Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Composite Multi-dimensional Trust-based Schemes (CMT) for the Threat Information Sharing

Jihen Bennaceur (jihene.bennaceur@medtech.tn)
University of Manouba, National School of Information Science (ENSI)

Wissem Zouaghi
SAMA PARTNERS Business Solutions GmbH

Imed Hammouda
Mediterranean Institute of Technology, South Mediterranean University

Ali Mabrouk
SAMA PARTNERS Business Solutions GmbH

Research Article

Keywords: Security threats, threat information sharing, trust and reputation management, trust dimensions, zero-trust, private/ public communities, penalty mechanism, 3d demonstrations

Posted Date: September 6th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-2017412/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Composite Multi-dimensional Trust-based Schemes (CMT) for the Threat Information Sharing

Jihen Bennaceur[1,2*], Wissem Zouaghi[3†], Imed Hammouda[1†] and Ali Mabrouk[3†]

[1*]Mediterranean Institute of Technology, South Mediterranean University, Tunis, 1053, Tunisia.
[2]University of Manouba, National School of Information Science (ENSI), Manouba, 2010, Tunisia.
[3] SAMA PARTNERS Business Solutions GmbH, Mannheim, 68159, Germany.

*Corresponding author(s). E-mail(s): jihene.bennaceur@medtech.tn;
Contributing authors: wissem.zouaghi@samapartners.com; imed.hammouda@medtech.tn; imed.hammouda@medtech.tn;
†ali.mabrouk@samapartners.com

Abstract

The trust concept becomes more and more popular by paving its way gradually into the modern field. Thus, it becomes a more alluring and attractive solution to secure and protect information sharing against attackers. Indeed, malicious entities can launch intentionally or unintentionally very harmful attacks against the information sharing process causing network paralysis. In this paper, we propose composite trust-based schemes from the perspective of direct experience and entities' recommendations to enhance the shared threat information in the public and private communities. Therefore, we introduce a first trust-based model defined by several specific dimensions to improve the security of private/targeted communities. Furthermore, a second trust-based scheme is proposed for the public community where the concept of zero-trust is introduced to enhance the shared critical data inside this open environment. Thus, our proposal reveals a new level of defense against the misbehaving entities by introducing a penalty scheme to punish the malicious and suspicious users and to exempt the attackers with continuous misbehaving from participating in the information sharing process. Extensive simulations demonstrate that the proposed trust-based model provides high stability and resistance in a heavily hostile environment for the public and private communities.

Keywords: Security threats, threat information sharing, trust and reputation management, trust dimensions, zero-trust, private/ public communities, penalty mechanism, 3d demonstrations.

Secure and effective information sharing processes are crucial to the success of individuals, teams, and especially organizations. Two hot research topics in building effective organizational architecture determine how to provide the right information to the right entities and how to secure the critical data during the information sharing process [1]. Many mechanisms are proposed to face the information sharing environment's security problems, such as the Trust and Reputation Management techniques (TRM) [2]. This emergent security solution aims to improve the reliability and the trustworthiness of the sharing network. Trust modeling for the information sharing concept may include characteristics of shared data. Furthermore, it requires an understanding of the community nature (open-nature, closed-nature) on security considerations. This paper introduces two composite trust schemes based on new and exhaustive dimensions: Competence, integrity, willingness, intent, mutual interactions, past experiences, geolocation, sector, capabilities, legal agreement, type of community, reputations, etc. We exploit the interest of trust and reputation management concepts to the trust-based schemes. The primary contributions of this paper are as follows:

- Two composite models are developed based on the trust and reputation management concepts for the threat information sharing to secure the network against malicious and suspicious users.
- A first composite trust-based scheme is designed for the private/ targeted community to secure the critical shared data during the information sharing process. This model comprises the initial trust and the updated trust models where several dimensions are introduced to build a trustworthy environment for information sharing.
- The second composite scheme is defined based on the zero-trust concept for the public community to secure the information sharing inside this critical environment.
- The reputation and penalty mechanisms are introduced to detect and punish malicious and suspicious entities launching harmful attacks.

The remainder of this paper is organized as follows: In section 1, the threat information sharing goal, types, architecture, and process will be detailed. Then, in section 2, the concepts and the characteristics of trust and reputation management will be defined. Thus, in section 3, the composite trust-based model for the private/targeted community will be introduced by explaining their dimensions. Section 4 will reveal the second trust scheme based on the zero-trust concept for the public community. Section 5 is dedicated to illustrate the results of the simulations. Finally, section 6 is meant to summarize the conclusion and to expose our directions for future work.

1 Threat Information Sharing (TIS)

This section will present the information sharing concept by defining all the taxonomies related to this field. Moreover, notations and acronyms used in this paper are summarized in Table 1.

Abbreviations	Technical names
TIS	Threat Information Sharing
SP	SAMA PARTNERS company
TTP	Tactics, Technics and Procedures
DNS	Domain Name System
IDS	Intrusion Detection System
URL	Uniform Resource Locator
CTI	Cyber Threat Information Sharing
TRM	Trust and Reputation Management
Tp_i	Pre-trust of the entity i
R_i^j	Reputation of the entity i about the entity j
In_i^j	Trust inherited of entity i form entity j
T_i	Trust of entity i
Tc_i	Type of the community
Ta_i	Legal agreement of the entity i
G_i^j	Geolocation of entity j
G_1^j	Data privacy laws
G_2^j	Copyright infringement
G_3^j	Cybercrimes
S^j	Sector of entity j
$H_i(t)$	Historical experience of entity i during the time=t
$S_i(t)$	New experience of entity i during the time=t
ϵ_1	The wight of the direct trust
ϵ_2	The wight of the indirect trust
Tc	Information sharing competence
Tw	Information sharing willingness
Ti	Information sharing integrity
RI	Risk management value
$E1$, $E2$, $E3$, $E4$	The IS functions of competence, willingness, integrity and intent

Table 1 Acronyms

1.1 Threat information sharing goal

Threat information sharing [3] is the procedure to exchange relevant information about threats, attacks, and vulnerabilities between multiple stakeholders. The exchanged cyber threat information is any data that can help organizations to identify, assess, monitor, and mitigate cyber threats. TIS's goal is to improve the security level in organizations and provide security services to customers (see Fig. 1). The TIS process gives several benefits to the participating organization like:

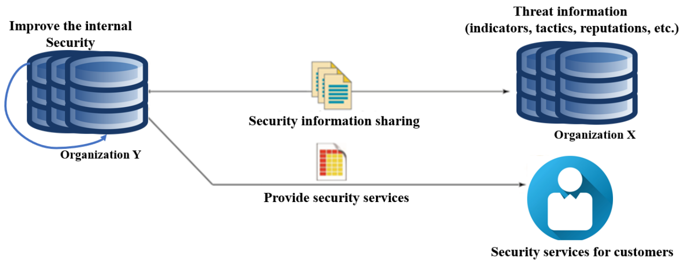

Improve the internal Security
Organization Y
Security information sharing
Threat information (indicators, tactics, reputations, etc.)
Organization X
Provide security services
Security services for customers

Fig. 1 TIS framework

1. Improve their security defenses in the organization: The TIS helps the organizations to better understand the environment and give a detailed overview of the risks, vulnerabilities, and attacks to provide a suitable security mechanism.
2. Bring the agility to the security safeguards: The organizations that share TI are more secure because they are informed about the threat changes and the need to detect and respond to the attacks. The security's agility minimizes both the response time and the probability of successful attacks.
3. Knowledge maturation, toward intelligence: The information enrichment process increases the amount of shared TI which improves the intelligence level of the security mitigation.

1.2 Threat information sharing types

The threat information can be classified into many categories based on the understanding level of the threats:

1. Indicators are the technical artifacts or observables that indicate the current activity of an attack. The indicators can include the Internet Protocol (IP) address of a suspicious user or request, also the Domain Name System (DNS) can be a direct indicator of the malicious domain. Moreover, the Uniform Resource Locator (URL) is used to indicate the nature of the continent.
2. Tactics, Technics and procedures (TTP) describe an actor's behavior. Tactics are a high-level description of a behavior. The word Tactics is meant to outline the way an adversary chooses to carry out his attack from the beginning to the end. Tactics describe how the threat actor operates during different steps of its operation/campaign. This includes tactics of gathering information for initial compromise, conducting the initial compromise, escalating privileges, performing lateral movement, deploying persistence measures, etc. Technics [3] provide a detailed description of the context of a

tactic. Procedures are the lower-level description, giving a detailed description of a technic. A precisely orchestrated tactical move that is carried out by using a set of techniques is needed. In other words, a special sequence of actions, known as procedures, is used by actors to execute every step in their attack cycle.

3. Security alerts or adversaries are technical security notifications regarding current vulnerabilities, risks and other security issues. The alerts may include the vulnerabilities advisories, high-level alert data, etc.
4. Strategic reports or threat intelligence reports are high-level documents that describe TTPs, actors, types of systems, and other threat-related information that provides a deep and extensive understanding of the attacks and greater security awareness to the organization
5. Tool configuration contains the information for updating the system while maintaining system integrity.

