can be modelled as an actor in trust relation and represented by an ownership of an organizational unit.

III. Circle of Trust Characteristics and Benefits in Military Environments

In this paper we define Circle of Trust as a consortium of a specified subject with only trusted parties. It means that each participant has sufficient amount of trust to other participant in relation to the subject. The sufficient can be considered as readiness for deliver and receive knowledge unconditionally without risking own operative ability. The motivation for creating the consortium is to construct a united force to gain improved capability in operations with the same goal. For achieving the goal it is essential to have an open and transparent information exchange between the participants. To sustain the circle, all parties should have indirect or direct benefit from collaboration and cooperation with each other. The participants rely operative enhancement that they gain from the participation of the circle. Enhancement can be for example improvement of efficiency in operative actions or overall reduction of operative costs. In practice the actions can be trading situational information between participants. Moreover, we argue that the Circle of Trust formed by combining the public authorities from different countries is the only real possibility to improve the situational awareness in order to operate successfully in cyberwar. Malicious actions in cyberwar are conducted always from international level and often routing is hiding the origins of the actor. Resolving the actor needs international collaboration with openness of information. We should not forget that defending from malicious action on solely national level can be only reactive by nature. That is why countermeasures are effective only when performed also on international level. The information collected by international consortium can help to identify the existence of malicious actor and to detect false information from the attacked systems.

The example of Circle of Trust is illustrated in Fig. 1. In Fig. 1 *A* represents us as a situational information provider. *B* and *C* are recipients of our information. Arcs represent the direction of information. Because information trading should happen in both directions, arcs are represented also from the recipient to provider. Each arc contains two parameters *s* for situational information and *w* for the weighted trust between information provider and recipient. It is notable, that if for example $w_{AC} \neq w_{AB}$ then $s_{AC} \neq s_{AB}$. In practice this means, that the situational information provided by the provider is not the same unless the trust relation between provider and recipient were exactly the same. It can also be noted that the trustworthiness of the recipient is in direct relation to the correctness and completeness of the situational information provided by the information provider.

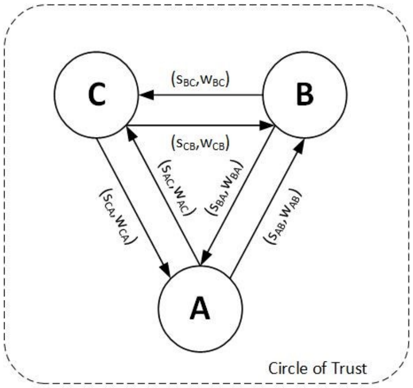

Fig. 1. Circle of Trust

As stated before, with Circle of Trust situational awareness can be improved by trading the intelligence and reconnaissance information within the participants of the Circle. Trading is usually mutual sharing where the quality and the amount of traded information are in balance.

The trading can also be used for identifying possible leakages. If there is a suspected malicious actor as a member in Circle of Trust, with labelled or water marked information to participants it is possible to detect and identify the source of leakage by following the trace of the information. If there is certainty of an intrusion to system, with Circle of Trust deceptive information can be fed to malicious actor without breaking the routines and not disconnecting the actor from the grid too soon. More over the capabilities of a hostile actor can

978-1-5386-7045-3/18/$31.00 ©2018 IEEE

be monitored and evaluated by observing the actions it performs in controlled environment [5].

Circle of Trust is a scalable and generic concept. In international scale we can consider a military alliance such as NATO as an example of Circle of Trust. On national scale example can found from the collaboration with public authorities of safety such as between police forces and rescue service. On organizational level we can have example from ministry like Ministry of the Interior and all the agencies that it conducts or the supply chain of financial ecosystem. On the technological level all nodes in a high security network form definite Circle of Trust.

IV. Challenges in Information Sharing

In this chapter we discuss more on challenges identified within the Circle of Trust. The Circle of Trust should enable openness of information exchange, but the openness also increases the risk of revealing too much sensitive information to public.

