Taxonomy of Governance Mechanisms for Trust Management In Smart Dynamic Ecosystems

Dasa Kusnirakova[a] and Barbora Buhnova[b]
Faculty of Informatics, Masaryk University, Brno, Czech Republic

Keywords: Trust, Trust Management, Governance, Taxonomy, Smart Dynamic Ecosystems.

Abstract: In our evolving society, a future is envisioned where humans and digital systems converge to shape dynamic and unpredictable ecosystems constantly adapting to ever-changing conditions. Such smart dynamic ecosystems, which seamlessly merge digital agents, physical infrastructure, and human-technology interactions, need to enable the formation of partnerships between their members to collectively solve complex tasks. This necessitates the establishment of trust together with effective governance mechanisms on the ecosystem level, which emerge as crucial elements to ensure the proper functioning, safety, and adherence to established rules. However, there is currently very little understanding of what such trust-supporting governance mechanisms could look like. In this paper, we open this promising scientific field with compiling a taxonomy of governance mechanisms aimed at supporting trust management in smart dynamic ecosystems. By this, we take an initial step into the development of a comprehensive governance model and stimulate further research to address this critical aspect of managing the complex and dynamic nature of these ecosystems.

1 INTRODUCTION

Our society is moving towards the future where digital systems, physical objects and social interactions among humans and technology all seamlessly merge to form intelligent and adaptive ecosystems (Liu et al., 2011; Capilla et al., 2021). These smart dynamic ecosystems, where all the members interact, collaborate, and adapt to the constantly changing needs of the environment (Xia and Ma, 2011), are however inherently unpredictable.

The need of ecosystem members to form partnerships and collaborate with others in order to collectively solve complex tasks thus calls for establishing trust, a crucial and yet under-researched concept necessary to support human-to-machine and machine-to-machine interactions (Schreieck et al., 2016; Mechanic, 1996).

Several studies underscore the key role of building and maintaining trust among the members of smart dynamic ecosystems for the successful adoption of autonomous and intelligent technologies (Capilla et al., 2021; Beer et al., 2014). The concept of trust and its importance within the digital world can play a major role, for instance, in selecting trusted information or service providers among various smart agents in the ecosystem, or as a self-protection mechanism against untrusted and potentially malicious agents (Buhnova et al., 2023), such as those designed with the intention to cause harm or deceive and manipulate others.

Besides establishing trust among the ecosystem's agents, effective governance is crucial to guarantee the proper functioning of such dynamic ecosystems in terms of safety and adherence to established rules. This governance includes developing strategies and rules (Schreieck et al., 2016) based on the specific needs of the ecosystem in question, i.e. rules for entering the ecosystem, ensuring trustworthy communication and forming partnerships among ecosystem's members. An efficient governance model should also encompass mechanisms for upholding moral and ethical responsibility and advancing principles like solidarity and fairness. Otherwise, agents might behave unethically or perform actions endangering other members or disrupting the whole ecosystem. Yet, the current understanding of the mechanisms and components that shall form such a governance model is so far very fragmented.

In this paper, we propose a taxonomy of governance mechanisms for trust management in smart dy-

[a] https://orcid.org/0000-0002-5341-902X
[b] https://orcid.org/0000-0003-4205-101X

Kusnirakova, D. and Buhnova, B.
Taxonomy of Governance Mechanisms for Trust Management In Smart Dynamic Ecosystems.
DOI: 10.5220/0012726100003687

In *Proceedings of the 19th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2024)*, pages 700-710
ISBN: 978-989-758-696-5; ISSN: 2184-4895

namic ecosystems, compiled from a review of existing literature. We believe that via interconnecting the fragmented knowledge on the topic, this paper offers a solid ground for the scientific community to stimulate further research and collaboration to address the critical aspect of managing the complex and dynamic nature of smart dynamic ecosystems.

The rest of this paper is organized as follows. Section 2 summarizes the related work, while section 3 describes the methodology employed to build the proposed taxonomy of governance mechanisms for smart dynamic ecosystems. The taxonomy itself is presented in section 4. Afterward, sections 5 and 6 conclude the paper with a discussion of future research directions.

2 RELATED WORK

The governance of trust management in smart dynamic ecosystems represents a complex research field in its scope (i.e., what research challenges need to be addressed), breadth (i.e., what mechanisms and in which interplay are needed to address the challenges), and depth of the individual mechanisms (i.e., what are the effective ways to address the individual challenges). While attempts to the depth aspect of the challenge exist in the literature, unless there is an understanding of the breadth and scope of the problem, which is currently very fragmented, we can hardly hope for an effective solution to the problem.

A notable pillar of knowledge in terms of taxonomies addressing the governance of quality aspects in complex ecosystems can be traced in Social Internet of Things (SIoT) (Alkhabbas et al., 2019), which however focuses on technical-quality aspects, such as ensuring resilience (Berger et al., 2021), security (Williams et al., 2019; Rizvi et al., 2018), or service discovery (Roopa et al., 2019), instead of trust. On the other hand, the works that focus on categorizing the aspects of trust and trust management within SIoT (Ahmed et al., 2019; Chahal et al., 2020; Ahmed et al., 2020), recognizing trust as the fundamental building block of SIoT (Khan et al., 2020) needed for effective interactions and collaboration of SIoT members, focus on particular aspects of trust such as properties, metrics, and trust attacks, leaving the governance mechanisms for trust management largely unexplored.

Governance in the context of Internet of Things (IoT) has been researched from the direction of decision-making (Almeida et al., 2017), and roles and responsibilities management (Gerber and Kansal, 2020), while unfortunately overlooking trust-based governance. Besides, considerable research effort has been dedicated to developing governance mechanisms and frameworks for Cyber-Physical-Social Systems (CPSS) (Katina and Keating, 2018; Katina et al., 2017). These works predominantly focus on individual systems, though, rather than holistically addressing the governance needs of entire ecosystems in which CPSS operate, and thus lack systematic organization of the necessary mechanisms.

