Eng Int Syst (2024) 1: 43–51

Engineering
Intelligent Systems

Enabling Trustworthy Collaboration for Sustainable Transformation

Marius Becherer[1,*], Michael Zipperle[1], Omar K. Hussain[1], Frank den Hartog[2], Yu Zhang[1], Elizabeth Chang[3] and Achim Karduck[4]

[1] *School of Business, UNSW Canberra, Canberra, Australia*
[2] *School of Systems & Computing, UNSW Canberra, Canberra, Australia*
[3] *School of Information and Communication Technology, Griffith University, Gold Coast, Australia*
[4] *Faculty of Computer Science, Furtwangen University, Furtwangen, Germany*

As global resource consumption surges, the 'Club of Rome' highlights the risks of unchecked quantitative growth in our constrained world, advocating for a shift to qualitative growth. The Internet of Things (IoT)emerges as a pivotal tool in this transition, exemplified by its transformative impacts to coordinate complex activities efficiently while reducing resource consumption in cities like Barcelona and Singapore already today. However, intricate network challenges such as network control, interoperability, and resource constraints complicate efficient communication in a large-scale IoT network. Concurrently, establishing trust among diverse devices often becomes a paramount concern, hindering expansive collaboration across domains and organisations. In response to these multifaceted challenges, the Social Internet of Things (SIoT) has been introduced to address intricate network challenges issues but also fosters a foundation of trust among devices. Despite, the potential benefits of developing trust in SIoT, one of the key challenges for the innovation adaption remains the determination of trust in continuously evolving and uncertain environments. Therefore, there is a need to understand specific situation and provide fine-grained trust mechanism to address multifaceted requirements and consider prevailing constraints of the environment. In this work, we study the existing literature on trust in the SIoT and present potential use cases of how trustworthy collaboration between devices can help to enable the sustainable transformation. We discuss prevailing trust challenges and introduce a novel research framework for trustworthy collaboration to bridge the gap between theoretical trust research and their real-world applicability in the SIoT landscape. Achieving trustworthy collaboration between devices of various organisations will help to improve the activity orchestration while reducing resource consumption.

Keywords: Social Internet of Things, Trustworthiness, Collaboration, Sustainable Transformation, Trust Management, Trust Mechanism

1. INTRODUCTION

In an era defined by rapid technological advancements and ever-growing resource consumption, the global quest for sustainable solutions has become paramount. The "Club of Rome," a consortium of renowned researchers, in their seminal book "The Limits of Growth", underscored the perilous consequences of pursuing quantitative growth amidst finite resource availability already more than 50 years ago [1]. In essence, they highlighted that the unbridled quest for quantitative growth risks our society and planet, emphasizing the significance of qualitative growth as a sustainable alternative.

Quality growth as a vision, based on Quality Innovations fostered by our Digital Ecosystems, provides a more positive and scalable projection for Social, Economic, and Ecologic Development (SEED). The World Economic Forum in Davos (WEF) had explicitly acknowledged our sustainability crisis by a purely quantitative growth paradigm during its 50th anniversary in 2020 as well. In 2023, the WEF put "collaboration in our fragmented world" on top of the agenda

*Cyber Security Cooperative Research Center, Perth, Australia. Email: m.becherer@adfa.edu.au

for mastering the global challenges. We state here, that without trustworthy collaboration, no sustainable transformation can tape place.

Internet of Things (IoT) stands at the forefront of modern solutions with its potential to interconnect devices that address these sustainability challenges. The IoT has the potential to enhance efficiencies by allowing devices to communicate and interact with other IoT systems to automate routine tasks, orchestrate activities, optimize resource usage and allocation, and streamline improve the quality of processes [2]–[4]. The wide range of connected devices enables to capture of a comprehensive representation of the environment and simplifies the spatial coverage of sensing information. Furthermore, the employment of existing sensing resources, such as smartphones or vehicles, can reduce costs and remove the need to deploy additional sensing equipment.

Leading the IoT revolution, smart cities such as Barcelona and Singapore have already showcased the technology's promise [5], [6]. By leveraging IoT, these cities efficiently manage utilities, monitor air quality, optimize waste management, and even refine traffic systems – collectively enhancing the quality of life, reducing costs, and promoting environmental sustainability. While trustworthy collaboration among devices can be achieved to improve situation awareness for decision-making in real-world applications, the existing state of the IoT suffers from technical and social issues.

From the technical perspective, the IoT provides a collaborative environment among billions of connected devices. With changing network topology, network control overhead incurs in limiting network scalability [7], [8]. Also, the heterogeneous environment of devices with multiple hardware and software suppliers raises interoperability issues to harmonize communications among devices [9], [10]. Furthermore, many devices have resource constraints that prevent computation and communication-intensive tasks [11]. Consequently, new technical approaches have been explored to address these challenges.