Situation data contains always some information about the collector or origins of data by nature. This information can relate to location information, resources or capability. This information can be used against the originator. Revealing information is always risk and the delivery should be somehow controlled so that the information, knowledge or capabilities are not leaked to any hostile or untrusted recipient.

A. *Absolute Trust Does not Exist in Reality*

Within closed Circle of Trust, some parties are always more trustworthy than others. For example, in military alliance some nations are in more deep cooperation than others and some nations can have doubts from history to others. In that sense the sufficient amount of trust can be varied a lot between the actors. The consequence is that the participants in the Circle of Trust are not in the same level. In authority cooperation trust within own organization is usually unreserved. This trust is based on mutual experience, common procedures and professional community. A lot harder is to trust another authority and different organization. We can find this element of distrust in each level of Circle of Trust concept. The main concern is the leakage of sensitive information illustrated in Fig. 2. After revealing information for recipient *C*, we are not able to manage the revealed information. If *C* has a connection with party *D*, which does not belong to our original Circle of Trust, *C* might still provide some information to *D*. Assuming that *A* is the only information source, the *D* will receive information $s_{CD} \subseteq s_{AC}$.

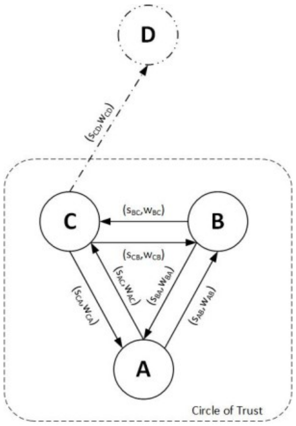

Fig. 2. Leakage of information

Another dimension of this challenge is the publicity of distrust. If one actor is not ready to release all information unconditionally to all other actors but is bound to principality of openness within the circle, how publicly this limitation of released information can be made.

B. *Managing Information Sharing in Open Network*

In the previous chapter we discussed on leakage of information. Regardless of how much we have trust on our allies, we need their information. To receive information from other parties the usual convention is to give or send information collected by the one. This actually forms a trading system where tradable information is defined by its usefulness, timeliness, trustworthiness, accuracy and comprehension. As stated in previous chapter, absolute trust does not exist in reality. Circle of Trust or any alliance is trying to form a framework where quality levels of information that are agreed on are written and we can rely that at least the exchange of information itself would actualize. Information providers try to minimize the amount of sent information but still receiving the maximum amount of information. The main goal of the recipient is to have sufficient amount of information to form awareness of a situation. The interesting question is that what is the sufficient amount of provided information to gain that goal?

Another issue arises when information is sent to the recipient. After transmission of information the provider loses all control of the sent information. That when a receiver has interpreted the information, the receiver immediately owns the information and can use it to any purpose needed. This includes also sending the information to other partners, avoided or simply not intended by original source. Having secured connection does not solve this issue since for the received information is presented in a decrypted form.

The accumulation of information can be also a problem. This situation is illustrated in Fig. 3. If *A* sends data fragment s_{AB} to recipient *B* and data fragment s_{AC} is send to recipient *C*, it is possible that both of the recipients send the data fragments to less trustworthy participant *D*. *D* can combine the both data fragments $s_{AB} \cup s_{AC}$ and create more comprehensive situation and indirectly form an increased risk to the originator *A*.