The authors in [4] described the multi-layer information sharing as a pyramidal architecture (see Fig. 2). They gave full and efficient answers to the following questions: How can these information types be shared and how they can be generated? For example, the lower layer of the pyramid comprises the important data related to the vulnerabilities, incidents, mitigations, and threats which can be shared with different groups publicly and without any constraint. However, the situational awareness level gives a detailed overview of specific information derived from the previous layer to respond to threats. The highest layer is the strategic analysis which refers to the in-depth analysis of data.

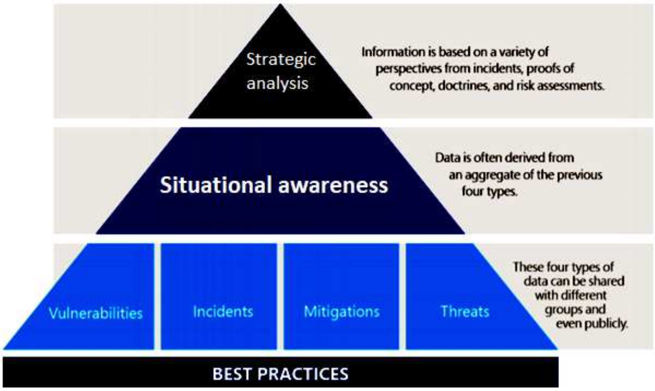

Strategic analysis
Information is based on a variety of perspectives from incidents, proofs of concept, doctrines, and risk assessments.
Situational awareness
Data is often derived from an aggregate of the previous four types.
Vulnerabilities
Incidents
Mitigations
Threats
These four types of data can be shared with different groups and even publicly.
BEST PRACTICES

Fig. 2 Types of cyber-security information which can be shared. Image courtesy of Microsoft [4]

1.3 TIS Architecture

Every company (stockholder) participating in the information sharing process is an entity. During the information sharing process, the organizations exchange the TI using two basic architectures: Centralized and distributed [5].

1.3.1 Centralized architecture

This architecture is usually labeled as "hub-and-spoke", where a central "hub" acts as a repository for information that is received from the spokes, i.e. participants members or any other sources. For example, SAMA PARTNERS may be considered as the hub and the other entities C_i building the community are the spokes. The index i is a number between 1 and N where N is the number of TIS participants. The hub's choice is related to many criteria, for example, scenarios, protocols, applications, etc. Information provided to the central repository by the TIS community participants is either directly forwarded to the community members or enhanced in some way by the hub before forwarding or disturbing it to the designated community members. SP can be the hub as well as the spoke based on the context and scenario. A drawback of using this architecture is that the threat information exchange is fully dependent on the central hub making it to a single point of failure, causing delays due to its network congestion and processing backlog. Another drawback is that all community members are affected if the central hub is not properly functioning or its performance is not satisfactory. Finally, the centralized hub is an attractive target for attack such as Denial Of Service (DOS) attack. Table 2 illustrates the advantages and limitations of the centralized architecture.

Benefits	Limitations
Low complexity	Abrupt failure
Simplicity	Security difficulties
Economical	Bottlenecks problem
Easy control and quick updates	Single point of failure

Table 2 Centralized architecture: Benefits vs limitations

1.3.2 Distributed architecture (peer-to-peer)

The distributed architecture is the opposite of centralized architecture. The absence of the hub characterizes it. The participants share information during the TIS process directly, rather than routing information through a central repository (hub). Therefore, each participant takes care of enrichment processes, including protecting and distributing information to the community members. The benefits and limitations are summarized in Table 3. Peer-to-peer architecture has several benefits. First, the threat information is shared in a peer-to-peer model. Therefore, it allows information to be distributed rapidly between the participants. Thus, this architecture gives more resiliency as information is available through different channels and does not represent a single point of failure or obvious target of attack. The peer-to-peer architecture has unfortunately also some drawbacks. Peer-to-peer architectures, which do not support standard formats and exchange protocols, may cause additional difficulties since all peers have to support different formats and protocols. When the number of peers in the community grows, the operating costs managing connections, information, e.g. collecting, enriching, protecting, and exchanging the trust relationships will grow exponentially.

Benefits	Limitations
Rapidity for the TS	Scaling difficulty
More secure	Complex
Resiliency	Expensive
Fault tolerance	Problems related to heterogeneity (protocols, formats, etc.)

Table 3 Distributed architecture: Benefits vs limitations

1.3.3 Hybrid architecture

The hybrid topology can be an efficient solution to overcome the limitations of the centralized and distributed architecture by combining the advantages of both discussed systems. In a hybrid architecture, a central hub may be responsible for resource discovery, broker sharing requests, or as a trusted third party for authentication. For example, an organization might exchange low-level intrusion alerts using a peer-to-peer architecture but send enriched alerts or incident reports to a central hub. Another use case involves sending the same information to peers individually, and the central hub. The hierarchical or cluster-based architecture can be a hybrid solution where both communications exist simultaneously. The architecture can be defined based on the use cases and different scenarios. Following Fig. 3 presents an example of the hybrid topology.

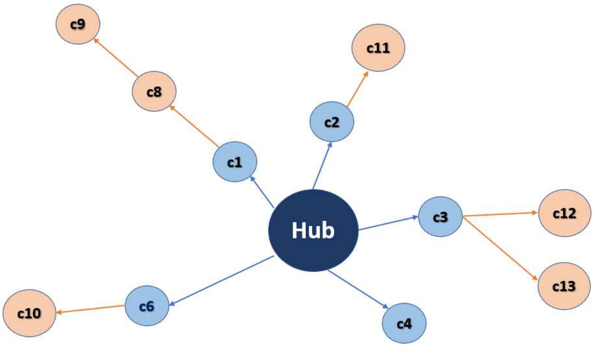


Fig. 3 Hybrid architecture example

1.4 TIS process

The threat information sharing process includes several steps (explained in Fig. 4). Before starting with information sharing, the organization must prepare the data to be shared through many sources. Then, it needs to establish the rules for the TIS process. In fact, the organizations involved in this process should identify the TI's list that may be shared without any constraints. The last step in the sharing process is to join a sharing community. In the next section, we will explain each step of the TIS process.

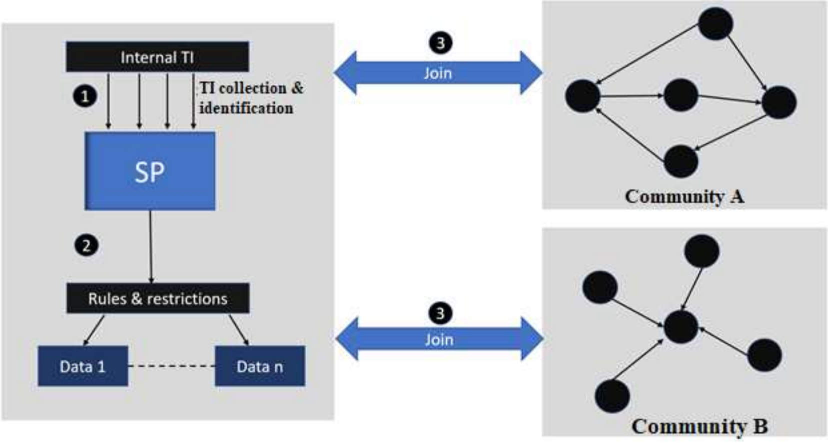


Fig. 4 Information sharing process

1.4.1 Scope of information sharing activities

The first and most important step in the preparation process is to define and specify the scope of IS. The organization must review the goals, objectives, and constraints during its eventual sharing activities. Identifying the IS scope can be achieved by identifying the types of information ready to be shared, the conditions of the permitted sharing, and companies or entities with whom the information can be shared. In our context, we need to identify the scope of information sharing. So, we need to address the previous questions.

1.4.2 Internal information selection

This process aims to provide continuous information collected from the organization's internal sources which can be classified into three categories. The examples of each category are illustrated in Fig. 5.

- The network data sources deliver the CTI data which are collected from the internal network analysis and monitoring. Examples of such sources are router, firewall, Wi-Fi, remote services, diagnostic and monitoring tools (IDS, packet capture, etc.).
- The host data sources deliver the CTI data which are collected from the different hosts. Examples of such sources are the OS, logs, antivirus products, web browsers, etc. That information helps to understand the threats related to the host.

- CTI data can be collected from other data sources like the emailing system or security information and event management.