As for the field of software ecosystems, there exist studies addressing trust management (Hou and Jansen, 2023) and governance (Alves et al., 2017) issues. However, it is crucial to recognize that smart dynamic ecosystems diverge from software ecosystems as the former encompasses a blend of physical and digital entities, adapting to real-world conditions, while the latter predominantly involves digital components and applications operating in virtual spaces. Due to this key difference, the principles and strategies employed in trust management and governance within software ecosystems cannot directly translate to the complexities presented by smart dynamic ecosystems but need to be addressed separately.

To sum up, while notable sources of knowledge exist on the fragments of the topic, there is a lack of (1) a comprehensive taxonomy of governance mechanisms, (2) tailored for smart dynamic ecosystems and (3) centered around trust. In this paper, we fill the gap by introducing an initial version of the taxonomy of governance mechanisms for trust management in smart dynamic ecosystems.

3 METHODOLOGY

To identify relevant papers, we conducted an exploratory search across electronic academic databases. The search utilized combinations of keywords on *trust*, *trust management*, *govern**, *IoT*, and *SIoT* to retrieve an initial set of papers. This collection was further expanded by incorporating selected reference papers cited in the initial set. The collected papers were then examined with a focus on the identification of mechanisms essential for the governance of trust management within smart dynamic ecosystems.

In order to classify the collected governance mechanisms, a classification scheme was developed following the methodology proposed by Usman et al. (Usman et al., 2017). Thus, we applied the following four phases: (1) Planning, (2) Identification and Extraction, (3) Design and Construction, and (4) Validation.

Table 1: References for *Trust Score Management* and *Ecosystem Wellbeing Management* mechanisms.

Trust Score Management

Trust Evidence Collection	Trust Metrics	QoS Metrics	Quality of Service (QoS) trust metrics (Xiao et al., 2015; Bao and Chen, 2012b)
		Social Metrics	social interactions (Yan et al., 2016), social metrics (Buhnova et al., 2023), honesty (Yan et al., 2016; Nitti et al., 2013), openness (Iqbal and Buhnova, 2022), fairness (Nwebonyi et al., 2019)
	Time Dimension		social trust parameters (Chen et al., 2014; Bao and Chen, 2012a)
		Past Behaviour	past subjective experiences (Gwak et al., 2017), past behaviours (Meena Kowshalya and Valarmathi, 2017)
		Present Behaviour	present experience (Buhnova, 2023), present behavior (Mehdizadeh and Farzaneh, 2022)
		Future Behaviour	futuristic behaviours (Meena Kowshalya and Valarmathi, 2017)
Trust Score Computation	Local		subjective trust calculation (Ghafari et al., 2020; Bo et al., 2017), distributed computing (Asiri and Miri, 2016)
	Global		centralized authority for computations (Asiri and Miri, 2016), guarantor (Clarke et al., 2013)
Trust Score Propagation	From Members to Central Authority		global share (Nitti et al., 2013), centralized (Resnick et al., 2000), reputation centre (Jøsang et al., 2007)
	From Members to Members		distributed collaborating filtering (Chen et al., 2014), distributed (Kamvar et al., 2003; Mendoza and Kleinschmidt, 2015), distributed stores (Jøsang et al., 2007)
	From Central Authority to Members		from central authority (Jøsang et al., 2007), intermediate or provider (Nitti et al., 2013)
Trust Score Lifecycle	Initialization		initial trust value (Chen et al., 2015), entrance of a new object (Atzori et al., 2012)
	Update		trust update (Chen et al., 2014; He et al., 2020; Peng et al., 2008), value update (Namal et al., 2015)
	Erosion		trust erosion (Sagar et al., 2022; Truong et al., 2017; Rana et al., 2022)

Ecosystem Wellbeing Management

Incentive Mechanisms	Reward Mechanisms	reward mechanisms (Bangui et al., 2023a; Bangui et al., 2023b; Guo et al., 2021; Zhaofeng et al., 2019; Malik et al., 2019; Xiaoxue et al., 2010), reward system (Singh and Kim, 2018)
	Punishment Mechanisms	punishment mechanisms (Bangui et al., 2023a; Bangui et al., 2023b; Guo et al., 2021; Xiaoxue et al., 2010), punishment (Etalle et al., 2007), penalties (Malik et al., 2019)
Safety Assurance	Isolation of Untrusted Members	isolate untrusted devices (Banerjee et al., 2018), isolation module (Hategekimana et al., 2020)
	Isolation of Trust Management Disruptors	isolation of attacking nodes (Muzammal et al., 2020; Alsumayt et al., 2017), isolating malicious devices (Nandhini et al., 2022; Seshadri et al., 2020; Ahmed et al., 2015)
Detection of Trust Management Disruptors	Detection of Disruptive Members	detection of malicious nodes (Liu et al., 2019; She et al., 2019; Li et al., 2020; Wang and Wei, 2021; Khatun et al., 2019; Illi et al., 2023)
	Detection of Trust Attacks	trust attack detection (Caminha et al., 2018; Abdelghani et al., 2019; Marche and Nitti, 2020; Masmoudi et al., 2020; Magdich et al., 2021)
Trade-off Analysis in Decision Making	Resolving Conflicting Values, Interests and Goals	conflicting preferences (Zavvos et al., 2021), conflicting information (Kökciyan and Yolum, 2020)
	Detection of Discrimination	discrimination of objects (Jafarian et al., 2020; Illi et al., 2023), discrimination attack (Marche and Nitti, 2020)
Corrective Mechanisms	Trust Score/Decision Reassessment	self-correction (Lochner and Smilek, 2023), trust miscomputation (Khan et al., 2015), feedback loop (Bangui et al., 2023a)
	Correction of Trust Score Miscomputation	self-correction (Lochner and Smilek, 2023), trust miscomputation (Khan et al., 2015)
	Reparation/Compensation of Affected Members	trust compensation (Yu et al., 2017)

The initial phase involved the planning process, where the ideas for the classification scheme were collected. In the second phase, the dimensions for the classification of governance mechanisms were developed, drawn from the grouping of the mechanisms found in the literature. This was performed iteratively by the authors and each dimension was discussed and agreed by the authors. Moving into the third phase, the taxonomy was constructed by combining proposed dimensions and validated in the fourth phase by correspondence and backward snowball analysis searches that have been used in the taxonomy descriptions, as elaborated in the discussion in section 5.2. The complete list of references for individual mechanisms is provided in Table 1.