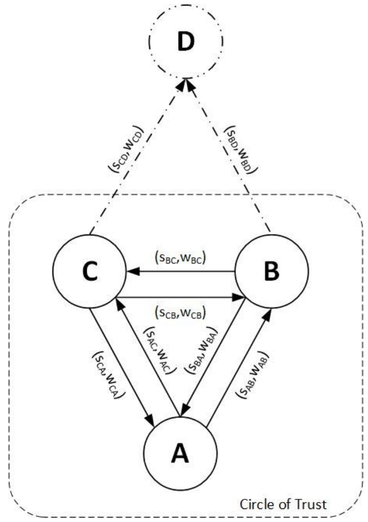

Fig. 3. Accumulation of information

C. Collateral Damage of Deception

Previously we described the possibility of deception with the identified intrusion in the secure environment. The challenge is how the intrusion is notified to other participants in the Circle without risking that the information is reached to the intruder. This problem setting is formalized in Fig. 4, in which *A* has some distrust with *C* (i.e. w_{AC} is small) and decides to send false information s_{AC}. At the same time *C* and *B* have a strong trust relation (i.e. w_{BC} and w_{CB} are large) and also *A* and *B* trust each other. If *C* transmits the information s_{AC} as s_{CB}, *B* receives false data which can be very harmful of course for *B*, but also for *A*. After exposure of deception the trustweight w_{BA} is most probable to decline, which influences the future information exchange and trade balance.

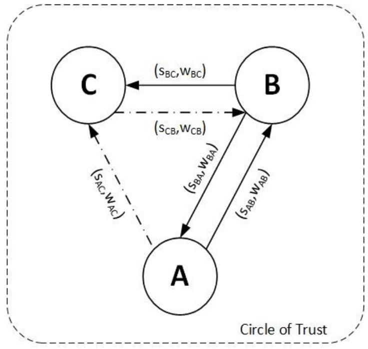

Fig. 4. Collateral damage of deception

A special case of this problem occurs when one participant in Circle of Trust identifies an intruder within the Circle. If the other participants are not trustworthy enough to identify the intruder and the deceptive data is fed to the intruder, how can we notify the other participants not to trust information that they receive from the intruder.

V. Overcoming Obstacles

Traditionally Information Sharing is technically conducted by the point to point (P2P) connections between information provider and recipient. Connections are usually secured by Public Key Infrastructure based Virtual Private Networking (VPN). The information shared within the connection is conducted by the trust between the provider and recipient. This sharing mechanism becomes complex if same information should be transmitted to several participants or a collaboration platform is needed. In addition to that, ensuring the survivability, timeliness, openness, privacy and usefulness of data across all participants of the mutual interest group is an expensive system to be developed.

We propose an approach based on blockchain technology to overcome the problems and obstacles in information sharing stated in previous section. Since implementations of the blockchain technology are evolving we will focus to the principles of our approach and relax platform specific details such as performance or security issues from the scope of this paper. The most essential additional requirements of our approach for the blockchain technology platform are support for smart contracts and privacy enabled joined transactions. In this paper we propose the Ethereum project as an example of platform containing sufficient technological features [6].

A. About Blockchain Technology and Smart Contracts

The blockchain technology is one of the most prominent new technologies. It utilizes the decentralized management of assets and ensures the consistency of information by encrypting the transactions with previous states of information. The information management and consistency are solved by miners that verify the correctness of the system and final states of information. These miners receive a small fee for their effort [7, 8].

The most famous implementation of blockchain technology is the Bitcoin system. Bitcoin is a cryptocurrency without any centralized management or issuer such bank [7]. All participating nodes the Bitcoin system have information on all accounts in the system and are responsible for ensuring the correctness of account balances. Accounts are anonymized but the contents and the transactions are public. If some amount of currency is to be transferred to the other account, a transaction entry is created with previous addresses of currency, the amount of currency and the recipient address. This entry is encrypted and delegated to the system nodes to be verified, validated and committed. System nodes that commit the transactions are called as miners and they receive a reward as Bitcoin currency [7]. This work increases the amount of currency in system which ensures the growth of the Bitcoin financial system.