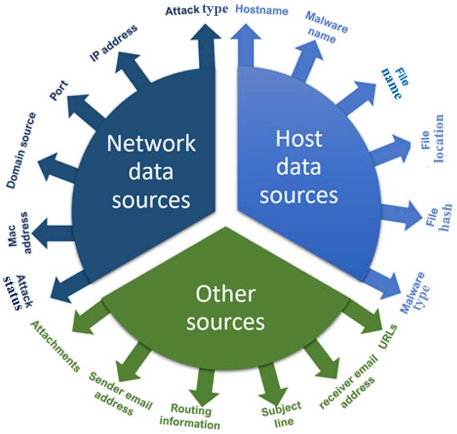


Fig. 5 Information sharing sources

1.4.3 Establish information sharing rules

The organization needs to protect its confidential and sensitive data by defining the rules and the information-sharing constraints. Moreover, the sharing conditions may be defined from the beginning to avoid sensitive information leakage. In fact, the organization must filter the information and classify the data into many categories: The basic classification is when the data is splitted into regular and sensitive data. The regular data can be shared with groups and even public organizations. However, sensitive data must be protected and shared only internally or with selected entities. For example, the network flow data contains sensitive information:

- Source and destination IP address
- Port and protocol information
- Byte counts and timestamps

Also, besides the need to identify the sensitive data and the rules of the sharing information, the organization needs to provide precise handling for any shared data. For example, the Traffic Light Protocol (TLP) [6] provides a framework for expressing sharing designations based on four labels illustrated in Fig. 6.

2 Trust and Reputation Management (TRM)

Generally, trust has several definitions according to the different disciplines in which it is used such as sociology, economics, philosophy, psychology, and information sharing context [7][8]. In the beginning, the trust should be defined in a general manner to understand the main idea and the basic concept of trust

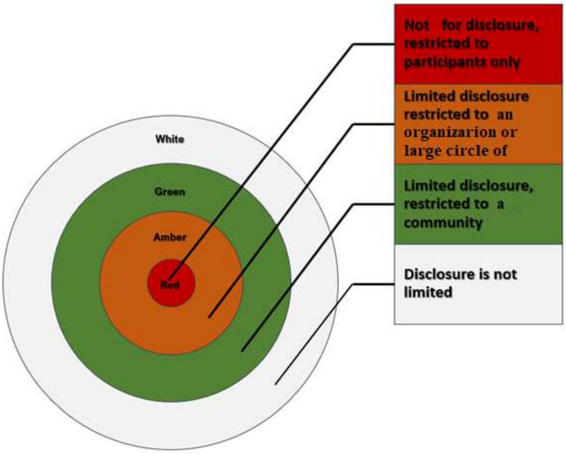

Not for disclosure, restricted to participants only
Limited disclosure restricted to an organizarion or large circle of
Limited disclosure, restricted to a community
Disclosure is not limited
White
Green
Amber
Red

Fig. 6 TLP version 1.0

management. In this context, trust represents an indicator for future actions based on the continuous interactions between entities. The trust management concept becomes so attractive in communication and networking security. The design of many networks and protocols uses this mechanism to build trust relationships among participating entities to create cooperative and collaborative environments to improve network performance. From the above discussions, it can conclude that generally, trust has the same main definition in different domains. Indeed, the differences appear only in the trust mechanisms and their sides (trustor, trustee). However, in the literature, the terms “trust,” “trustworthiness,” and “reputation” seem to be used interchangeably without clear distinction.

• Trust: It is defined as the subjective level of trustworthiness in which the aspect of belief plays an important role, and by which one (trustor) relies on another and expects that trustee would depend on its (trustor) own good. We define the trust level as the probability of trustworthiness varying from 0 (complete distrust) to 1 (complete trust).

• Trustworthiness: The trustworthiness is an objective probability by which the trustee performs a given action on which the trustor’s welfare depends.

• Reputation: The reputation can be defined as the opinion of one person or entity about the another, of one customer about a product, and by construct, of one node about another. In fact, trust is a derivation of the reputation of an entity. A trust level is computed for an entity by using the reputation. Indeed, the reputation itself has been built over time based on that entity’s behavior history.

2.1 TRM characteristics

• Trust is context-dependent: Trust has a specific context in its scope. For example, different types of trust (computational power trust, unselfishness trust, reporting trust, etc.) are required for a given task. In our case, the trust is computed for the information-sharing task.

• Trust is composability: Different composed functions can be used to aggregate the trust information depending on the situation and the kind of trust information. The trust value is computed based on the reputation values collected from the other information-sharing participants and direct trust.

• Trust is slow: High trust and reputation need time to be built. Trust values grow slowly with good participant behavior for an extended period, depending on the historical values.

• Trust is indirect: It is second-hand information. When the trust level is based on the other's recommendations about an entity that one does not know directly, it is considered as an indirect trust.

• Trust is direct: We talk about the first-hand information that should always be the most reliable. In our context, an entity (participant) uses its information, observation, and trust parameters to calculate the specific entity's trust value without external recommendations.

• Trust is subjective: If Alice thinks that Bob's ideas are good, John may not believe that Bob's ideas are good. In the information sharing environment, the trust level given to the same trustee entity can be different due to the various network topology changing dynamically, the attacks targeting the trust and reputation value, etc. Therefore, the trust value cannot be objective.

• Trust is not transitive: If John trusts Peter, and Peter trusts Carl, this does not mean that John trusts Carl. In our context, if an entity X trusts an entity Y and Y trusts node Z, this does not imply that X trusts Z. To use the trust transitivity between two entities to a third party, a trustor should trust a trustee as well as the trustee's recommendation of the third party.

• Trust is dynamic: The indirect trust measures collected from the other entities about a specific information provider are not equivalent and not always subjective. To capture the trust level's dynamicity, the latter should be expressed as a continuous rather than as a binary variable or even a discrete-valued entity.

• Trust is asymmetric: The higher participant in the information sharing process may not trust the companies with low information participation at the same level that companies with low participation trust companies with high participation. For example, in the studied framework, a supervisor tends to trust a student less than the student trusts the supervisor. Thus, we can conclude that the relationship between entities cannot be symmetric due to the degree of involvement, sector of the company, country of the company, credibility of the company, etc.

• Trust is propagative: If Alice knows Petric, who knows Stephany, and Alice does not know Stephany, then Alice can have some amount of trust in Stephany based on how much she trusts Petrick and how much Petrick trusts Stephany. In this context, if "A" trusts an entity "X" which trusts an entity "Y", so "A" may trust company "Y". The propagation is the most studied trust property.

• Trust is event sensitive: Trust takes a long time to be built. However, a single high-impact event may erase it completely. This trust aspect is less interested in computer science.

• Trust is self-reinforcing: Members act positively with other members whom they trust. Similarly, if the trust between two entities is below some threshold, it is highly unlikely that they will interact with each other, leading to even less trust in each other. This aspect of trust has received comparatively less attention in the literature.

2.2 TRM calculation

Two types of mechanisms can calculate the trust value: the direct and the indirect functions. Firstly, the direct function means that the trust is measured objectively based on the direct exchanges and interactions with a specific entity. The function of trust is composed of the dimensions of trust in information sharing. Secondly, the indirect function is defined by the other entities' collected opinions about a specific participant. This measure is based on the reputation systems. Finally, the hybrid mechanism is the most efficient and accurate where the two mechanisms are combined to exploit the advantages of both mechanisms. The trust measure is calculated by merging the direct and indirect interactions into an unique value.

3 Trust model for the IS model

3.1 State of the art

Sharing threat information may involve exposing the vulnerabilities of the hackers' entities, which may attract more attacks. In fact, the attackers take advantage of the gathered critical data (e.g., detecting new vulnerabilities, stop/disguise ongoing attacks) to launch more harsh attacks. Therefore, the entities hesitate to share information unless strong and trustworthy connections exist between the parties. Many researchers aimed to provide a trustworthy framework for information sharing based on trust management and reputation. In [9], the authors introduced a new trust model to protect the threat information sharing against the attackers. Moreover, they raised three dimensions of trust, willingness, competence, and intent derived from the social sciences and communication network domains. Furthermore, the authors in [10] proposed a Bayesian network-based trust and reputation mechanism that allows peers to discover the trustworthy partners who meet their requirements through three dimensions: the historical experiences, the quality of the transmitted data, and the recommendations (reputations) from the other entities. In the paper [11], the reputation measures and the historical experience are exploited in order to introduce a novel graph-based trust and reputation framework for social networks. Moreover, competence and willingness are used in [12] to build the agent-based model for trust and information sharing in networked systems. The need for trust in the information-sharing

Papers/ Dimensions	Competence	Willingness	Intent	Integrity	Interaction quality	Before Trust	Type of community	Type of commitments	Legal agreement	Capability of the entity	Data Privacy Laws	Copyright infringement	Cybercrimes	Sector	Historical experience	Penalty mechanism	Reputation measures	Zero-trust
[9]	×	×	×															
[10]					×										×		×	
[11]															×		×	
[12]	×	×																
[13]	×	×	×	×														
[14]	×	×		×													×	
Our proposal	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

Table 4 Trust based approaches classification

context increases in health systems. Trust becomes more and more indispensable in health information sharing where any information leakage will lead to a critical situation and a regional scandal. For this reason, the authors in [13] proposed a new trust model to secure the shared health information between the parties based on four dimensions: integrity, competence, willingness, and intent. In the same context, four different dimensions are illustrated in [14] to ensure the health information sharing in the health systems: competence, willingness, integrity, and reputation measures.