4 TAXONOMY

One of the initial findings when exploring the collected governance mechanisms is the clustering of the mechanisms around two core concepts: trust assessment and trust assurance. While the governance mechanisms connected to trust assessment can be explained as answering the question of ”Can I trust?”,

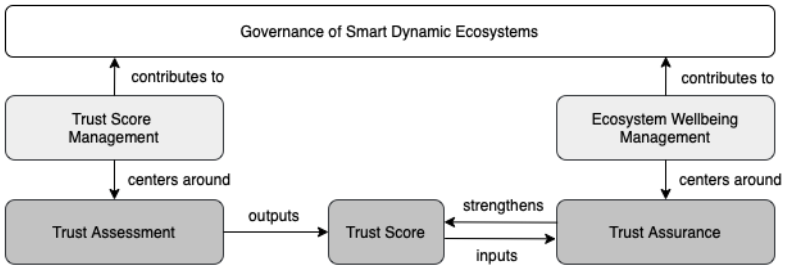

Figure 1: Relationship between Trust Assessment and Trust Assurance, and their contribution to governance.

the governance mechanisms connected to trust assurance can be essentially reduced to the support of answering the question of "How to ensure I can trust?".

The former cluster consists of mechanisms of trust score computation, collection of trust evidence and inputs for such computation, trust score propagation, and management of the trust score over time, and is referred to as *Trust Score Management* in our taxonomy introduced in section 4.1.

The latter cluster consists of incentive mechanisms to motivate trustworthy behaviour (and punish its violations), detection of untrustworthy members and their isolation to promote safety and wellbeing of the remaining ecosystem members, and corrective mechanisms in case of trust misjudgement and discrimination that happens in effect of that. We refer to this cluster as *Ecosystem Wellbeing Management*, which is presented in section 4.2.

The symbiotic relationship between these two clusters is visualized in 1. *Trust Score Management* activities center around trust assessment. It serves as the foundation for the initial evaluations of each ecosystem member's trustworthiness. Once an entity is assessed for trust, it is awarded a trust score, and trust assurance comes into play. This is the center of *Ecosystem Wellbeing Management* mechanisms, whose role is to gradually increase the trustworthiness of individual members (via motivating them to better behaviour and expelling disruptors). Together, *Trust Score Management* and *Ecosystem Wellbeing Management* contribute to the governance of smart dynamic ecosystems by creating a cycle that reinforces and sustains the concept of trust within the ecosystem over time.

4.1 Trust Score Management

The focus of Trust Score Management mechanisms centers around trust assessment, i.e. awarding a trust score to an entity. In order to do that, there need to be mechanisms in place responsible for collecting evidence that serves as input data for trust score calculation, keeping the scores updated, and propagating it across the network.

We describe the governance mechanisms responsible for trust score management in the following paragraphs and summarize them in 2.

1. *Trust Evidence Collection and Information Gathering*

   Collecting information is a necessary prerequisite for the calculation of trust scores representing the trustworthiness of individual ecosystem members. These trust scores are calculated on the basis of selected features called trust metrics, that are monitored and combined in time (Meena Kowshalya and Valarmathi, 2017).

   Trust metrics capture different qualities of interactions occurring between agents. These can refer to QoS metrics reflecting the ability of an agent to provide quality services in terms of reliability or accuracy (Xiao et al., 2015; Bao and Chen, 2012b). Other mechanisms focus on capturing social relationships among agents in terms of honesty, openness, altruism, or unselfishness (Nitti et al., 2013) by monitoring social metrics.

   To address the time dimension, it is necessary to consider mechanisms that monitor past, present, and future behaviour. Monitoring trust metrics over time enables the ecosystem to gain understanding of how trust dynamics changes and to adapt to evolving trust scenarios by feeding design-time, runtime, and predictive models, respectively, and allows for the anticipation of potential malicious intentions (Meena Kowshalya and Valarmathi, 2017).

   Evidence collection also serves as a promising tool for justifying decisions that might be opposed by certain ecosystem agents, detecting any potential trust attacks, and proving malicious intentions of agents before they become fully evident (Buhnova, 2023).

   Note that in all these cases, various mechanisms can be in place to promote the exchange of the metrics between the trustor and the trustee. However, as trust is essentially a belief of the trustor

about the trustee's trustworthiness, the trustor needs to be given a way to validate the metrics themselves, which can be supported by the trustee by sharing an explanation of their actual or intended actions (Iqbal and Buhnova, 2022).

2. *Trust Score Computation*

   Different mechanisms must be applied to calculate trust scores at different levels of the ecosystem. Typically, the literature mentions local and global trust score computation (Ghafari et al., 2020).

   Local trust scores are calculated on the ecosystem member level. They are derived from agent-to-agent relationships, which involve the assessment of one agent's trustworthiness by another, utilizing local information such as current observations or past experience. In contrast, global trust score extends beyond individual interactions, representing an agent's reputation within the broader ecosystem. In this context, each agent's reputation is linked to the local trust scores assigned by other agents in the ecosystem, creating a network of mutual influence on overall trustworthiness. These calculations are made at the central authority level, e.g. by reputation models (Asiri and Miri, 2016).

3. *Trust Score Propagation*

   Trust score propagation describes how trust information spreads throughout the network. There are various kinds of trust score propagation schemes found in the literature – (1) centralized schemes depending on a central node that is responsible for gathering trust-related data and propagating it across the network (Nitti et al., 2013), (2) decentralized schemes where each ecosystem member is responsible for trust computation and propagation on its own (Chen et al., 2014), and (3) hybrid schemes combining centralized and decentralized principles (Nitti et al., 2013).

   While centralized schemes are vulnerable to a single point of failure and are not suitable for large-scale networks (Karthik and Ananthanarayana, 2017), decentralized schemes face challenges associated with limited computational capacity of individual nodes and unbiased propagation of trust scores across the network (Jøsang et al., 2007). Since hybrid schemes are able to mitigate the challenges of both aforementioned propagation schemes (Karthik and Ananthanarayana, 2017), they are frequently employed throughout the research works (Karthik and Ananthanarayana, 2017; Mahmood et al., 2019). It is, therefore, necessary to ensure that appropriate trust score propagation mechanisms are employed in the ecosystem. These include mechanisms capable of propagating individual trust scores not only between members of the ecosystem and the central authority (in both directions) but also among the members themselves.