Bitcoin success story has brought up several other application areas where similar technology could be utilized. Bitcoin implementation has some limitations such as scripting or lack of meta-protocols [6]. A need for passing agreements between stakeholders in more comprehensive manner was also observed. Ethereum is one of the projects that address these limitations by introducing an abstraction layer on top of the basic blockchain platform [6]. The layer contains built-in Turing-complete programming language which ensures that more complex systems can be implemented. In Ethereum, contracts can have data, conditions, operations and they can

978-1-5386-7045-3/18/$31.00 ©2018 IEEE

return a value similarly than functions. An interesting feature is that the contract itself can also create another contract and the role of created contract in system can differ from the originating contract. This allows us to implement more sophisticated systems such as escrow-, reputation-, identity management- or gambling applications where a third party is needed for guaranteeing the agreement between contractors [6, 9].

B. *Enhanced Information Sharing Management*

Our approach is based on improved blockchain technology platform with additional components for sharing and managing the information. The blockchain implements features such as traceability and openness by design. Decentralized management improves the survivability of system and enhances the collaboration between participants [7]. The blockchain platform ensures consistency and trustworthiness of the whole chain of information with the audit trail leading back to the information origins [10, 11]. Circle of Trust requires closed environment and encryption of shared business-critical information content.

In our information sharing management scheme set of data fragments *S* from information providers are pooled and made available for every participant to use. The trust is determined towards the system by the quality of information received. This relaxes the need for trusting the other participants and transmits the trust management to the information management engine. This allows data providers to determine trust from their own perspective and asymmetry for the whole system is reached. For Information Sharing Management we extend the CoinJoin of Bitcoin [8] methodology with rules management and transaction monitoring features as an exemplary illustration in Fig. 5.

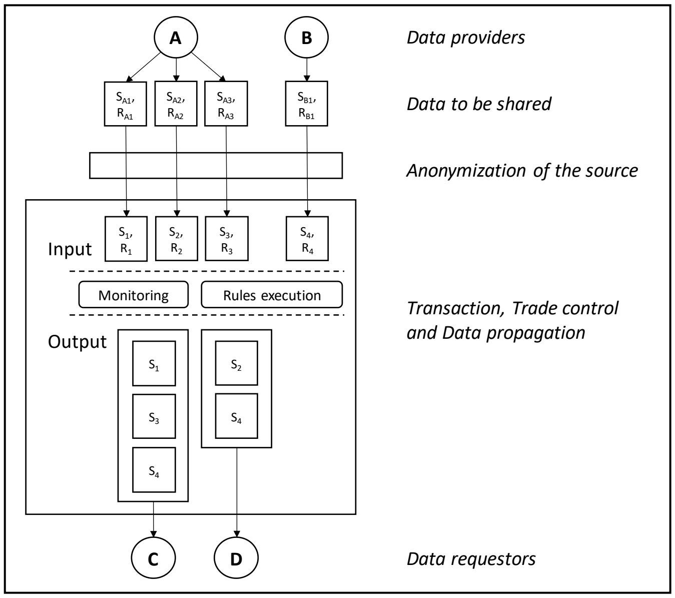

Fig. 5. Enhanced Information Sharing Management.

Before information to be shared are used as input in pool of data, the data origins are anonymized by using virtual front organization layer. The need for anonymization is to hide the exact source of the data. Despite of the anonymization, in the system the traceability still exists in consistent blockchain yet more difficult to solve.

Data pooled and entered in the transaction engine contain the data *S* and the associate rules *R* for the data. Rules can be represented as Smart Contracts in Ethereum [6]. With rules we can manage the information delivery in the system. We can for example exclude recipients from the information, prevent that two different data fragments are delivered together, adjust preconditions of delivery depending on execution of other rules, set a sequence timeline etc.

In algorithm 1 an example is provided to give an idea of contract structure for preventing accumulation of information. Coding notation resembles roughly Solidity language for smart contracts. It is essential to observe the possibility to change implicitly state of the contract, query external contracts and create highly sophisticated conditions that control behavior of the contract through whole lifecycle.