Besides the technical challenges of IoT to manage the network topology, there are also social challenges between diverse affiliated IoT devices. Especially in open distributed environments where various devices communicate with each other, there is a trust problem between a service-consuming device and a service-providing device. In other words, how can devices ensure that the requested information is authentic or that requested action toward another device, such as closing a gate, will be conducted?

One promising approach to overcome the above-mentioned technical and social challenges represents the Social Internet of Things, a paradigm that integrates social network paradigms into the IoT [12]. More specifically, devices in the SIoT manage its own network topologies by connecting to other devices using social relationships that are formed based on subjective preferences, such as required services capabilities in a given context.

The promise to improve efficient network navigability to enable trustworthy service composition for complex tasks provides advantages for a socialised device network that is aware of mutual capabilities to fulfill assigned tasks. Another aspect that considers SIoT for future network management is the distributed organisation of the network management, whereas each device manages its social relationship to other devices without relying on a central network manager. Consequently, the concept of trustworthiness can be integrated in the relationship management of each device to ensure the overall network's integrity. Therefore, the resulting SIoT may present a sustainable approach to improve the network navigability of information while ensuring the integrity of the network.

In this paper, we present how SIoT can be a critical enabler for trustworthy collaboration. More specifically, we study conceptual use cases of how SIoT uses the capabilities of socialised devices to find information and orchestrate and delegate tasks in the given environment settings. We identify the unresolved challenges in current trust recommendation research and introduce a research framework that bridges the gap between existing trust recommendation research and their practical real-world application. We focus in this paper on the device-to-device interaction, but also device-to-user interactions have been considered [13]. The subsequent sections are structured as follows: Section II reviews related work, offering context and drawing parallels with our study. Section III outlines potential use-case scenarios that highlight SIoT's capabilities and we discusses the potential and challenges of trustworthy collaboration within SIoT in Section IV. Subsequently, we introduce our innovative research framework designed to address these existing trust issues in Section II. Finally, we conclude this paper and summarizing our findings in Section VI.

2. RELATED WORK

The concept of social-based network management has been explored in literature for an extended period [14], [15]. Subsequently, the term "Social Internet of Things" emerged, detailing methods for establishing social relationships between devices using attribute-based approaches, such as proximity-based social relationships [12]. Further attribute-based relationships have also been recognized [16].

While initial effort has been focusing on exploring social relationships and the SIoT architecture, trust management has been identified as an area for research to ensure the network's integrity [17], [18]. Existing methods explored network-based performance metrics, such as throughput or bandwidth usage, from the social devices network to establish new relationships by applying a threshold to classify the trustworthiness [19]. Trust input features can be deviated from the context-dependent device attributes, previous interactions, or the network that can be categorized into social and physical network-based features (Link ontology). The vast majority of trust model reuses experiences from previous interactions to establish social relationships. Hence, robustness has been considered to safeguard trust mechanism against uncertainties and malicious behaviours. Incorporating techniques like Markov chains with exponential smoothing [20] and confidence functions [21] can distinguish between node performance and recommendation quality. Recent advancements include metrics like the degree of importance and contribution [22] and leveraging deep learning for trust

predictions [23]. The existing research has also proposed proactive approaches to target trust-related attacks. The array of methodologies to address trust-related attacks ranges from Dirichlet-based distributions [24] to clustering techniques such as k-means [24]–[26] and multi-layer perceptrons [27]. Enhancing robustness against malicious activities is further fortified by the deployment of witness nodes [28] and fuzzy classification techniques [29].

More research focused on improving the accuracy of trust evaluations by prioritizing contextual multi-scale models [21] and weight transitions [30], [31]. Also, filtering methods have been applied that vary from time-based [26] to interest-based evaluation techniques [31], [32] to amplify the trust evaluation's accuracy.

The decision-making process of trustworthiness encompasses methods such as threshold-based evaluations, consolidating trust impressions into a singular score [26], and ranking-based methodologies [33], [34]. To improve the trust lifecycle based on trust decision, different techniques, such as Markov chains has been used to identify honest clusters [35]. Concurrently, trust convergence mechanisms like sliding windows [25], [33], [36] and trust decay strategies [22], [27], [37]–[39] maintain timeliness of trust scores. Also, reward and punish feedback functions are incorporated to maintain correct trust scores [21], [22], [40]. The addition of reputation scores enriches subjective trust experiences [41].

More research has considered the dynamic environment that causes uncertainties of the number of available devices, the correctness of trust input features, or the completeness of the information. To verify the correctness of data, various methods like Bayes risk [42], evidence-based subjective logic [43], and Dempster-Shafer Theory [44] have been applied. Complementary techniques, including fuzzy logic [45] and adaptive trust parameters [25], cater to the nuanced incomplete trust input features nature of trust recommendations.

Especially scenarios with a limited amount of devices and absence of existing previous interaction experiences are considered for the problem of the initial trust bootstrapping stage. The proposed methods span from feature-property matches [22], [46] to kernel-based predictions [45] and deep learning strategies [23], [47].