4. *Trust Score Lifecycle*

   Besides the evidence collection, computation and propagation of trust scores throughout the ecosystem, governance mechanisms dealing with trust score lifecycle need to be established, too. Trust score lifecycle covers multiple phases, namely the trust score (1) initialization, (2) update and (3) erosion, and shall be implemented at both the local levels (i.e., ecosystem members storing the trust scores of their peers) and global levels (i.e., trust scores managed by the global reputation model). They are responsible for ensuring the integrity and reliability of the scoring system.

   The mechanisms for trust score initialization (sometimes referred to as bootstrapping) are responsible for assigning a trust score value to agents newly entering the ecosystem without any previous records (Atzori et al., 2012). Determining the appropriate initial trust score value is a challenging task (Chen et al., 2015). If the initial trust score is too low, new agents might experience difficulties in engaging in meaningful interactions with other agents within the ecosystem, as they are not trusted. On the other hand, setting the initial trust score value too high may pose a risk that malicious agents could exploit this initial trust to inflict harm before being identified as untrustworthy, or abuse it to whitewash their reputation via leaving and re-entering the ecosystem with a clean trust score.

   The update phase demands dynamic mechanisms that facilitate real-time adjustments, considering evolving circumstances and agents' behaviour. The updates are typically managed through event-driven, time-driven, or hybrid approaches. In the event-driven scenario, trust scores are updated upon the completion of an interaction with other agents, or after a specific event has occurred (Chen et al., 2014). However, this approach introduces the drawback of increased network traffic overhead. Alternatively, in the time-driven approach, trust is updated regularly at specific time intervals, ensuring a periodic assessment of an agent's trust score (Namal et al., 2015). Lastly, the hybrid approach combines both aforementioned approaches, enabling trust updates at set intervals and/or in response to

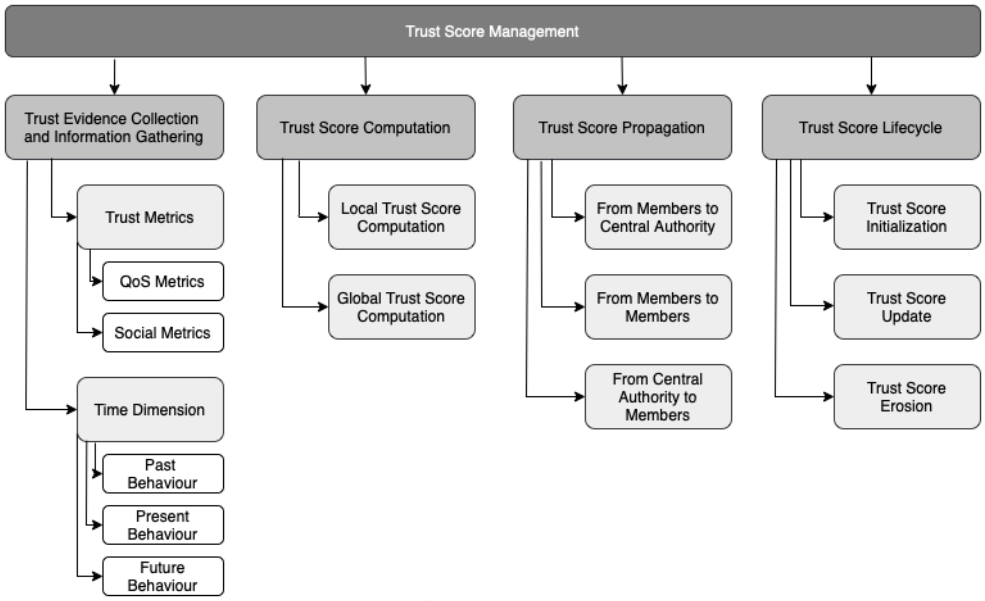

Figure 2: Taxonomy of Governance Mechanisms for Trust Score Management.

specific events or interactions (Xiao et al., 2015).

In addition to the dynamic nature of an agent's trust score within the ecosystem, a high trust score or reputation shall deteriorate towards a neutral value when an agent experiences a lack of interactions or engages in too few interactions (Truong et al., 2017). It is therefore necessary to establish mechanisms taking into account the lifespan of trust values, whereby the trust score of inactive agents undergoes the erosion process after a specified duration of inactivity (Sagar et al., 2022) in order to keep the trust scores up to date.

4.2 Ecosystem Wellbeing Management

Trust represents a valuable resource influencing the overall health of the ecosystem. It elevates various aspects of the ecosystem wellbeing, such as the ability for the ecosystem members to depend on each other and feel safe, fairness by promoting equitable interactions and decision-making, or solidarity through encouraging collaboration and mutual support within the ecosystem.

In the following paragraphs, we list the governance mechanisms responsible for the ecosystem wellbeing identified in our study. The mechanisms are also summarized in 3.

1. *Incentive Mechanisms*

   Encouraging behaviours aligned with ecosystem's rules and values belongs to the key mechanism for enhancing the well-being of the ecosystem that need to be established. This is being achieved through incentives, i.e. a system of rewards and punishments. The decision to reward or punish an agent can be determined by various factors, e.g. its current trust score or based on the recent relative changes in it, such as an increase or decrease (Bangui et al., 2023a; Bangui et al., 2023b).

2. *Safety Assurance*

   Given that trust in smart dynamic ecosystems is understood as *"the attitude or belief of an agent (trustor) to achieve a specific goal in interaction with another agent (trustee) under uncertainty and vulnerability"* (Buhnova, 2023), trust management is only meaningful in the environments where the members feel vulnerable in some way. This lies behind the importance of safety assurance on the ecosystem level, which needs to be in place to protect vulnerable members in the presence of members with questionable trustability.