Algorithm 1. Example of contract

```
contract ShareExample
{
    address[] sharelist; // allowed recipients
    address[] deliveredlist; // where information is already delivered
    address[] exclusionlist; // accumulation preventionlist
    data information; // information to be shared, any type of data

    /* Transaction manager can use this function for getting the
    recipients of information. */
    function getSharelist() public
        returns (address[] out) {
        return sharelist();
    }

    /* Function that checks whether certain recipient has received
    information. */
    function isDelivered(address recipient) public
        returns (boolean out) {
        if (deliveredlist.exists(recipient))
            return true;
    }

    /* Function returns actual data for transaction manager. */
    function pullDeliver(address requestor) public
        returns (data out) {
        if (
            requestor in sharelist() &&
            preventAccumulation(requestor) {
                setDelivered(requestor);
                return information;
        }
    }

    /* Function that stores information on shared data. */
    function setDelivered(address recipient) private {
        deliveredlist.push(recipient);
    }

    /* Function that checks if other contract has sent its information to
    same recipient. */
    function preventAccumulation(recipient) private (boolean)
        // referring directly to another contract
        if (recipient in exclusionlist() && !(Y.isDelivered(recipient))
            return true;
    }
}
```

The transaction engine is responsible for consistency blockchain data after sharing the information to recipients. Engine decides and shares the processed information according to the ruleset of the information to the participants of the system.

The transaction engine contains monitoring service for the quality of information, trading balance between participants and liabilities of stakeholders. Trading service enables more sophisticated features such as analysis how participants have met their commitments in the Circle.

We argue, that encouraging participants to share information to the system according to their risk evaluation and enabling functional information trading system with objective commitment monitoring, the threshold for sharing critical and collaborative useful information declines and overall openness increases.

C. Evaluation

To analyze our approach, we evaluate the differences of security risk when sharing critical information. We compare our approach to the traditional VPN based P2P information transfer in Circle of Trust environment. We assume that data encryption strengths are equal in both schemes. We evaluate protection of the source, data leakage, collateral damage of deception and data accumulation.

1) Protection of the source: In VPN based system there is no protection of the source since the transmission is executed between two participants. Even if data is transferred across several nodes, the most likely origins of the data can be derived from the known relations of stakeholders. In our Information Sharing Management, anonymization of the origins ensures the improved privacy of the source. This anonymization phase ensures also privacy of distrust.

2) Data leakage: As we see from Fig. 2 data leakage can be evaluated by the distrust probability (weight) of w_{AC} and trust probability (weight) w_{CD}. The strentgth of our approach is, that we need to evaluate the stakeholder that creates the greatest risk of data leakage for our sensitive information. In VPN based P2P system, we need to consider that any distrust – trust arc combination could occur to our shared data s. In our Information Sharing Management we are able to prevent the data to be shared to most distrusted stakeholders. The evaluation of risk approximation can be formulated as in (1). The left side represents the VPN P2P system and right side our new approach.

$$\sum^{n}_{x=1} [(1-w_{Ax})(w_{xy})] > (1-w_{AC})(w_{CD}). \tag{1}$$

wherein x represents the direct information recipient from provider A, n the amount of arcs Ax and y all the malicious recipients from transmitter x. For simplicity we mark C as the most distrusted recipient of those that receive information s and D as the most trusted partner for C who is also malicious in relation to A. Simplifying the evaluation, we can approximate the greatest risk of data leakage from our most trusted partners. If data provider should care data leakage from several trusted partners (i.e. similar as C), the necessity of data provision should be revised, the position of the provider in Circle of Trust ecosystem should be analyzed or the sensitivity of information content should be decreased. In these cases, problem of information sharing is more political than technical. From the evaluation can also be seen, that our approach works even better the larger Circle is.

Recipient that duplicates sensitive information and publishes it against agreements or otherwise violates confidentiality is a challenge to any technical or political system. Naturally our Information Sharing Management can not prevent data duplication outside Circle of Trust if an actor intentionally executes that. However, controlled information sharing provides traceability and with watermarking the information malicious actors can be verified and exposed.