Most used approaches in the literature don't consider all the possible dimensions for trust structuring by focusing only on the following main dimensions: integrity, willingness, intent, and competence. In order to build an efficient and robust trust model for the information-sharing framework, new trust dimensions must be investigated to cover all the trust requirements for the trustworthy information-sharing process between the different parties (see Table 4).

3.2 Trust cycle

In this part, the life cycle of our trust model will be explained (Fig. 7) in order to calculate, update, or delete the trust values for a specific entity. The trust cycle is composed of two main phases:

- The initialization phase starts when a company aims at joining an existing community. A trustworthiness level must be established before engaging in a sharing information interaction with this new partner. The computed trust determines the entity's position inside the community and the impact of the entity on the information sharing process.
- The trust update phase is dedicated to recompute the trust after each IS interaction based on many dimensions. Indeed, this phase is composed of many sub-steps. Firstly, a trust model is defined in order to update the value of trust for each partner involved in the information sharing process. Then, the company 'X' must verify the trustworthiness of the partner 'Y' before sharing any information with it based on the trust measurements. Then, the decision to establish the information interaction is taken. A penalty mechanism can be introduced in order to counter the suspicious and malicious behavior of the

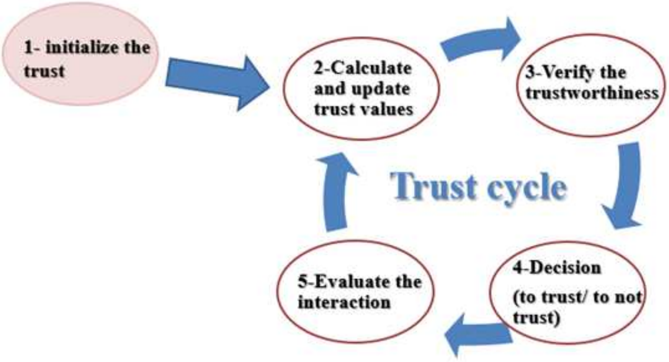

1- initialize the trust
2-Calculate and update trust values
3-Verify the trustworthiness
Trust cycle
4-Decision (to trust/ to not trust)
5-Evaluate the interaction

Fig. 7 Life cycle of the proposed trust model

company. If the company chooses to be involved in the information sharing process with the partner 'Y', an evaluation process is executed in order to assess the level of the interaction. The evaluation process is based on the answers to the following questions:

- Is the new entity aiming to join a public or private(targeted) community?
- Does the existing entity respect the information sharing processes requirements in terms of information competence/willingness/ intent/ integrity?
- Does the partner violate the established rules and agreements for information sharing?
- Is any change or update detected in terms of many metrics (as the position, capability, sector, etc.)?

The answers to the previous questions define the exhaustive and complete dimensions of our proposed trust model.

4 Private/ targeted community

In this section, the trust model for the private/targeted community is introduced. In fact, this type of community is closed with many restrictions where all the entities are supposed to be trustworthy. The proposed model is composed of two phases: The initial and the update of trust models.

4.1 Initial trust model

The initial trust is calculated based on the weighting modeling in order to give more importance and weight to a term. This model is defined through five composite dimensions illustrated by Fig. 8: Pre-trust, legal agreement, type of communities, entity capabilities and indirect trust.

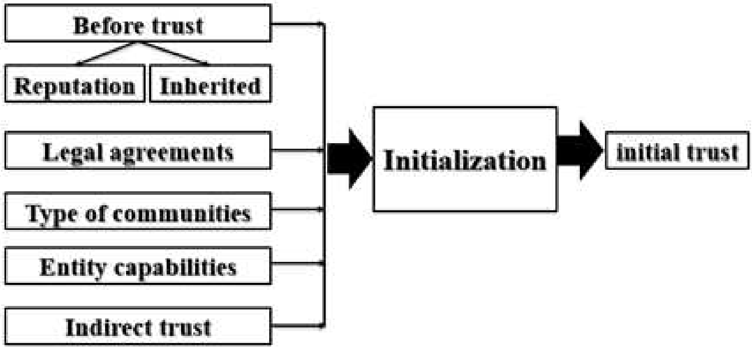


Fig. 8 Trust initialization

Moreover, the trust model is calculated through the following formula:

$$Tr_i = w_1 \times Tp_i + w_2(Ta_i) + w_3 \times Tc_i + w_4 \times C_i + \beta \tag{1}$$

Where w_i is the weight for the trust calculation:$\sum_{i=1}^{4} w_i = 1$.

4.1.1 Pre-trust

Pre-trust defines the level of the preliminary trust which is calculated based on the collected recommendations, so-called "reputation", of the other entities about the new participant and/or it can be inherited trust from an old participant. The pre-trust measurement denoted by Tp is equal to:

$$Tp_i = (In_i^j + R_i)/2 \tag{2}$$

Where the In and$R$ are respectively equivalent to the inherited trust and the collected reputations.
During the initial integration into the community, the entity can receive two types of trust measurements. The inherited trust (In) is a value of trustworthiness inherited by a company. In fact, every entity can introduce a new member to the community and it grants its trust value to the new participant as the inherited trust which is calculated as the following:

$$In_i^j = \frac{T_j}{Trust\ boundary} \tag{3}$$

Thus, the community collects the reputation values from all the members about the new entity through the following formula (4):

$$R_i = \frac{\sum_{j}^{N} R_j}{N \times Trust\ boundary} \tag{4}$$

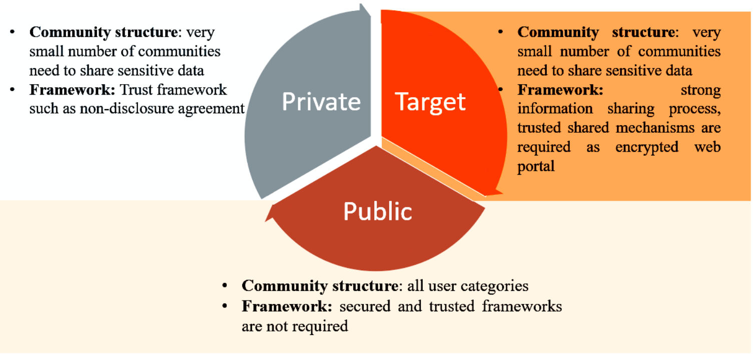
Finally, the community can anticipate the nature of the new entity based on a threshold explained through the following classification Table 5.

Nature	Condition	Pre-trust measure
Malicious	$Tp \in [0 - 0.4]$	0
Suspicious	$Tp \in]0.4 - 0.6[$	1
Suspicious	$Tp \in [0.6 - 1]$	2

Table 5 Pre-trust classification

4.1.2 Type of community

The second dimension is the type of community denoted by Tc_i because it deeply affects the initial trust. In the public community, the trusted framework is not necessary due to the membership's open nature. However, the targeted community is composed of a small number of members who need to share sensitive data. Therefore, a strong information-sharing framework and trusted sharing mechanisms are required, such as encrypted web portals in order to protect the shared data in the targeted community. Thus, a very secure framework is necessary for information sharing in the private community characterized by tiny members (see Fig. 9). The entity joined the private and targeted community, and has a high level of trust than the entity in the public community. Table 6 expresses the variation of trust.



- **Community structure**: very small number of communities need to share sensitive data
- **Framework:** Trust framework such as non-disclosure agreement
Private
Target
- **Community structure**: very small number of communities need to share sensitive data
- **Framework:** strong information sharing process, trusted shared mechanisms are required as encrypted web portal
Public
- **Community structure**: all user categories
- **Framework:** secured and trusted frameworks are not required

Fig. 9 Community's variation

Type of the community Tc_i	Trust measure
Public	0
Targeted	1
Private	2

Table 6 Trust-based communities classification

4.1.3 Legal agreement

The legal agreement is a contract signed by the entity before joining the community that stipulates that they will keep information private and will not under any circumstance disclose the information to a third party without authorization. The legal agreement, also referred to as a data confidentiality disclosure agreement ensures data privacy by preventing unauthorized access or disclosing data. The entity which signs this legal agreement can be trusted than the entity without a legal agreement. Therefore, the data confidentiality disclosure agreement considers as the third dimension denoted as Ta_i. The trust value related to this dimension is calculated based on Table 7. If the entity has good contrast with the community, the trust level is very high compared with the case with no signed agreement.

Legal agreement	Trust measure
Zero	0
Medium	1
High	2

Table 7 Trust based legal agreement classification

4.1.4 Capabilities

The capabilities of the entity inside the community denoted by Tc_i defines the next dimension. During the information sharing process, the entity's capability in terms of cyber-security knowledge can affect the trust level of this entity while joining the community. In fact, the community members trust the IBM company, known for their security solutions products, more than the companies without any cyber-security knowledge.