   Ensuring safety within the ecosystem is closely tied to the ability to expel or isolate untrusted agents, which might be dangerous, or disruptors, which are assumed to disrupt the wellbeing of the ecosystem. In situations where trust is used to navigate the sharing of information or provision of services, the trustor can easily choose not to use the knowledge or services provided by untrustworthy agents. However, in complex scenarios involving physical safety and human lives, e.g. avoiding collisions with malicious autonomous

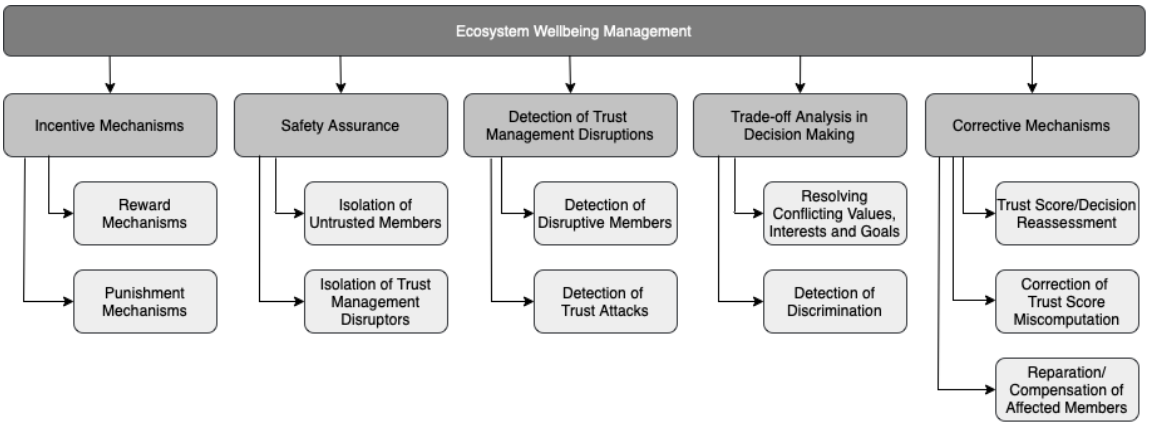

Figure 3: Taxonomy of Governance Mechanisms for Ecosystem Wellbeing Management.

vehicles, ensuring safety becomes a challenging task. In these cases, it becomes essential to avoid the collision by employing mechanisms of adaptive function restriction in order to regulate the ability of untrusted members to cause harm (Halasz and Buhnova, 2022).

3. *Detection of Trust Management Disruptions*
   To be able to deal with misbehaving agents, it is first crucial to have mechanisms in place capable of identifying ongoing disruptions within the ecosystem (Sagar et al., 2022). Detecting these disruptions involves not only identifying malicious agents as such, but also encompasses the recognition of various trust attacks that substantially undermine the fundamental pillars of the ecosystem.

4. *Corrective Mechanisms*
   It is essential to implement mechanisms that enable corrections of past trust decisions or eliminations of unfairness observed in the ecosystem in order to maintain a just and fair environment. These mechanisms do not only include identification and elimination of injustice such as discrimination or unfairness occurring within the ecosystem (e.g. newly joining agents facing issues with earning the required trust for establishing meaningful interactions), but also allow to correct trust misjudgements (Bangui et al., 2023a) made in the past, all by reassessing trust scores, correcting trust score miscomputations, and providing compensation to the affected agents.

5. *Trade-off Analysis in Decision Making*
   A smart ecosystem represents a place where often the collective objectives of individual systems, their goals, and the goals of human members intersect (Tofangchi et al., 2021). Within this dynamic setting and all ongoing interactions, conflicts may arise. For instance, while the ecosystem as a whole may prioritize efficiency, agents may seek full control over their actions. Simultaneously, people may require privacy and ethical considerations in their interactions with the ecosystem. Effectively managing these conflicting values and finding common ground requires governance mechanisms that achieve a balance between pursuing the goals of all involved parties. For instance, trust-based trade-off analysis using incentives could serve as a tool for resolving conflicting values, interests, and goals within a smart dynamic ecosystem. Members striving toward the ecosystem's shared goals could be rewarded with special tokens, which could then be replaced as a form of currency in case a member wants to prioritize its own goals even if they may not align with the goals of the ecosystem as a whole.

5 DISCUSSION

While this paper only takes the initial steps towards a comprehensive taxonomy of governance mechanisms for trust management in smart dynamic ecosystems, we believe it lays a solid foundation covering the breadth of the governance mechanisms for this challenging context, which can serve as a starting point for the research community filling the necessary details.

5.1 Opportunities for Further Research

Building upon the initial work presented in this paper, further research can focus on studying the governance of smart dynamic ecosystems in more depth, classifying the individual mechanisms according to more parameters and refining them to deeper levels of

categorization. Then, a possible research path is the development of a comprehensive governance model, systematically organizing the identified governance mechanisms within a structured framework. Such a model would provide a holistic understanding of the relationships and dependencies among various governance components.

Next, there is an opportunity to explore the creation of a logical architecture that aligns with the previously mentioned governance model. Such an architecture would facilitate the implementation of effective governance mechanisms in diverse smart dynamic ecosystems. The steps towards composing the logical architecture involve the identification of the ecosystem's actors, defining their roles, and investigating the network of the relationships among them. The contribution of such an architecture lies in its ability to provide the underlying structure of smart dynamic ecosystems, and thereby provide guidance for the development of future governance mechanisms tailored to these ecosystems.

Last, each of the identified governance mechanisms would deserve a proper examination and research of its underlying principles, especially in the context of the governance mechanisms it shall be integrated with. Understanding these deeper levels of detail is necessary for leading the discussion about implementing trust management governance in terms of both technology and policy making.

5.2 Threats to Validity

To promote the external validity of the taxonomy, which is threatened by the possibility of overlooking papers that could substantially impact the findings, a proactive approach was taken to mitigate the risk. We employed a backward snowball analysis, which allowed us to extend our reach beyond the initially identified papers and ensured a more comprehensive inclusion of relevant sources. Besides, we iteratively re-examined the identified keywords to ensure that variations of trust governance terminology are covered.