The absence of interaction experiences can also be addressed by considering trust inference approaches. Various methods establish similarity metrics, such as distance-based, key-based, or node-based. Popular methods include distance-based contextual similarity with attribute-based filtering [28], [48] and collaborative filtering [39]. Key-based similarity approaches of social relationships have been discussed to consider similar subgraphs [16], [22]. Node-based properties have been considered to identify nodes with similar properties, such as their interest and capabilities [31], [32]. Also, hybrid filtering approaches that consider content- and collaborative filtering have been considered [49]. Besides trust inference approaches for trust recommendation of trust artifacts, a multi multi-objective approach using Pareto optimal solution mechanisms provides trustworthiness across domains [50].

Existing literature partially addresses data-dependent issues, such as the uncertainty of the information environment and the scenario-specific nature of trust models. Additionally, there are recommendation-dependent challenges, including the lack of situation-awareness in trust model adaptation and insufficient trust inference methods to tackle information sparsity. As a result, existing research has studied various aspects of trust recommendations in SIoT, however, existing research lacks an inter-contextual, domain-independent trust recommendation scheme that is able to fulfill various application requirements in multiple situation settings. Hence, we demonstrate the usefulness of leveraging the notion of a socialised device network in our proposed use case scenarios to identify existing shortcomings trust research in SIoT.

3. USE CASE SCENARIOS

The SIoT presents the transformative potential for various applications, particularly in contexts where real-time decision-making and interconnected device communication are pivotal. Two standout applications that underscore the capabilities of SIoT are in the realms of emergency response and traffic light prioritisation requests. The reason for those applications lies in their natural challenges including multi-dimensional device heterogeneity, dynamicity of devices, the interdependence of application scenarios, incompleteness of information, and uncertain environment settings – all inherent complexities in IoT environments. In the subsequent subsections, we delve into these specific use case scenarios, elaborating on how SIoT can be a game-changer in both instances.

3.1 Emergency Response

One of the promising applications of SIoT lies in its potential to transform emergency response systems, an idea well-discussed in existing literature reference. Currently, as documented in the Cocom report [51] and [52], many countries grapple with false emergency calls. These false alarms can exhaust the limited resources of emergency services and jeopardize the delivery of medical aid to genuine emergencies, consequently putting human lives at risk.

In this context, the importance of verifying the authenticity of an emergency call becomes paramount, with SIoT providing an innovative solution to optimise resource allocation. The underlying principle is to leverage the collaborative nature of SIoT to allow surrounding devices to sense their environment, thereby assessing the authenticity of the reported emergency. Trustworthiness comes into play when these devices share the sensed data; each device is assigned a trust score based on factors like its proximity to the incident, the type of data it provides, and past reliability. Therefore, the system can compute a trustworthiness score for each data input, contributing to the decision-making process in validating an emergency call.

Consider a scenario in which a car accident has been reported. Surrounding devices such as traffic cameras, smartphones of bystanders, and nearby vehicles equipped with IoT sensors can provide crucial data for assessing the situation. Traffic cameras can provide real-time visuals of the incident, while smartphone microphones can pick up

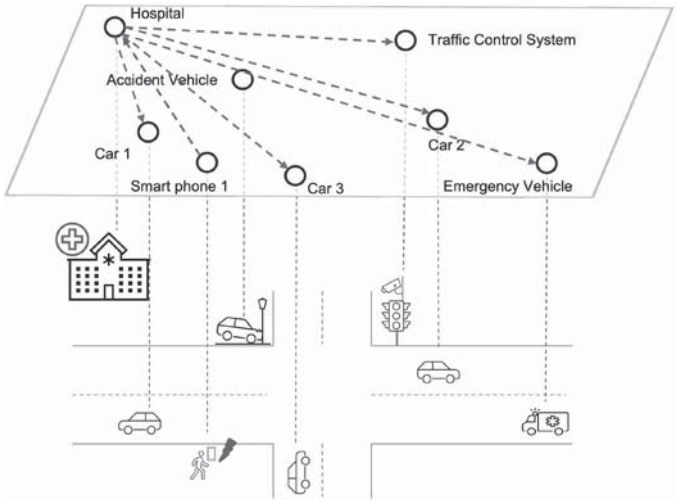

Figure 1 Conceptual model of the emergency response system operation to verify the authenticity of an emergency call