3) Data accumulation (Fig. 3): Dangerous data accumulation occurs in VPN P2P system if there is any transfer path for all data fragments in S that transit same stakeholder node. In our Information Sharing Management stakeholders should trust the information received from the system and not to have any other transfer schemes with partners. However, this can happen if there is more distrust between participants of Circle of Trust than to the system information. In this case having all data fragments in S accumulated, we need to calculate the distrust probability for all data fragments in S recipients. In other words, distrust represents that one stakeholder considers essential to forward received information suspecting that new recipient has not received information for original provider. Data accumulation is formulated as in (2). The left side represents the VPN P2P system and right side our new approach.

$$\sum^{n}_{x=1} (w_{Ax1} * \ldots * w_{Axn}) > \Pi^{n}_{x=1} (1-w_{Ax}). \tag{2}$$

wherein n represents the amount of data fragments S. In VPN P2P based system where participants trust each other information is transmitted to each other without consideration. Any information is propagated to the whole circle, which increases the risk of data accumulation. In our approach, the information provider has the possibility to prevent the accumulation. In (2) we see, that if the Circle of Trust is strong, the distrust is little and the risk of accumulation approximates 0. In other words, in our approach strong trust between the Circle participants prevents accumulation of data in contrast to P2P system where strong trust emphasizes it.

4) Collateral damage of deception (Fig. 4): Evaluation of this is special case from the data leakage. We send intentionally false information and hope that there is small trust relation w_{CB}. Protecting B from false information requires better information to be sent to B. With two different information contents of s from different providers (s_{1CB} and s_{1AB}), B evaluates the trustworthiness of the sources w_{BA}, w_{BC} and chooses the information to be trusted. In VPN P2P type system can happen that B trusts C more and gets false information. The possible damage and reveal of the true origin can impact negatively to the trust relation or trade balance

978-1-5386-7045-3/18/$31.00 ©2018 IEEE

between *A* and *B*. It can also happen that *B* corrects *C*'s information with more trusted information from *A*, which exposes the *A*'s distrust to *C*. In our Information Sharing Management we can specify a rule for s_1 that s_{1AB} excludes s_{1CB}. If *C* transmits s_1 again to the system, *B* needs to evaluate the trustworthiness of the information received and to choose which one to use. Only difference is that origins of the two versions s_1 are anonymous, so the false choice affects *B*'s trust to the system not the trust towards actors *A* or *C*.

VI. Ensuring Openness in Circle of Trust

Openness in information sharing does not remove the need for privacy nor the protection of the information itself. The shared ledger that enables the collaboration and survivability with data replication, creates significant risk of exposure when propagating information across the Circle stakeholders. Minimizing the risk of exposed information, we adopt the latest research results in cryptography conducted by Huang et al. [12, 13, 14, 15]. Huang presents a novel approach to existing public key encryption schemes. For our problem we utilize his commutative encryption algorithm based on ElGamal encryption [13, 16]. With commutative encryption we are able to encrypt information more than once with different public keys. The usefulness in our problem is that the decryption order may vary as needed. This permits us to distribute the same ledger across the Circle of Trust having data sufficiently secured.

The participants have individual keys for encryption of the solution, but as we stated in previous chapters, they are not aware the accuracy or exact trustworthiness of the decrypted information with their own key. The trustworthiness is measured on trust to the whole system. Consequently, everyone has access to every decrypted solution, but only the original provider has the information of correct original data and which key or keys decrypt the best solution.

The approach is illustrated in Fig. 6. $f(A_{key})$ is the encryption on original information provided by A which results the encrypted information *A'*. For each recipient there is a key which decrypts the information with f' resulting the recipient specific information (in Fig. 6 [*B*, *C, D*]). It is noteworthy that there can also be a key or several keys for parties outside the Circle of Trust as presented in Fig. 6.