To maximize the internal validity, which is influenced by our expertise in taxonomy creation, the correspondence analysis was employed, drawing on insights from five reference papers (Sagar et al., 2022; Buhnova et al., 2023; Berger et al., 2021; Ahmed et al., 2019; Chahal et al., 2020) published in the last four years. This methodological choice served to enhance the credibility of the taxonomy by aligning it with established literature and ensuring that the distinctions made were well-founded.

6 CONCLUSION

The aim of this paper was to propose a taxonomy of governance mechanisms desgined for trust management in smart dynamic ecosystems. To achieve this, we reviewed the existing literature, identified the key governance principles and organized them in a cohesive structure. The proposed taxonomy serves as a starting point for further discussion and research within this field. Our intention is to stimulate the exploration of governance mechanisms, and fostering a deeper understanding of the necessities and complexities involved in governing trust within smart dynamic ecosystems.

ACKNOWLEDGEMENTS

The work was supported by Grant Agency of Masaryk University (GAMU), Interdisciplinary Research Projects sub-programme, project "Forensic Support for Building Trust in Smart Software Ecosystems" (no. MUNI/G/1142/2022).

REFERENCES

Abdelghani, W., Zayani, C. A., Amous, I., and Sèdes, F. (2019). Trust evaluation model for attack detection in social internet of things. In *Risks and Security of Internet and Systems: 13th International Conference, CRiSIS 2018, Arcachon, France, October 16–18, 2018, Revised Selected Papers 13*, pages 48–64. Springer.

Ahmed, A., Abu Bakar, K., Channa, M. I., Haseeb, K., and Khan, A. W. (2015). A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. *Frontiers of Computer Science*, 9:280–296.

Ahmed, A. I. A., Ab Hamid, S. H., Gani, A., Khan, M. K., et al. (2019). Trust and reputation for internet of things: Fundamentals, taxonomy, and open research challenges. *Journal of Network and Computer Applications*, 145:102409.

Ahmed, K. I., Tahir, M., and Lau, S. L. (2020). Trust management for iot security: Taxonomy and future research directions. In *2020 IEEE Conference on Application, Information and Network Security (AINS)*, pages 26–31. IEEE, IEEE.

Alkhabbas, F., Spalazzese, R., and Davidsson, P. (2019). Characterizing internet of things systems through taxonomies: A systematic mapping study. *Internet of Things*, 7:100084.

Almeida, V. A., Goh, B., and Doneda, D. (2017). A principles-based approach to govern the iot ecosystem. *IEEE Internet Computing*, 21(4):78–81.

Alsumayt, A., Haggerty, J., and Lotfi, A. (2017). Using trust to detect denial of service attacks in the internet

of things over manets. *International Journal of Space-Based and Situated Computing*, 7(1):43–56.

Alves, C., de Oliveira, J. A. P., and Jansen, S. (2017). Software ecosystems governance-a systematic literature review and research agenda. *ICEIS (3)*, pages 215–226.

Asiri, S. and Miri, A. (2016). An iot trust and reputation model based on recommender systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pages 561–568. IEEE.

Atzori, L., Iera, A., Morabito, G., and Nitti, M. (2012). The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. *Computer networks*, 56(16):3594–3608.

Banerjee, M., Lee, J., Chen, Q., and Choo, K.-K. R. (2018). Blockchain-based security layer for identification and isolation of malicious things in iot: A conceptual design. In *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–6. IEEE.

Bangui, H., Cioroaica, E., Ge, M., and Buhnova, B. (2023a). Deep-learning based trust management with self-adaptation in the internet of behavior. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, pages 874–881.

Bangui, H., Ge, M., and Buhnova, B. (2023b). Deep-learning based reputation model for indirect trust management. *Procedia Computer Science*, 220:405–412.

Bao, F. and Chen, I.-R. (2012a). Dynamic trust management for internet of things applications. In *Proceedings of the 2012 international workshop on Self-aware internet of things*, pages 1–6.

Bao, F. and Chen, R. (2012b). Trust management for the internet of things and its application to service composition. In *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*, pages 1–6. IEEE.

Beer, J. M., Fisk, A. D., and Rogers, W. A. (2014). Toward a framework for levels of robot autonomy in human-robot interaction. *Journal of human-robot interaction*, 3(2):74.

Berger, C., Eichhammer, P., Reiser, H. P., Domaschka, J., Hauck, F. J., and Habiger, G. (2021). A survey on resilience in the iot: Taxonomy, classification, and discussion of resilience mechanisms. *ACM Computing Surveys (CSUR)*, 54(7):1–39.

Bo, Z., Huan, Z., Meizi, L., Qin, Z., and Jifeng, H. (2017). Trust traversal: a trust link detection scheme in social network. *Computer Networks*, 120:105–125.

Buhnova, B. (2023). Trust management in the internet of everything. In *Software Architecture. ECSA 2022 Tracks and Workshops*, pages 123–137, Cham. Springer International Publishing.

Buhnova, B., Halasz, D., Iqbal, D., and Bangui, H. (2023). Survey on trust in software engineering for autonomous dynamic ecosystems. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, pages 1490–1497.

Caminha, J., Perkusich, A., and Perkusich, M. (2018). A smart trust management method to detect on-off attacks in the internet of things. *Security and Communication Networks*, 2018.

Capilla, R., Cioroaica, E., Buhnova, B., and Bosch, J. (2021). On autonomous dynamic software ecosystems. *IEEE Transactions on Engineering Management*, 69(6):3633–3647.

Chahal, R. K., Kumar, N., and Batra, S. (2020). Trust management in social internet of things: A taxonomy, open issues, and challenges. *Computer Communications*, 150:13–46.

Chen, R., Bao, F., and Guo, J. (2015). Trust-based service management for social internet of things systems. *IEEE transactions on dependable and secure computing*, 13(6):684–696.

Chen, R., Guo, J., and Bao, F. (2014). Trust management for soa-based iot and its application to service composition. *IEEE Transactions on Services Computing*, 9(3):482–495.

Clarke, S., Christianson, B., and Xiao, H. (2013). Trust*: Using local guarantees to extend the reach of trust. In *Security Protocols XVII: 17th International Workshop, Cambridge, UK, April 1-3, 2009. Revised Selected Papers 17*, pages 171–178. Springer.