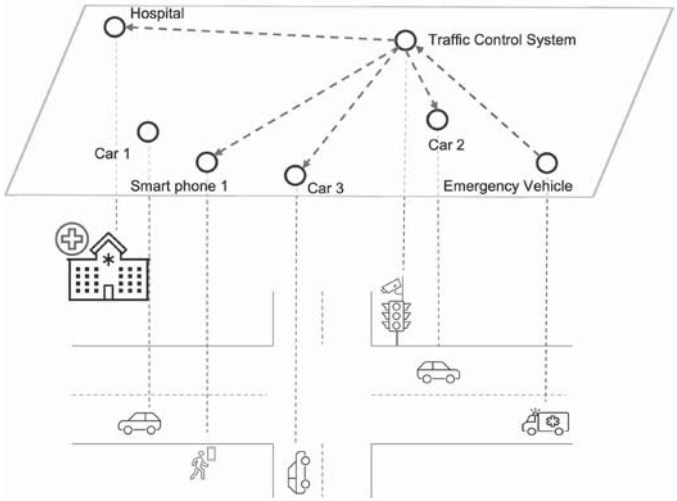

Figure 2 Conceptual model of an Intelligent Traffic Management System to verify the authenticity of an emergency vehicle

sound signatures indicative of a collision. Simultaneously, vehicle sensors can relay information on sudden decelerations or changes in direction, corroborating the reported accident. This aggregation of data from various trusted sources enables the SIoT system to determine the authenticity of the emergency, thereby improving the efficiency of emergency response.

In Figure 1, the model presents a detailed visual representation of an SIoT-based emergency response system. Starting from the initial emergency call to the data collection from various devices and finally to the decision-making process at the emergency centre, the sequence elucidates the role of trustworthiness in improving emergency response operations.

The SIoT, equipped with trustworthiness features, therefore, provides a robust system that not only reduces the misallocation of resources due to false alarms but also ensures a quick response to genuine emergencies by validating their authenticity in real-time. The inclusion of trustworthiness in SIoT applications like emergency response services underscores its transformative potential, thereby paving the way for a more effective, reliable, and responsive IoT environment.

3.2 Intelligent Traffic Light Management

Intelligent traffic light management, a notable smart city application, is recognized in the literature for its potential to alleviate traffic congestion [53]. By optimizing traffic flow, not only reduces travel times for all road users but also ensures priority passage for crucial vehicles such as emergency services.

Traffic light scheduling is a powerful tool that can be adapted based on real-time traffic situations. Yet, it necessitates fine-grained situational awareness and identifying authentic emergency vehicles amidst normal traffic. This task is complex due to potential trust breaches, such as non-emergency vehicles masquerading as emergency vehicles or misusing emergency privileges.

As shown in Figure 2, the scenario begins with an emergency vehicle requesting priority at an upcoming intersection. The traffic light management system then gathers information from surrounding devices to verify the authenticity of the request. While external sensors are useful in vehicle identification, task context from the emergency response system plays a crucial role in evaluating the request's legitimacy.

In an urban landscape replete with various sensing devices and online services, traffic cameras, vehicle IoT sensors, traffic sensors, and accident reports from the emergency response centre can provide valuable data. By utilizing this information, the system assesses the authenticity of (1) the emergency vehicle, (2) the reported emergency, and (3) the selected route towards the emergency.

Based on the results of these assessments, the traffic light management system modifies its scheduling strategy and communicates its decision to the emergency vehicle. This ensures that only authenticated requests gain priority, aiding in more effective emergency responses.

4. DISCUSSION

Building upon the two use case scenarios, this subsection aims to elucidate the profound potential inherent in Trustworthy Collaboration within the SIoT framework, while concurrently addressing the multifaceted challenges that emerge therein.

4.1 Potential of Trustworthy Collaboration in SIoT

Trustworthy collaboration is vital for coordinating activities across devices, people, and systems in diverse situations. This trust is essential for seamless interactions in various contexts. The SIoT revolutionizes traditional crisis management, especially in emergencies. Historically hindered by communication gaps and disjointed systems, SIoT enables devices to communicate on-the-fly, leveraging social connections to enhance network navigability. For instance, SIoT can pinpoint fire safety tools or provide real-time traffic accident data in emergencies, underscoring its potential when devices collaborate based on trust.

This collaborative value extends to sectors like transportation. With the advent of autonomous driving, real-time data sharing becomes crucial to prevent accidents and streamline traffic. Trust between devices facilitates cooperative scenarios, such as intersections working harmoniously with vehicles, promoting smoother operations and sustainability.

Incorporating trust in SIoT transforms device communication, marking a shift from isolated to socially-connected devices. This collaboration boosts efficiency in sectors like healthcare and transportation and fosters sustainability by reducing redundancies and conserving resources. SIoT's collaborative environment ensures community safety and resilience. Embedding trust in SIoT paves the way for a more unified, efficient, and green future.

4.2 Challenges of Trustworthy Collaboration in SIoT

However, the idea of Trustworthy Collaboration within the SIoT environment brings forth a unique set of challenges. These challenges arise from the distinct characteristics of IoT devices, their data interactions, intricacies in trust-based decision-making, and inherent methodological complexities. For instance, the SIoT network's dynamic nature, where devices frequently join and leave, creates an unstable environment that complicates trust establishment and management. The diversity of devices in terms of functionality, capability, and manufacturing leads to varied communication standards, posing integration and trust assessment challenges. As the number of interconnected devices grows, managing trust relationships becomes increasingly complex, demanding scalable solutions. Consequently, the design of an inter-contextual, domain-independent trust mechanism becomes complicated by the fundamental constraints of IoT environments.