Legal agreement	Trust measure
Zero	0
Medium	1
High	2

Table 8 Trust-based capabilities classification

4.1.5 Indirect trust

In this part, the indirect trust dimensions, defined by the sector and the geolocation of the company, are introduced. On the one hand, the participant's sector can deeply affect the initial trust of the new entity. On the other hand, the localization of the entity in the world changes the trust initialization. In fact, every entity tends to trust more the participants localized in a safe area. The β is calculated through the following Table 9:

However, the geolocation dimension comprises three sub-dimensions:

Geolocation G	Sector S	Trust measure
Safe=1	Relevant=1	$\beta = G + S$
Medium=0.5	Medium=0.5	
Critical=0	Irrelevant=0	

Table 9 Trust-based indirect trust classification

- Data Privacy Laws (DPC): It is information privacy or data protection laws that prohibit the disclosure or misuse of information about private individuals in the country. From the map illustrated by Fig. 10, we can classify the countries based on data privacy laws into three categories: Countries with low, medium, and low data privacy laws. The initial trust of the joining entities is different based on the DPC categories.

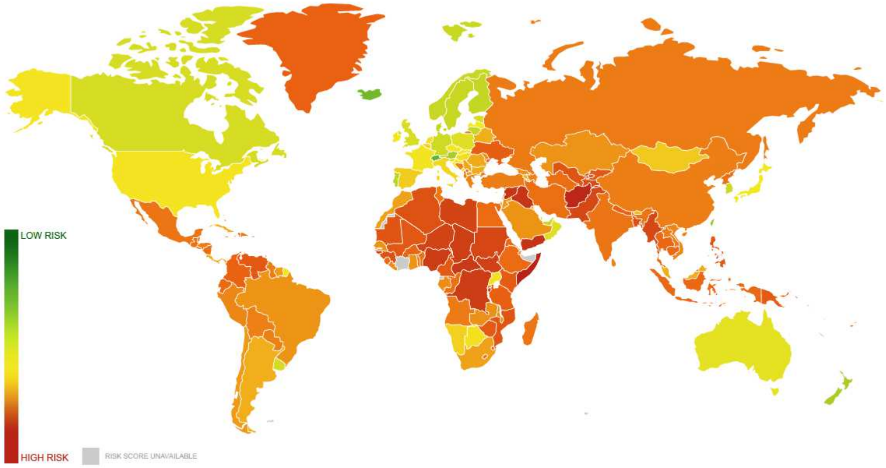
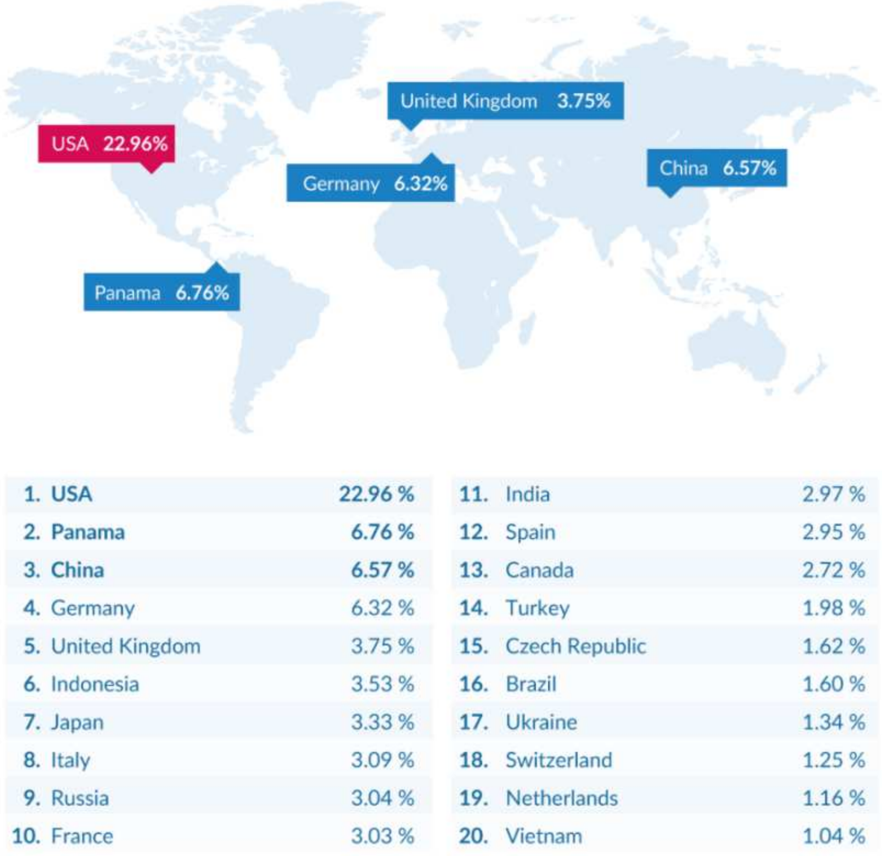


Fig. 10 Data privacy risk (Source: artmotion) [15]

- Copyright Infringement (CI): is comprised of the statistical analysis of many copy track user profiles. Illegal image uses have been investigated based on all search hits considered illegal by individual account holders, and website owner data based on information collected by internally developed web crawlers. Moreover, the entities located in countries with high copyright infringement are less trustworthy than countries with low copyright infringement. Therefore, the CI illustrated in Fig. 11 defines the geolocation sub-dimensions where we introduce three categories: the countries with low, medium, high CI.
- Cybercrimes (CC): It defines the most targeted countries from the cyber-attackers. It is the last dimension to measure the safeness of the country. In fact, we introduce three categories of countries based on the cybercrimes



1.	USA	22.96 %	11.	India	2.97 %
2.	Panama	6.76 %	12.	Spain	2.95 %
3.	China	6.57 %	13.	Canada	2.72 %
4.	Germany	6.32 %	14.	Turkey	1.98 %
5.	United Kingdom	3.75 %	15.	Czech Republic	1.62 %
6.	Indonesia	3.53 %	16.	Brazil	1.60 %
7.	Japan	3.33 %	17.	Ukraine	1.34 %
8.	Italy	3.09 %	18.	Switzerland	1.25 %
9.	Russia	3.04 %	19.	Netherlands	1.16 %
10.	France	3.03 %	20.	Vietnam	1.04 %

Fig. 11 Copyright infringement by country (Source: copy track) [16]

dimension: countries with low, medium and high cybercrimes (see Fig. 12). The initial trust is different from category to other.

The geolocation measure calculation is equal to the summation of all the sub-dimensions CI, CC and DPL which is illustrated through Table 11.

Data privacy laws $G_{i,1}$	Copyright infringement $G_{i,2}$	Cybercrimes $G_{i,3}$	Trust measure
High=1	Low=1	Low=1	$G_i = \frac{\sum_{j=1}^{3} G_{i,j}}{3}$
Medium=0.5	Medium=0.5	Medium=0.5	
Low=0	High=0	High=0	

Table 10 Trust based geolocation dimensions classification

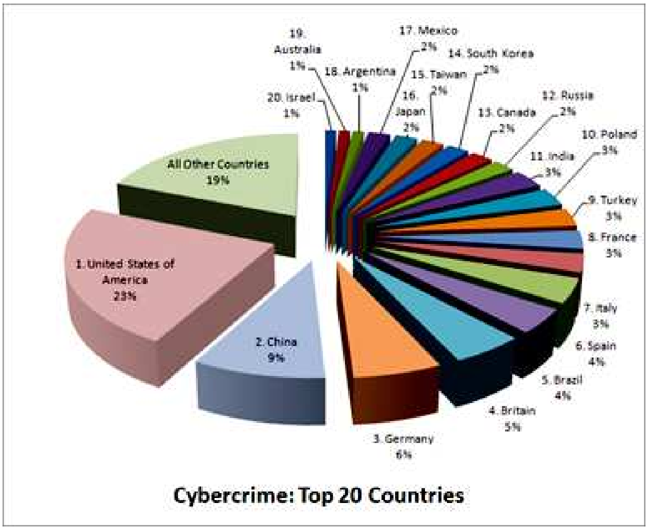


Fig. 12 Cybercrime by country (Source: copy track) [16]

4.2 Update trust model

The update of the trust measure is based on a time-based model with dynamic weighting and the historical experience with the entity. The new trust denoted as $Tr_i(t)$ is calculated through the following formula:

$$Tr_i(t) = H_i(t) + S_i(t) \tag{5}$$

H, S are the historical experiences, the new experience (negative/positive), and the indirect trust dimension.

The historical experience is defined as the value of the previous trust and the previous reputations collected from the other nodes about the entity i. Trust is a subjective value calculated from the direct interaction with a specific entity which can lead to inaccurate and not precise measurements. Therefore, a hybrid system is introduced by combining the reputations collected from the other nodes and the trust value to adjust the final trust's computation.

$$H_i(t) = \epsilon_1 \times Tr_i(t-1) + \epsilon_2 \times \frac{\sum_{j=1}^{N} R_j^i(t-1)}{N} \tag{6}$$

Where ϵ_1, ϵ_2 are the direct and indirect trust parameters and are fixed respectively to 0.8 and 0.2. The parameters will be validated and adjusted through the simulations.
Moreover, the trust can be increased or decreased according to the new interaction with this entity. The organization evaluates the interaction according to the three previous dimensions. S is the negative or positive experience with

entity i during the time t. The evaluation is expressed through the following formula:

$$S(t) = \frac{E1(Tc) + E2(Tw) + E3(Ti) + E4}{4} \tag{7}$$

Where S $\in [-1 - 1]$ and $E1$, $E2$, and $E3$ are the functions representing respectively the competence, the willingness, the integrity, and the intent. Thus, Tc, Tw, and Ti are the dimensions of the new experience.