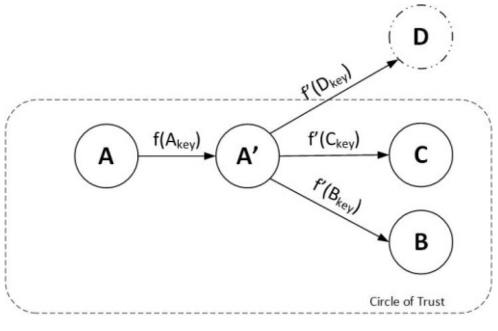

Fig. 6. Encryption and decryption of information with different levels of trust.

In practice this is achieved by encrypting the information so, that the each of the decryption key results a valid outcome. According the Huang encryption $f(A_{key})$ contains all the encryption for each recipient. That is $f(B_{key})$, $f(C_{key})$ and $f(D_{key})$. After keys are delivered to recipients the encrypted information is opened for open access. For example, with information trading between *B* and *C* the differences can be identified, but the accurate reliability cannot be solved.

For a computational issue, the malicious actor has no possibility to decrypt all possible solutions and if they do that, they are not aware which one of the results is the most accurate representation of the encrypted information. Moreover, we argue that even if the malicious actor could collect all the decrypted instances of the information from certain time, it cannot reliably determine what represent the best information.

This solution works best in timely systems where the amount of information is huge. Of course, with infrequent high security information exchange other conventional encryption methods are more useful.

VII. Related Work

In this chapter we will present a brief overview of existing concepts and technologies that are discussed similar problems such as Circle of Trust. We point out the main differentiator of our approach compared to observed one.

First, we observe the knot concept. Circle of Trust can be considered as a virtual community. In sense, it shares the similar context that Gal-Oz et al. have presented in their approach on knots [17]. A knot is defined as a subset of community members identified as having overall strong trust relations among them by directly from trust model of indirectly via transitive trust. Moreover, knots are groups of members that can rely on each other's' recommendations even if they did not rate the same experts. However, the Gal-Oz model emphasizes the symmetry of trust. The knot concept lacks also a mechanism for weighed trust relations, which is a way of quantifying the distrust in Circle of Trust. In our approach, trust might also vary when changing the recipient to a sender and vice versa. It means that the trust between the actors is not symmetrical. This feature descents from the reality, where occasionally recipient has to rely the information provided by the provider, even if there is a suspicion that the information received is not good quality and it might be that the information traded back is best that can be provided by the provider. This kind of asymmetric situation occur when the trading parts had significantly different capabilities of providing and testing the reliability of transmitted data. The technically stronger, more capable and with larger resources can use deception in information sharing and demand full accuracy and highest quality of information in return. In other words, trust varies between the actors in the context of Circle of Trust.

Second, we examine the idea of trust transitivity. Jøsang et al. have published several papers where they discussed features and possibilities of trust transitivity [18]. This research has a potential platform for enhancement where transitivity is limited by threshold when weighed arcs are chained. However, this does not avoid the fact that the first recipient owns the received data after interpretation. Trust transitivity method needs an

978-1-5386-7045-3/18/$31.00 ©2018 IEEE

external broker to control the threshold of the chained arcs. We still find that kind of system vulnerable for exposure of data.

Third we point out that Chen et al. [19] have published a methodology where attributes of trust are delegated subjective trust evaluation. Approach considers the aspects of distrust and include a mechanism to avoid exposure of data regardless of the trust values. However, delegation of attributes and building a global trust map can quantify the accumulation problem and at least increase the knowledge on leaked and possibly accumulated information. Despite of that, it solves the collateral damage of deception problem, because the trust values can prevent sending distrusted information via trusted arcs.

VIII. Conclusions

In this paper we examined information sharing within trusted stakeholders. We defined that environment as the Circle of Trust and limited our discussion to the military context. We stated that the absolute trust never existed and information exchange is necessary in order to build a comprehensive situational awareness. We identified the three primary obstacles to adopting Circle of Trust in a military context and examined possible solutions to overcoming them. We proposed a novel Enhanced Information Sharing Management that utilizes modern blockchain and cryptographic technology. We examined how the smart contracts could improve the overall approach by ensuring the integrity and confidentiality of the shared information. We showed our system enhances the privacy, the data leakage prevention, data accumulation prevention and collateral damage of deception in contrast to traditional VPN P2P system.