More specifically, SIoT can suffer from spatiotemporal data relationships, whereas the recorded information is only valid at a certain location and time. Furthermore, the dynamic nature of the IoT network topology causes uncertainty that complicates designing a trust mechanism. In contrast, the incompleteness of information varies presented by previous interaction experiences, previously trusted devices, and the absence of required context-dependent features. As a consequence, guaranteeing data integrity and completeness presents one of the critical challenges for trustworthy collaboration.

Another aspect to consider presents trust recommendations that require suffering from the previously mentioned dynamic and complex nature of SIoT. Understanding an existing situation poses another challenge to adapt the trust model according to the given situation. Additionally, the trust lifecycle between devices remains challenging as devices may be trustworthy but will only sometimes interact due to spontaneous encounters on the highway. Also, devices may offer various services and functionality, whereas trustworthiness between individual functions can differ. All these factors must be considered to manage trust between devices sustainably.

Lastly, existing research evaluates the proposed trust mechanisms based on individual experiments, whereas benchmarking trust mechanisms in various situations becomes challenging. More specifically, existing experiments need to sufficiently consider device diversity, various situations, potential adversarial models, and interdependencies between different scenarios.

To address these challenges, a multidisciplinary approach is essential, combining insights from trust computing, knowledge engineering, and distributed systems. Overcoming these challenges is vital to harness the full potential for trustworthy collaboration in SIoT, paving the way for a more effective, efficient, and secure IoT ecosystem.

5. PROPOSED RESEARCH FRAMEWORK FOR TRUSTWORTHY COLLABORATION

The proposed research framework introduces a situationaware trust middleware meticulously designed to enable trustworthy collaboration in various situations that reuses concepts from [54] to achieve semantic interoperability. This multilayered architecture provides a holistic approach, from establishing physical links between devices to ensuring that trust is established in the socially aware trust network layer. The

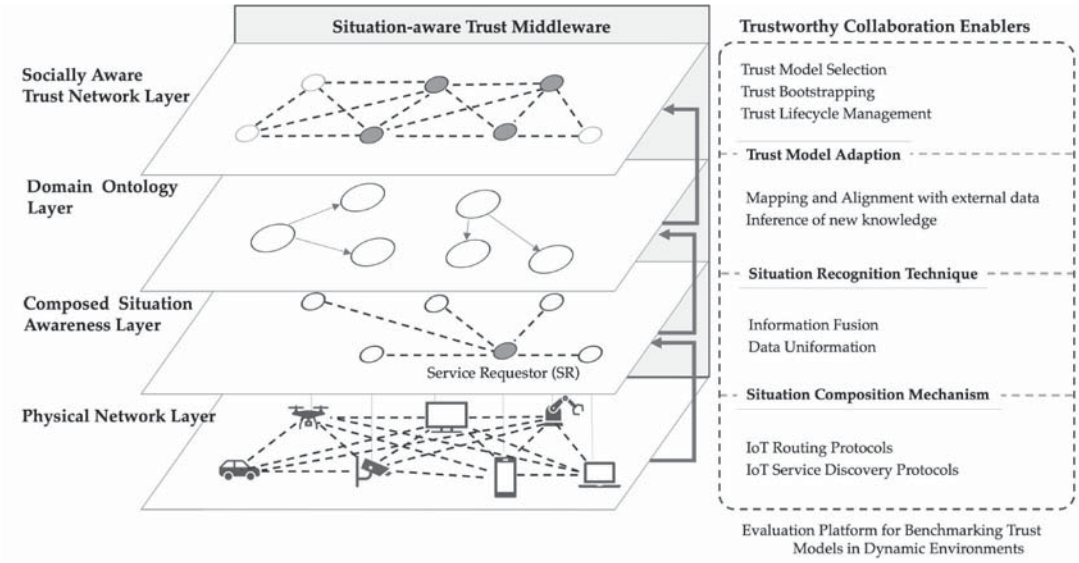

Figure 3 Proposed Trust Research Framework for Trustworthy Collaboration.

proposed research framework is illustrated in Figure 3. The proposed research framework is subdivided into four layers: the physical network layer, the composed situation awareness layer, the domain ontology layer, and the socially aware trust network layer. Hereby, the integration between two layers is ensured by trustworthy collaboration enablers are described subsequently.

This foundational physical network layer enables the connection between devices. By employing existing IoT Routing Protocols, devices can discover and communicate with one another, setting the stage for more complex interactions. While existing protocols perform adequately in static environments, the dynamic nature and the multi-dimensional requirements complexity of SIoT applications requires innovative approaches to deal with fluctuating Quality-of-Service requirements and consider future applications to address the rapid increase in traffic demand [55].