Fig. 13 explains the dimensions of the new experience update. The model starts with evaluating the interaction with an entity $'A'$ based on the three dimensions: integrity, competence, and willingness. However, those criteria are not efficient in evaluating the entity because the judgment can be unjust and incorrect due to many factors. As a solution, reputation measures is introduced as an enhancement factor to improve the trust model's efficiency. After the trust computation, the reputations collected from the nodes will be evaluated.

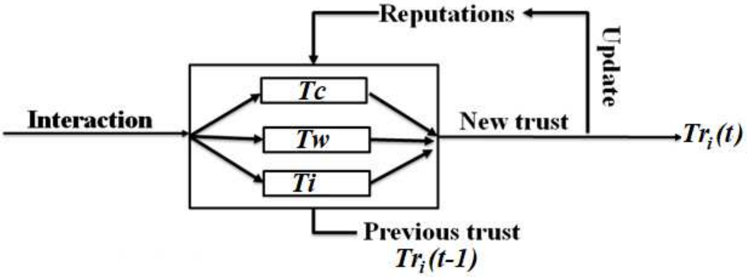


Fig. 13 Trust dimensions for the new experience

4.2.1 Competence and Willingness

To update the trust values, the model analyses the received information from entity i in terms of the competence of shared data and the company's willingness during the information sharing process.

- Competence Tc is defined as the entity's ability to accomplish the task by providing a useful service. In our information sharing context, is considered a quality dimension defining the competence of the data during the information sharing process.
- Willingness determines the intention of the entity to share valuable data. Tw can be measure as the amount of information that circulates from a node to another.

The function $E1$ and $E2$ are introduced in [9] based on the beta-binomial distribution to evaluate the competence and the willingness of the shared information. We compare the $E1$ and $E2$ to thresholds in order to evaluate whitener the trust is high or low as follow:

$$E1 = \begin{cases} 1 & \text{if } E1 > Th_1 \\ -1 & \text{if } E1 < Th_1 \end{cases} \tag{8}$$

$$E2 = \begin{cases} 1 & \text{if } E2 > Th_2 \\ -1 & \text{if } E2 < Th_2 \end{cases} \tag{9}$$

Where Th_1 and Th_2 are the thresholds for $E1$ and $E2$.

4.2.2 Integrity

The organization must have sophisticated security mechanisms in order to filter the received information and protect the system against malicious shared data. For example, the first defensive layer will be the firewall and the intrusion detection system. Then, after each interaction, the participant will measure the number of alerts and classify the risks into categories in order to evaluate the interaction with a specific participant. T_i measures the number of alerts during the information sharing process. Then, the risk of T_i is estimated, which is called R_i. The risk assessment categories are presented through Table 11.

Risk Values	Significations
0,1,2,3	Low
4,5,6	Medium
7,8	High
9,10	Critical

Table 11 Risk assessment categories

In order to evaluate whether the interaction is trustworthy or unsafe, we introduce the integrity evaluation defined by function $E3(T_i)$ where we assess the received alerts during the information sharing process based on the four risk management classifications. Then the$E3$ is defined based on two risk tests.

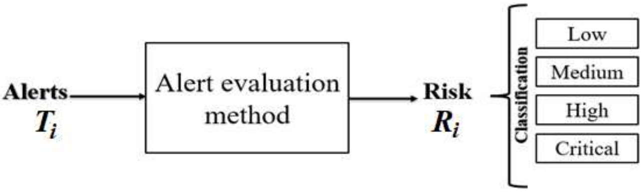


Fig. 14 Integrity proposed function

If the calculated risk is upper than a threshold, the $E3$ is equal to 1 and -1 for the inverse case explained through the following formula:

$$E3(T_i) = \begin{matrix} -1 & \text{if } R_i^j \in [7-10] \\ 1 & \text{if } R_i^j \in [0-6] \end{matrix} \quad (10)$$

4.2.3 Intent

In our model, the intent denoted as $E4$ is the reputation's consistency during a predefined period. The consistency behavior is to deliver correct reputation values to the requesting entity. The entity with inconsistent behavior is considered a possible Sybil attacker. Therefore, the intent is another dimension in our trust model. $E4$ is calculated as the correlation (reputation collected from entity i about entity j, reputations from all entities about entity j) and T_h is the threshold.

$$E4(T_i) = \begin{cases} 1 & \text{if } diff(R_i^j, AVG(\sum R)) < Th_4 \\ -1 & \text{if } diff(R_i^j, AVG(\sum R)) > Th_4 \end{cases} \quad (11)$$

Where diff() is a function to calculate the difference between two parameters and AVG is a function to calculate the average between the reputation of entity i about entity j and the average of all the collected reputations about the entity j.

4.3 Penalty mechanism

Another level of security defense is applied to contain suspicious and malicious entities. Besides the decreasing reputation system for the misbehaving entities, a new penalty mechanism is defined for the private/targeted community to exempt the malicious entities from the information sharing process during a predefined period. A central entity is introduced which is responsible for the collection of the reputations about a specific entity from all the participants. It then applies a majority decision to remove or to keep the suspicious entity during a predefined period. Moreover, this central entity broadcasts the decision between all the entities and controls the suspicious entities. If the punished entities continue the malicious behaviors, they will be eliminated eventually and for good from the community.

5 Public community

In this section, the updated trust model for the public community is proposed and detailed. This type of community is different from the private and targeted communities. Moreover, it requires new constraints and considerations related to its public nature, where all the entities are considered suspicious. The community is open without any restrictions for the members joining. To protect the public community, which attracts strikingly malicious entities, the zero trust and the update trust model are defined.

5.1 Zero Trust

The zero trust model [17] was introduced by the analyst firm Forrester Research to reinforce the security defense against hostile attacks in information security. Behind this model, there is a unique rule of ”never trust, always verify”. Thus, all data traffic generated must be untrusted, no matter if it has been generated from the internal or external network. The zero-trust model is applied to secure many emergent applications such as the IoT [18]. Therefore, the zero-trust concept is applied to initialize the new entities' trust values before joining the public community. The trust value is equal to zero for all the new entities:

$$Tr_i = 0 \tag{12}$$

5.2 Update trust model

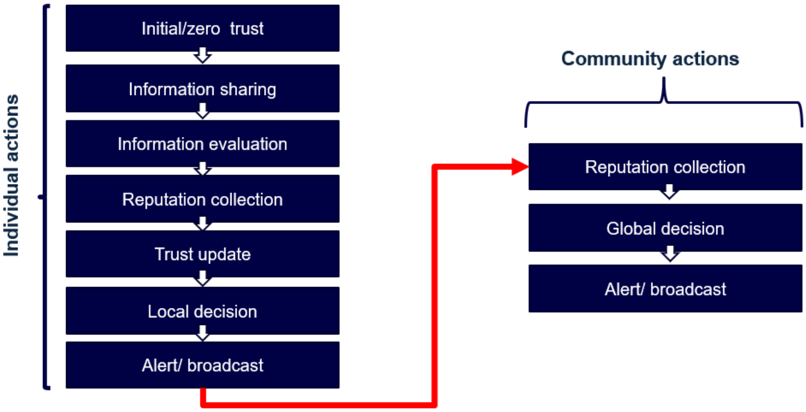


Fig. 15 The features of the CMT model

The trust values are updated after the information sharing evaluation. The quality, intent, willingness, and competence are direct dimensions to assess the new experience. Moreover, the reputations and the direct trust values are used to assess the historical experience. Therefore, the same trust update calculation is applied (see Eq. 5) for the private community to reveal the new values of trust after sharing the threat information between the entities.

5.3 Implementation

In this section, the main features resuming the model goals are discussed. Then, the algorithm for the CMT model executed by the entities is illustrated during the threat information sharing process.

5.3.1 CMT model's features

The difference between the actions and functions executed by the individual entity and those committed by all the community are distinguished (see Fig. 15).

- For the first case: This model starts by calculating the initial trust for the new entity. Then, after the peer-to-peer interaction, each entity evaluates the quality of the shared information based on the collected reputation values from all the participants in the community. Thus, the entity updates the trust values of the other participants. Moreover, the entity decides locally whether it keeps the information-sharing relationship with the previously communicated entity or stops communicating with it. The local decision is communicated with the other entities to beware of this suspicious entity. When the entity detects continuous individual hostile behaviour, an alert will be sent to the hub through alert system in order to inform the centralized entity about this targeted attack. The centralized entity controls the suspicious entity and takes the appropriate security measurement if a malicious behaviour is detected.
- For the second case: In order to take a majority decision about a suspicious entity, the community collects the reputation values from all the participants. If the mean reputation values are under a threshold, this entity is considered officially malicious and will be removed from the community. Otherwise, the community keeps the activities of this entity with caution.