We ensured the openness of system by encrypting the information simultaneously with different keys which are delivered one for each recipient. The decryption result can be controlled on encryption phase. We argued that revealing all solutions of decryption are vast, that any malicious actor has no capability to solve in reasonable time which solution has most accurate information in which parameter.

References

[1] Zaerens, K, Enabling the Benefits of Cloud Computing in a Military Context, Proceedings of 2011 IEEE Asia-Pacific Services Computing Conference (APSCC'11).

[2] Grandison, T, Sloman, M, Specifying and analysing trust for internet applications, In Proceedings of the Second IFIP Conference on e-Commerce, e-Business and e-Government, 2002.

[3] Abdul-Rahman, A, Hailes, S, A distributed trust model, In Proceedings of the 1997 New Security Paradigms Workshop, pp.48-60, 1998.

[4] Zhou, Z. X., Xu, H, Wang, S.P, A Novel Weighted Trust Model based on Cloud, Advances in Information Sciences and Service Sciences, 2011.

[5] Handel, M, Intelligence and deception, Journal of Strategic Studies Vol. 5 , Iss. 1,1982.

[6] Buterin, V, A Next Generation Smart Contract & Decentralized Application Platform. Ethereum White Paper. [Online]. Available: http://www.Ethereum.org

[7] Nakamoto, S, Bitcoin: a peer-to-peer electronic cash system, 2008. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[8] Bitcoin Developer Guide. [Online]. Available: http://www.bitcoin.org/

[9] Stajano F., Clayton R. (2011) Cyberdice: Peer-to-Peer Gambling in the Presence of Cheaters. In: Christianson B., Malcolm J.A., Matyas V., Roe M. (eds) Security Protocols XVI. Security Protocols 2008. Lecture Notes in Computer Science, vol 6615. Springer, Berlin, Heidelberg

[10] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 839-858.

[11] Delmolino K., Arnett M., Kosba A., Miller A., Shi E. (2016) Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. In: Clark J., Meiklejohn S., Ryan P., Wallach D., Brenner M., Rohloff K. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, vol 9604. Springer, Berlin, Heidelberg

[12] Huang, K, Tso, R, Chen, Y, Rahman, M, Almogren, A and Alamri A, PKE-AET: Public Key Encryption with Authorized Equality Test, The Computer Journal first published online April 20, 2015 doi:10.1093/comjnl/bxv025

[13] Huang, K, Tso, R, A commutative encryption scheme based on ElGamal encryption, In Information Security and Intelligence Control (ISIC), 2012 International Conference on IEEE, 2012, p. 156-159.

[14] Huang, K, Tso, R, Chen, Y. C, Li, W, Sun, H. M, A New Public Key Encryption with Equality Test, In Network and System Security, Springer International Publishing, pp. 550-557.

[15] Huang, K, Chen, Y. C, Tso, R, Semantic Secure Public Key Encryption with Filtered Equality Test - PKE-FET, SECRYPT 2015, p. 327-334.

[16] El Gamal T,. A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31(4), 1985, p. 469-472.

[17] Gal-Oz, N, Gudes, E, Hendler, D, A robust and knot-aware trust-based reputation model, Proceedings of the 2nd Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM 2008), Trondheim, Norway, pp. 167–182, 2008.

[18] Jøsang, A, Pope, S, Semantic Constraints for Trust Transitivity, Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling-Volume 43. Australian Computer Society, Inc., 2005.

[19] Chen, B, Zeng, G.S, Li, L, Attribute Delegation Authorization Based on Subjective Trust Evaluation, 2008 IFIP International Conference on Network and Parallel Computing, 2008.