Transitioning from the physical layer, the Situation Composition Mechanism requires novel service discovery protocols to identify devices based on contextual features, such as location. This mechanism ensures that only relevant devices are considered in subsequent layers. Although some mechanisms can identify devices based on proximity, the increasing density of IoT devices in urban environments necessitates more granular, situation-aware methodologies [56]. Further service discovery methods may explore dynamic and adaptable multi-criteria service discovery approaches that can consider the various and changing requirements of future applications.

Upon identifying the relevant devices, the composed situation awareness layer focuses on creating a comprehensive understanding of the situation. Through data pre-processing for features extraction, data uniformation and information fusion techniques, diverse data streams are merged, offering a holistic view of the current context. While there are established methods for individual data uniformation, the fusion of trust-dependent input features has not been addressed [13]. Therefore, ontologies for IoT domain can be used and enriched for SIoT environments.

The situation recognition technique exploits the provided information fusion of the combined situation awareness layer. The situation recognition method helps to identify suitable domain ontologies that will be used to adapt trust models to enable a situation-responsive trust recommendation. Furthermore, situation recognition enables inference approaches of interaction experiences of other devices in similar situations.

The recognition of various situations enables the usage of the domain ontology layer and acts as a bridge, interfacing the raw data with abstracted knowledge. Hereby, the mapping and alignment with external data is facilitated to infer missing knowledge gaps of potential trust input features. Furthermore, this layer is vital to provide trust model configuration settings. More specifically, each domain may have relevant features and defined criteria represented as trust indicators to measure trust against domain-dependent criteria. The provided information may contain features selection, features mapping tables, trust decision-based threshold parameters, features weights and trust indicators to improve trust recommendation in various situations.

To acknowledge that trust is not static rather than evolving based on a given situation requires trust model adaption mechanisms to tune the trust model. The trust model adaption mechanism adapts trust models based on the recognized situation by leveraging the domain ontology's insights, historical data, and context-dependent input features.

Consequently, a socially aware trust network layer can be established to represent the trust between devices. In this context, 'socially' refers to the mutual interests and preferences of devices that form the foundations of the SIoT paradigm to establish social relationships based on similar objectives. To specify the underlying social relationships, trust represents the strength and quality of relationships formed based on these interests. This layer operates various trustrelated operations, such as selecting appropriate trust model, bootstrap trust relationships, and managing the trust lifecycle between devices within the network.

Additionally, an evaluation platform for benchmarking trust models in dynamic environments is needed to stress-test trust

models in various situations and ensure resilience against adversary behaviour and accuracy in real-world applications. The benchmarking evaluation platform will be crucial to enable a comparative analysis of various trust models to evaluate the performance in various domains.

6. CONCLUSION

In this study, we investigated the domain of trust research within the Social Internet of Things (SIoT) as a potential enabler for trustworthy collaboration. We discussed findings from the existing literature to offer a synthesis of current understandings and knowledge gaps in this evolving field. Additionally, practical use case scenarios are presented to underscore the imperative nature of trustworthy collaboration in real-world applications, emphasizing its tangible impact on real-world activities and resource orchestration. Furthermore, this work outlines the intricacies of conceptualizing and actualizing an inter-contextual and domain-independent trust mechanism. While the potential of such a mechanism is vast, spanning improved interoperability, enhanced security, and optimized collaborations, the challenges are equally challenging. The intricacies of bridging diverse domains, ensuring seamless transitions across varying contexts, and managing trust dynamics in multifaceted environments are presented. Consequently, we propose a research framework to guide future research to enable inter-contextual and domain-independent SIoT trust mechanisms. More specifically, we layer our research framework into a physical network layer, composed situation awareness layer, domain ontology layer, and socially aware trust network layer. We highlighted the purpose of each layer and presented how we anticipate transiting between the presented layers. We also call for an evaluation benchmarking platform to evaluate trust mechanisms in SIoT that respect the real-world dynamics of devices. As the landscape of SIoT continues to expand and evolve, the pursuit of trustworthy collaborations remains paramount. We are convinced that with rigorous research, robust frameworks, and a sharp understanding of challenges and potentials, the SIoT community can guide us in a new era of secure, efficient, and trustworthy interactions.