5.3.2 CMT model's Algorithm

The following algorithm explains the implemented instructions during the information sharing phase. Moreover, the complexity of this algorithm 1 is calculated, which is equal to $\theta(N^2)$, where N is the number of entities in the network.

6 Simulations and results

6.1 Simulation setup

Simulations are performed using Matlab software based on two basic scenarios. The paper's purpose is to evaluate the efficiency of the proposed trust model in a hostile environment. Fig. 16 shows the graphic illustration of the trust based models and the connection between the different entities during the network initialization and before launching the attacks.

The simulations aim to study the behavior and efficiency of the trust model under the Random-Byzantine Attack (RBZ) [19] where the adversary has full control of an authenticated device and can perform arbitrary behavior to disrupt the system. During the simulations, the mean reputation ratio is studied as the main metric to be compared between the public and private communities based on three variables: The number of attackers, the number of entities, and the time (interaction number). The mean reputation ratio is the mean

Algorithm 1 Trust model

```
Input:
  • Entities are participating in information sharing.
  • $N$: Number of entities in the network.
  • Type of communities
Output: trust and reputation values after the information sharing.
if $ET_i$ is new then
    Identify the type of community
    if The community is public then
        ZeroTRust();
        /* Calculate the zero trust based on Eq.12*/ else
        InitialTRust();
        /* Calculate the initial trust based on Eq.1*/
    end if
    MajorityDecision();
    /* Majority decision is called in order to determine if the request of joining the community will be approved or denied */
end if
for Each $ET_i$ asks for the information sharing do
    for $j = 1, j++, N$ do
        $ListOfEntity \leftarrow EntitySelection(ET, R_i^j)$
    end for
    for $j = 1, j++, ListOfEntity$ do
        /* Start the information sharing with the entities */
        $S_j(t) \leftarrow InfoEvaluation(ListOfEntity, j, information)$ based on Eq.7
        Ask for the reputation values about the entity $ET_j$ from all entities
        $H_j \leftarrow HistoricalExperience(Reputations, Trust)$ based on Eq.6
        Calculate the new trust value $Tr_i(t)$ according to Eq.5
        if $Tr_i(t)$ ¡ threshold then
            checkStatus();
            if $ET_i$ is suspicious then
                Status ← malicious;
                LocalPenality();
                /* Remove the link with the malicious entity */
                AlertTOcommunity()
                /* Broadcast the local decision and ask for a global decision */;
            end if
        end if
    end for
end for
for Each interaction do
    for $j = 1, j++, N$ do
        GlobalDecision(status, R, Alerts);
        /* the global decision is a vote which seeks for determining whether the entity $ET_j$ will be removing or not from the community */
        BroadcastDecision();
    end for
end for
```

value of reputation collected from all the entities in the network. The three variables are:

- The attacker's number is a percentage of the attackers launching the RBZ (between 5% and 70%).

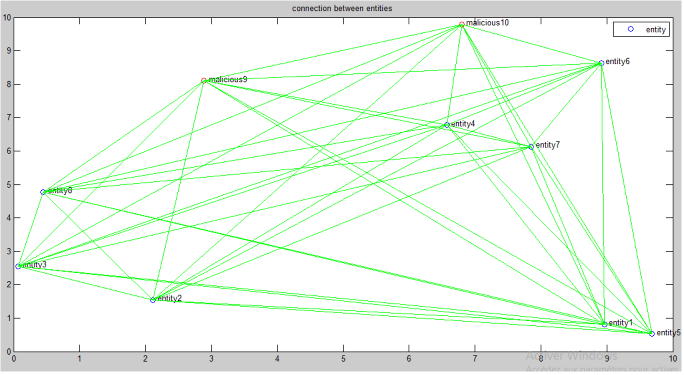


Fig. 16 Network initialization

- The entities number represents the number of the participants in the information sharing context (between 10 and 30).
- The time is defined by the sharing information interactions number (between 10 and 30).

6.2 Results and interpretations

Fig. 17 illustrates a 3D demonstration with 4-dimensional data where the mean reputation ratio is simulated in terms of the number of attackers, the number of entities and the time under the RBZ attack in the private community. The

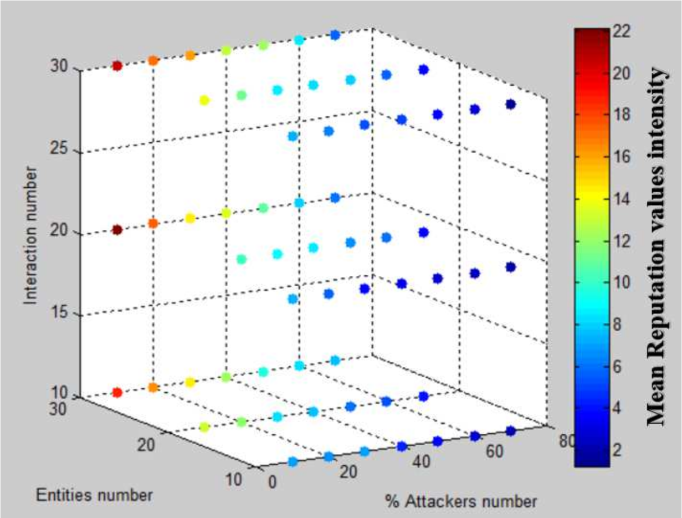


Fig. 17 3D Demonstration with 4-dimensional data: The mean reputation ratio variation

obtained results show that the number of attacks affects the mean reputation ratio which decreases progressively to a low level. When the number of attackers increases, the shared data will be affected: Quality, integrity, quantity, and intent which are the proposed dimensions used to evaluate the interaction and also to calculate the reputation values. However, Fig. 17 exhibits that our model maintains a higher reputation ratio equals to 12 even with the high number of attackers equals to 50% with 30 interactions and 30 entities. We conclude that our model shows a high resistance and stability in a very hostile environment which is explicated by the two mechanisms of penalties proposed by the CMT model: it decreases the reputation values for the malicious users and then it applies a penalty mechanism (by the individual or by all the community). Moreover, we find that reputation values increase in terms of time. In fact, this is the previously studied property of trust (Trust is slow: High trust and reputation need time to be built. Trust values grow slowly with the good participant behavior at a long period, depending on the historical values.). So, the number of interactions reinforces the reputation measures evolution. Furthermore, we find that there is a correlation between the number of entities and the mean reputation ratio. The more we raise the entity's number inside the community the more the precision of the reputation is ameliorated and the ratio is increased. This result confirmed the theoretical proposed formula 6 where the reputation calculation depends essentially on the number of participants. We observe that cooperative behavior among entities is less affected by the threat or vulnerability in the information sharing environment. The more the entities are involved and cooperative in the trust and reputation process, where they are requested to share their trust calculation about an entity to rate its behaviors, the more the environment is secure and resistant against the attackers. This cooperative behavior is ensured and rewarded by our trust

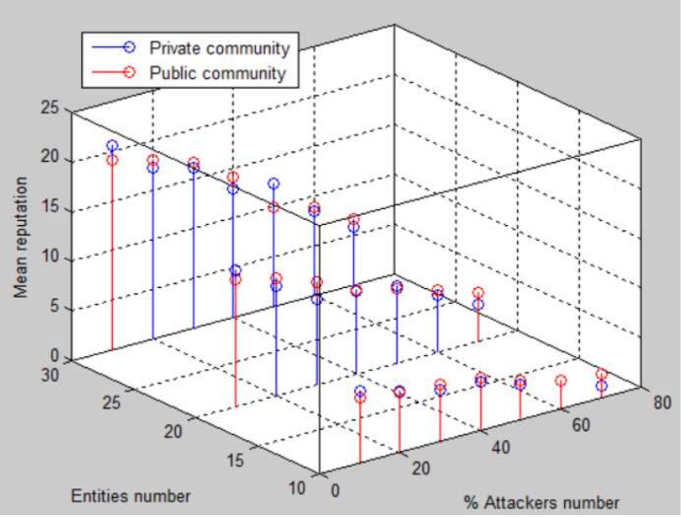


Fig. 18 3D Demonstration of the mean reputation ratio: Public vs private communities

model through the quantity dimension where each cooperative interaction will increase the entity's trust model. The proposal can resist as we observed in the previous figure, against many harmful attacks even against the Sybil attack targeting the reputations systems to fraud and mislead the entities inside the closed communities. The intent dimension guarantees the protection against those types of attacks targeting the reputations values by detecting any variation between the mean reputations and the individual reputations calculated by a single entity. Moreover, the proposed penalty mechanism contains this malicious behavior as a new security safeguard layer for our CMT model. The detected attackers with faulty reputation will be punished until he adopts the honest behaviors or banned from the system.

Thus, the most critical attack is the single-target attack where the adversary launches malicious behaviors against a single victim. However, the proposed trust model resists against single-target attacks by our alert systems that can catch this particular attack. Table 12 resumes the proposed dimensions of the CMT which are responsible to prevent many crucial attacks.