Etalle, S., den Hartog, J., and Marsh, S. (2007). Trust and punishment. In *1st International ICST Conference on Autonomic Computing and Communication Systems*.

Gerber, A. and Kansal, S. (2020). Simplify the development of your iot solutions with iot architectures. IBM. Accessed online: 6 December 2023. Available from: https://developer.ibm.com/articles/iot-lp201-iot-architectures/.

Ghafari, S. M., Beheshti, A., Joshi, A., Paris, C., Mahmood, A., Yakhchi, S., and Orgun, M. A. (2020). A survey on trust prediction in online social networks. *IEEE Access*, 8:144292–144309.

Guo, L., Yang, H., Luan, K., Luo, Y., Sun, L., and Zheng, X. (2021). A trust management model based on mutual trust and a reward-with-punishment mechanism for cloud environments. *Concurrency and Computation: Practice and Experience*, 33(16):e6283.

Gwak, B., Son, H., Kang, J., and Lee, D. (2017). Iot trust estimation in an unknown place using the opinions of i-sharing friends. In *2017 IEEE Trustcom/BigDataSE/ICESS*, pages 602–609. IEEE.

Halasz, D. and Buhnova, B. (2022). Rethinking safety in autonomous ecosystems. In *IEEE 17th Conference on Computer Science and Intelligence Systems*, pages 81–87.

Hategekimana, F., Whitaker, T. J., Pantho, M. J. H., and Bobda, C. (2020). Iot device security through dynamic hardware isolation with cloud-based update. *Journal of Systems Architecture*, 109:101827.

He, Y., Han, G., Jiang, J., Wang, H., and Martinez-Garcia, M. (2020). A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks. *IEEE Transactions on Mobile Computing*, 21(3):811–821.

Hou, F. and Jansen, S. (2023). A systematic literature review on trust in the software ecosystem. *Empirical Software Engineering*, 28(1):8.

Illi, E., Qaraqe, M., Althunibat, S., Alhasanat, A., Alsafasfeh, M., de Ree, M., Mantas, G., Rodriguez, J., Aman, W., and Al-Kuwari, S. (2023). Physical layer security for authentication, confidentiality, and malicious node detection: a paradigm shift in securing iot networks. *IEEE Communications Surveys & Tutorials*.

Iqbal, D. and Buhnova, B. (2022). Model-based approach for building trust in autonomous drones through digital twins. In *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 656–662. IEEE.

Jafarian, B., Yazdani, N., and Haghighi, M. S. (2020). Discrimination-aware trust management for social internet of things. *Computer Networks*, 178:107254.

Jøsang, A., Ismail, R., and Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision support systems*, 43(2):618–644.

Kamvar, S. D., Schlosser, M. T., and Garcia-Molina, H. (2003). The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th international conference on World Wide Web*, pages 640–651.

Karthik, N. and Ananthanarayana, V. (2017). A hybrid trust management scheme for wireless sensor networks. *Wireless Personal Communications*, 97:5137–5170.

Katina, P. F. and Keating, C. B. (2018). Cyber-physical systems governance: a framework for (meta) cybersecurity design. *Security by Design: Innovative Perspectives on Complex Problems*, pages 137–169.

Katina, P. F., Keating, C. B., Gheorghe, A. V., and Masera, M. (2017). Complex system governance for critical cyber-physical systems. *International Journal of Critical Infrastructures*, 13(2-3):168–183.

Khan, M. S., Midi, D., Khan, M. I., and Bertino, E. (2015). Adaptive trust update frequency in manets. In *2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS)*, pages 132–139. IEEE.

Khan, W. Z., Hakak, S., Khan, M. K., et al. (2020). Trust management in social internet of things: Architectures, recent advancements, and future challenges. *IEEE Internet of Things Journal*, 8(10):7768–7788.

Khatun, M. A., Chowdhury, N., and Uddin, M. N. (2019). Malicious nodes detection based on artificial neural network in iot environments. In *2019 22nd International Conference on Computer and Information Technology (ICCIT)*, pages 1–6. IEEE.

Kökciyan, N. and Yolum, P. (2020). Turp: Managing trust for regulating privacy in internet of things. *IEEE Internet Computing*, 24(6):9–16.

Li, B., Ye, R., Gu, G., Liang, R., Liu, W., and Cai, K. (2020). A detection mechanism on malicious nodes in iot. *Computer Communications*, 151:51–59.

Liu, L., Ma, Z., and Meng, W. (2019). Detection of multiple-mix-attack malicious nodes using perceptron-based trust in iot networks. *Future generation computer systems*, 101:865–879.

Liu, Z., Yang, D.-s., Wen, D., Zhang, W.-m., and Mao, W. (2011). Cyber-physical-social systems for command and control. *IEEE Intelligent Systems*, 26(4):92–96.

Lochner, M. and Smilek, D. (2023). The uncertain advisor: trust, accuracy, and self-correction in an automated decision support system. *Cognitive Processing*, 24(1):95–106.

Magdich, R., Jemal, H., Nakti, C., and Ayed, M. B. (2021). An efficient trust related attack detection model based on machine learning for social internet of things. In *2021 International Wireless Communications and Mobile Computing (IWCMC)*, pages 1465–1470. IEEE.

Mahmood, A., Butler, B., Zhang, W. E., Sheng, Q. Z., and Siddiqui, S. A. (2019). A hybrid trust management heuristic for vanets. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 748–752. IEEE.

Malik, S., Dedeoglu, V., Kanhere, S. S., and Jurdak, R. (2019). Trustchain: Trust management in blockchain and iot supported supply chains. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 184–193. IEEE.

Marche, C. and Nitti, M. (2020). Trust-related attacks and their detection: A trust management model for the social iot. *IEEE Transactions on Network and Service Management*, 18(3):3297–3308.

Masmoudi, M., Abdelghani, W., Amous, I., and Sèdes, F. (2020). Deep learning for trust-related attacks detection in social internet of things. In *Advances in E-Business Engineering for Ubiquitous Computing: Proceedings of the 16th International Conference on e-Business Engineering (ICEBE 2019)*, pages 389–404. Springer.

Mechanic, D. (1996). The logic and limits of trust. *Contemporary Sociology*, 25(4):455.