ACKNOWLEDGMENT

The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

REFERENCES

1. D. H. Meadows, D. L. Meadows, J. Randers, and W. W. Behrens III, "The limits to growth," 1972.
2. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013, ISSN: 0167739X. DOI: 10.1016/j.future.2013.01.010.
3. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, ISSN: 1553877X. DOI: 10.1109/COMST.2015.2444095.
4. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010, ISSN: 13891286. DOI: 10.1016/j.comnet.2010.05.010.
5. J. Vodák, D. Šulyová, and M. Kubina, "Advanced technologies and their use in smart city management," *Sustainability (Switzerland)*, vol. 13, no. 10, 2021, ISSN: 20711050. DOI: 10.3390/su13105746.
6. J. M. Hernández-Muñoz, J. B. Vercher, L. Muñoz, *et al.*, "Smart cities at the forefront of the future internet," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6656, pp. 447–462, 2011, ISSN: 03029743. DOI: 10.1007/978-3-642-20898-0{_}32.
7. R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, pp. 51–58, Sep. 2011, ISSN: 0018-9162. DOI: 10.1109/MC.2011.291.
8. J. Guo, I.-R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications*, vol. 97, pp. 1–14, Jan. 2017, ISSN: 01403664. DOI: 10.1016/j.comcom.2016.10.012.
9. V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Sahafi, "Trust-based recommendation systems in Internet of Things: a systematic literature review," *Human-centric Computing and Information Sciences*, vol. 9, no. 1, p. 21, Dec. 2019, ISSN: 2192-1962. DOI: 10.1186/s13673-019-0183-8.
10. L. Daniele, M. Solanki, F. den Hartog, and J. Roes, "Interoperability for Smart Appliances in the IoT World," in *The Semantic Web – ISWC 2016*, P. Groth, E. Simperl, A. Gray, *et al.*, Eds., vol. 9982, Cham: Springer International Publishing, 2016, pp. 21–29. DOI: 10.1007/978-3-319-46547-0{_}3.
11. Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014, ISSN: 10958592. DOI: 10.1016/j.jnca.2014.01.014.
12. L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a social structure to the internet of things," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193–1195, 2011, ISSN: 10897798. DOI: 10.1109/LCOMM.2011.090911.111340.
13. R. M.S., S. Pattar, R. Buyya, V. K.R., S. Iyengar, and L. Patnaik, "Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions," *Computer Communications*, vol. 139, no. March, pp. 32–57, May 2019, ISSN: 01403664. DOI: 10.1016/j.comcom.2019.03.009.
14. M. Kranz, L. Roalter, and F. Michahelles, "Things That Twitter: Social Networks and the Internet of Things," in *International Conference on Pervasive Computing*, 2010.
15. L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H.-W. Gellersen, "Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts," in *Proceedings of the 3rd International Conference on Ubiquitous Computing*, ser. UbiComp '01, Berlin, Heidelberg: Springer-Verlag, 2001, 116–122, ISBN: 3540426140. DOI: 10.5555/647987.741340.
16. U. S. Premarathne, "MAG-SIoT: A multiplicative attributes graph model based trust computation method for social Internet of Things," in *2017 IEEE International Conference on Industrial and Information Systems (ICIIS)*, Peradeniya: IEEE, Dec. 2017, pp. 1–6, ISBN: 978-1-5386-1674-1. DOI: 10.1109/ICIINFS.2017.8300344.