Model	Attacks Type		
	Random-Byzantine Attack	Reputation attack	Single-target attack
CMT model	All the proposed dimensions	Intent and penalty	Alert systems and penality

Table 12 Dimensions of CMT responsible of attack prevention

To conclude, many parameters have a direct and indirect impact on the CMT model for the first scenario which is the private community:

- Time or the number interactions between entities: We discussed the effect of time in the CMT model of the information sharing experiments. The detected significant variation indicates that the mean reputation values increase over time.
- Number and type of attacks: Many attacks were investigated and simulated to validate the efficiency of the proposed model in a hostile private community. The model enhances the security of the information sharing environment by maintaining the stability and the reliability of the reputation systems against increasing malicious users.
- Number of entities: We discussed the impact of the increasing number of entities inside the private community. The main argument explaining why we observed mean reputation value enhancement in terms of the increasing number of entities is because of the abundance of the reputation values about an entity which makes the mean more reliable and more exhausted.
- Nature of cooperation between entities: We determined that the cooperative environment improves the accuracy of reputation systems in the private community by providing more information and reputation values to verify the credibility of the requested entity after each interaction. Repeated

interaction with partial information feedback suffices to induce reputation concern and threats.

Fig. 18 illustrates the mean reputation ratio in the private and public communities under the increasing number of attackers, interactions, and entities. This comparison aims to study the behavior of the trust-based model for each community in a malicious environment. The results indicate that the private community outcomes the public community for the first interactions (due to the initial trust). This is equal to 22 for the private community and 19 for the public community. However, the mean reputation ratio of the private community is more event-sensitive than the public community due to the closed nature of the community where the malicious behavior can destruct entirely the community. For this reason, the mean reputation ratio of the public community overcomes the private community during the attack launching. To further discuss the results of Fig. 18, we need to investigate the three stimuli of our simulations:

- Time or the interactions between entities: During the initial time, the two models start by calculating the initial trust for the private community and the zero-trust for the public community. Since the initial trust model contains many dimensions compared with 0 dimension for the zero-trust model, the resulting initial trust and reputation for the private community must be higher than the public community. This theoretical analysis is confirmed by the simulation. As time goes by, the public community shows more resistance against the attacks, this is explicated by the nature of the framework. The credibility of entities in private community are higher than the public one. Therefore, the entities inside this open environment are more aware about sharing and receiving information from the other entities. However, the impact of malicious event is more dangerous in the private and targeted communities since the entities trust each others.
- Attacks variation: Attacks, information leaks, or threats are more dangerous and have a harmful impact on the private community. On another hand, all entities are aware of the open nature of the public community, and they will not share sensitive or critical data in this infrastructure. Therefore, the impact of attacks will be limited and manageable compared with the private community. The results in Fig. 18 confirm the theoretical analysis where the public community overcomes the private community by maintaining higher mean reputation values.
- Entity variation: The increasing number of entities have a similar impact on the private and public communities. The two curves are almost merged in many locations but the private curve remains in the foreground only for the initial interaction explicated by the initial trust values.

To conclude, the two CMT models maintain a high mean reputation ratio under the harmful attacks in the public and private communities. The behavior and the resistance of the two models are similar however, the CMT model for the public model shows a better resistance during the launching attack. Table

13 illustrates the comparison between the private and public communities in terms of the variation of time, number of entities and number of attacks. We note that this discussion is intended only for illustrative purposes and requires further empirical and field research to be definitive with the consideration of many real-case scenarios.

Community	System initialization			Functioning system		
	Time	Entity variation	Attacks	Time	Entity variation	Attacks
Public	++	++	++	+++	+++	+++
Private	+++	+++	+++	++	++	++

Table 13 Public and private communities' comparison

7 Conclusion and discussion

One of the key techniques to ensure security is to share and receive relevant information related to the security (the type of attack, the technology, type of alerts, etc.) to understand the attack's behavior and predict and mitigate the security problems. However, the shared information can be itself the source of classical and new vulnerabilities and security threats affecting the participants. Therefore, trust and reputation management have been used to overcome the security and leakage of critical data in the information sharing field. In this paper, we propose two efficient and robust security schemes based on trust and reputation frameworks to secure information sharing against harmful attacks. We introduce a first trust model to ensure the information exchange inside the private and targeted community based on existing and novel trust dimensions. Thus, we formulated a second trust model for the public community based on zero-trust to protect information sharing inside the open-nature environment. The simulation results validate the theoretical analysis and demonstrated that our approach shows high adaptability and resistance in a malicious large-scale network. The proposal maintains a high and efficient mean reputation ratio in the private and public communities.

As possible future ongoing research, we aim to propose a distributed architecture based on the Blockchain solution to secure not only the information sharing framework but also to ensure the integrity and trustworthiness of exchanged trust and reputation measures. We also intend to apply a machine learning method to secure the CMT approach against malicious entities launching sophisticated attacks.

Declarations

- Ethics approval and Consent to participate : No ethical approval is required.
- Consent for publication: Not applicable.

- Human and Animal Ethics: No human and animal ethics approval is required.
- Availability of supporting data: Data sharing not applicable to this article as no datasets were generated or analysed during the current study
- Competing interests: The author declares no conflict of interest.
- Funding: Not applicable.
- Authors' contributions: Jihen Bennaceur, and Wissem Zouaghi contributed to the study conception and design. Material preparation, data collection and analysis were performed by Jihen Bennaceur, and Wissem Zouaghi. The first draft of the manuscript was written by Jihen Bennaceur. All authors read and approved the final manuscript.
- Acknowledgments: No applicable.

References

[1] Thomas Olsson, Martin Hell, Martin Höst, Ulrik Franke, Markus Borg, *Sharing of vulnerability information among companies – a survey of Swedish companies*, 45th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), Greece, 2019.

[2] Yue Wu1 , Yimeng Zhao, Michel Riguidel, Guanghao Wang and Ping Yi, *Security and trust management in opportunistic networks: a survey*, SECURITY AND COMMUNICATION NETWORKS, 2015.

[3] Ozalp Ozer, Upender Subramanian, Yu Wang, *Information Sharing, Advice Provision, or Delegation: What Leads to Higher Trust and Trustworthiness?*, Management Science, 2018

[4] Goodwin, Nicholas, Bryant, J. Ciglic, K. Kleiner, A. Kutterer, C.Sullivan, *A framework for cybersecurity information sharing and risk reduction*, Retrieved from http:download.microsoft.comdownload801801358EC2A0A-4675-A2E7-96C2E7B93E73Framework for Cybersecurity Info_Sharing.pdf

[5] Gordon LA, Loeb MP, Lucyshyn W, Sohail T, *The impact of the Sarbanes-Oxley act on the corporate disclosures of information security activities*, Journal of Accounting Public Policy, pages 503–530, 2006

[6] David Sutton, *Trusted information sharing for cyber situational awareness*, Elektrotechnik und Informationstechnik- Springer, 2015

[7] Diego De Siqueira Braga, Marco Niemann, Bernd Hellingrath, Fernando Buarque Neto, *Survey on Computational Trust and Reputation Models*, Journal on ACM Computing Surveys, Vol. 51, No. 5, 2018

[8] Adis Medić, *Survey of Computer Trust and Reputation Models – The Literature Overview*, International Journal of Information and Communication Technology Research, Vol. 2, No. 3, 2012

[9] Kevin Chan, Jin-Hee Cho, Sibel Adalı, *Composite Trust Model for an Information Sharing Scenario*, 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing, 2012

[10] Yao Wang, Julita Vassileva, *Trust and Reputation Model in Peer-to-Peer Networks*, Peer-to-Peer Computing conference, 2003

[11] RaquelUreña, Francisco Chiclana, Enrique Herrera-Viedma,*DeciTrustNET: A graph based trust and reputation framework for social networks*, journal on information fusion, Vol. 61, pages 101-112, 2020

[12] Kevin Chan, Sibel Adalı, *An Agent Based Model for Trust and Information Sharing in Networked Systems*, International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, 2012

[13] Jodyn E. Platt, Peter D. Jacobson, and Sharon L. R. Kardia,*Public Trust in Health Information Sharing: A Measure of System Trust*, journal on Health Serv Res, pages 824–845, 2018

[14] Jodyn E. Platt, Peter D. Jacobson, and Sharon L. R. Kardia,*Public Trust in Health Information Sharing: Implications for Biobanking and Electronic Health Record Systems* , journal on personalized medicine, Vol. 5, pages3-21, 2015.

[15] https://artmotion.eu/en/insights/cloud-security-risks-map.html

[16] https://www.copytrack.com/wp-content/uploads/2019/04/190328 _Global_Infringement_Report_2019_EN_Online.pdf

[17] J. Kindervag, "No More Chewy Centers : Introducing The Zero Trust Model Of Information Security," pp. 1–15, 2010

[18] Mayra Samaniego, Ralph Deters, "Zero-Trust Hierarchical Management in IoT", IEEE International Congress on Internet of Things (ICIOT), 2018

[19] Sekgoari Mapunya, Mthulisi Velempini, *the Design of Byzantine Attack Mitigation Scheme in Cognitive Radio Ad-hoc Networks*, International Conference on Intelligent and Innovative Computing Applications (ICONIC), 2018