Meena Kowshalya, A. and Valarmathi, M. (2017). Trust management for reliable decision making among social objects in the social internet of things. *IET Networks*, 6(4):75–80.

Mehdizadeh, N. and Farzaneh, N. (2022). An evidence theory based approach in detecting malicious controller in the multi-controller software-defined internet of things network. *Adhoc & Sensor Wireless Networks*, 51(4).

Mendoza, C. V. and Kleinschmidt, J. H. (2015). Mitigating on-off attacks in the internet of things using a distributed trust management scheme. *International Journal of Distributed Sensor Networks*, 11(11):859731.

Muzammal, S. M., Murugesan, R. K., and Jhanjhi, N. Z. (2020). A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches. *IEEE Internet of Things Journal*, 8(6):4186–4210.

Namal, S., Gamaarachchi, H., MyoungLee, G., and Um, T.-W. (2015). Autonomic trust management in cloud-based and highly dynamic iot applications. In *2015 ITU Kaleidoscope: Trust in the Information Society (K-2015)*, pages 1–8. IEEE.

Nandhini, P., Kuppuswami, S., Malliga, S., and DeviPriya, R. (2022). A lightweight energy-efficient algorithm for mitigation and isolation of internal rank attackers in rpl based internet of things. *Computer Networks*, 218:109391.

Nitti, M., Girau, R., and Atzori, L. (2013). Trustworthiness management in the social internet of things. *IEEE Transactions on knowledge and data engineering*, 26(5):1253–1266.

Nwebonyi, F. N., Martins, R., and Correia, M. E. (2019). Security and fairness in iot based e-health system: A case study of mobile edge-clouds. In *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 318–323. IEEE.

Peng, S., He, J., and Meng, Y. (2008). Reputation-based trust update in network environment. In *2008 International Symposium on Electronic Commerce and Security*, pages 118–123. IEEE.

Rana, K., Singh, A. V., and Vijaya, P. (2022). Recent trust management models for secure iot ecosystem. *International Journal of Intelligent Systems and Applications in Engineering*, 10(1s):23–33.

Resnick, P., Kuwabara, K., Zeckhauser, R., and Friedman, E. (2000). Reputation systems. *Communications of the ACM*, 43(12):45–48.

Rizvi, S., Kurtz, A., Pfeffer, J., and Rizvi, M. (2018). Securing the internet of things (iot): A security taxonomy for iot. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 163–168. IEEE.

Roopa, M., Pattar, S., Buyya, R., Venugopal, K. R., Iyengar, S., and Patnaik, L. (2019). Social internet of things (siot): Foundations, thrust areas, systematic review and future directions. *Computer Communications*, 139:32–57.

Sagar, S., Mahmood, A., Sheng, Q. Z., Pabani, J. K., and Zhang, W. E. (2022). Understanding the trustworthiness management in the social internet of things: a survey. *arXiv preprint arXiv:2202.03624*.

Schreieck, M., Wiesche, M., and Krcmar, H. (2016). Design and governance of platform ecosystems-key concepts and issues for future research. In *Ecis*, volume 16, pages 12–15.

Seshadri, S. S., Rodriguez, D., Subedi, M., Choo, K.-K. R., Ahmed, S., Chen, Q., and Lee, J. (2020). Iotcop: A blockchain-based monitoring framework for detection and isolation of malicious devices in internet-of-things systems. *IEEE Internet of Things Journal*, 8(5):3346–3359.

She, W., Liu, Q., Tian, Z., Chen, J.-S., Wang, B., and Liu, W. (2019). Blockchain trust model for malicious node detection in wireless sensor networks. *IEEE Access*, 7:38947–38956.

Singh, M. and Kim, S. (2018). Trust bit: Reward-based intelligent vehicle commination using blockchain paper. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pages 62–67. IEEE.

Tofangchi, S., Hanelt, A., Marz, D., and Kolbe, L. M. (2021). Handling the efficiency–personalization trade-off in service robotics: A machine-learning approach. *Journal of Management Information Systems*, 38(1):246–276.

Truong, N. B., Um, T.-W., Zhou, B., and Lee, G. M. (2017). From personal experience to global reputation for trust evaluation in the social internet of things. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pages 1–7. IEEE.

Usman, M., Britto, R., Börstler, J., and Mendes, E. (2017). Taxonomies in software engineering: A systematic mapping study and a revised taxonomy development method. *Information and Software Technology*, 85:43–59.

Wang, F. and Wei, Z. (2021). A statistical trust for detecting malicious nodes in iot sensor networks. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 104(8):1084–1087.

Williams, P., Rojas, P., and Bayoumi, M. (2019). Security taxonomy in iot–a survey. In *2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 560–565. IEEE.

Xia, F. and Ma, J. (2011). Building smart communities with cyber-physical systems. In *Proceedings of 1st international symposium on From digital footprints to social and community intelligence*, pages 1–6.

Xiao, H., Sidhu, N., and Christianson, B. (2015). Guarantor and reputation based trust model for social internet of things. In *2015 International wireless communications and mobile computing conference (IWCMC)*, pages 600–605. IEEE.

Xiaoxue, M., Zixian, W., Jing, B., and Fei, L. (2010). Trust model based on rewards and punishment mechanism. In *2010 Second International Workshop on Education Technology and Computer Science*, volume 2, pages 182–185. IEEE.

Yan, Z., Ding, W., Niemi, V., and Vasilakos, A. V. (2016). Two schemes of privacy-preserving trust evaluation. *Future Generation Computer Systems*, 62:175–189.

Yu, Y., Jia, Z., Tao, W., Xue, B., and Lee, C. (2017). An efficient trust evaluation scheme for node behavior detection in the internet of things. *Wireless Personal Communications*, 93:571–587.

Zavvos, E., Gerding, E. H., Yazdanpanah, V., Maple, C., Stein, S., et al. (2021). Privacy and trust in the internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 23(8):10126–10141.

Zhaofeng, M., Lingyun, W., Xiaochang, W., Zhen, W., and Weizhe, Z. (2019). Blockchain-enabled decentralized trust management and secure usage control of iot big data. *IEEE Internet of Things Journal*, 7(5):4000–4015.