17. M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of Things," in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, Sydney: IEEE, Sep. 2012, pp. 18–23, ISBN: 978-1-4673-2569-1. DOI: 10.1109/PIMRC.2012.6362662.
18. Fenye Bao and Ing-Ray Chen, "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)*, San Francisco: IEEE, Jun. 2012, pp. 1–6, ISBN: 978-1-4673-1239-4. DOI: 10.1109/WoWMoM.2012.6263792.
19. M. Nitti, R. Girau, and L. Atzori, "Trustworthiness Management in the Social Internet of Things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266, May 2014, ISSN: 1041–4347. DOI: 10.1109/TKDE.2013.105.
20. E. K. Wang, C. M. Chen, D. Zhao, W. H. Ip, and K. L. Yung, "A dynamic trust model in internet of things," *Soft Computing*, vol. 24, no. 8, pp. 5773–5782, 2020, ISSN: 14337479. DOI: 10.1007/s00500-019-04319-2.
21. S. E. A. Rafey, A. Abdel-Hamid, and M. A. El-Nasr, "CBSTM-IoT: Context-based social trust model for the Internet of Things," in *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)*, Cairo: IEEE, Apr. 2016, pp. 1–8, ISBN: 978-1-5090-1743-0. DOI: 10.1109/MoWNet.2016.7496623.
22. L. Wei, J. Wu, C. Long, and B. Li, "On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4775–4787, Mar. 2020, ISSN: 2327-4662. DOI: 10.1109/JIOT.2020.3028380.
23. Y. Wen, Z. Xu, R. Zhi, and J. Chen, "Trust Prediction Model Based on Deep Learning in Social Internet of Things," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 346, Cham: Springer International Publishing, 2021, pp. 557–570. DOI: 10.1007/978-3-030-67514-1{_}44.
24. O. Ben Abderrahim, M. H. Elhedhili, and L. Saidane, "DTMS-IoT: A Dirichlet-based trust management system mitigating on-off attacks and dishonest recommendations for the Internet of Things," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir: IEEE, Nov. 2016, pp. 1–8, ISBN: 978-1-5090-4320-0. DOI: 10.1109/AICCSA.2016.7945691.
25. G. Chen, F. Zeng, J. Zhang, T. Lu, J. Shen, and W. Shu, "An adaptive trust model based on recommendation filtering algorithm for the Internet of Things systems," *Computer Networks*, vol. 190, no. February, p. 107 952, May 2021, ISSN: 13891286. DOI: 10.1016/j.comnet.2021.107952.
26. S. Sagar, A. Mahmood, Q. Z. Sheng, and W. E. Zhang, "Trust Computational Heuristic for Social Internet of Things: A Machine Learning-based Approach," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, vol. 2020-June, online: IEEE, Jun. 2020, pp. 1–6, ISBN: 978-1-7281-5089-5. DOI: 10.1109/ICC40277.2020.9148767.
27. A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, A. Mac-Dermott, and X. Wang, "CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5432–5445, Jun. 2019, ISSN: 2327-4662. DOI: 10.1109/JIOT.2019.2902022.
28. Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Computers & Security*, vol. 39, no. PART B, pp. 351–365, Nov. 2013, ISSN: 01674048. DOI: 10.1016/j.cose.2013.09.001.
29. H. Ouechtati, B. A. Nadia, and B. S. Lamjed, "A fuzzy logic-based model for filtering dishonest recommendations in the Social Internet of Things," *Journal of Ambient Intelligence and Humanized Computing*, Mar. 2021, ISSN: 1868-5137. DOI: 10.1007/s12652-021-03127-7.
30. O. Ben Abderrahim, M. H. Elhedhili, and L. Saidane, "CTMS-SIOT: A context-based trust management system for the social Internet of Things," *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017*, pp. 1903–1908, 2017. DOI: 10.1109/IWCMC.2017.7986574.
31. S. Talbi and A. Bouabdallah, "Interest-based trust management scheme for social internet of things," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1129–1140, 2020, ISSN: 18685145. DOI: 10.1007/s12652-019-01256-8.
32. I.-R. Chen, J. Guo, and F. Bao, "Trust management for service composition in SOA-based IoT systems," in *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, Istanbul: IEEE, Apr. 2014, pp. 3444–3449, ISBN: 978-1-4799-3083-8. DOI: 10.1109/WCNC.2014.6953138.
33. U. Jayasinghe, N. B. Truong, G. M. Lee, and T.-W. Um, "RpR: A Trust Computation Model for Social Internet of Things," in *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Toulouse: IEEE, Jul. 2016, pp. 930–937, ISBN: 978-1-5090-2771-2. DOI: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld. 2016.0146.
34. S. Rajendran and R. Jebakumar, "Object Recommendation based Friendship Selection (ORFS) for navigating smarter social objects in SIoT," *Microprocessors and Microsystems*, vol. 80, no. October 2020, p. 103 358, 2021, ISSN: 01419331. DOI: 10.1016/j.micpro.2020.103358.
35. C. Boudagdigue, A. Benslimane, A. Kobbane, and M. Elmachkour, "A Distributed Advanced Analytical Trust Model for IoT," in *2018 IEEE International Conference on Communications (ICC)*, vol. 2018-May, Kansas City: IEEE, May 2018, pp. 1–6, ISBN: 978-1-5386-3180-5. DOI: 10.1109/ICC.2018.8422726.
36. J. Caminha, A. Perkusich, and M. Perkusich, "A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things," *Security and Communication Networks*, vol. 2018, pp. 1–10, 2018, ISSN: 1939-0114. DOI: 10.1155/2018/6063456.
37. W. Fang, W. Zhang, L. Shan, X. Ji, and G. Jia, "DDTMS: Dirichlet-Distribution-Based Trust Management Scheme in Internet of Things," *Electronics*, vol. 8, no. 7, p. 744, Jul. 2019, ISSN: 2079-9292. DOI: 10.3390/electronics8070744.
38. N. B. Truong, T.-W. Um, B. Zhou, and G. M. Lee, "From Personal Experience to Global Reputation for Trust Evaluation in the Social Internet of Things," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, vol. 2018-Janua, Singapore: IEEE, Dec. 2017, pp. 1–7, ISBN: 978-1-5090-5019-2. DOI: 10.1109/GLOCOM.2017.8254523.
39. A. Altaf, H. Abbas, F. Iqbal, F. A. Khan, S. Rubab, and A. Derhab, "Context-oriented trust computation model for industrial Internet of Things," *Computers & Electrical Engineering*, vol. 92, p. 107 123, Jun. 2021, ISSN: 00457906. DOI: 10.1016/j.compeleceng.2021.107123.

40. G. Xu, Y. Zhao, L. Jiao, *et al.*, "TT-SVD: An Efficient Sparse Decision-Making Model With Two-Way Trust Recommendation in the AI-Enabled IoT Systems," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9559–9567, Jun. 2021, ISSN: 2327-4662. DOI: 10.1109/JIOT.2020.3006066.
41. A. U. Rehman, A. Jiang, A. Rehman, and A. Paul, "Weighted Based Trustworthiness Ranking in Social Internet of Things by using Soft Set Theory," in *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, Chengdu: IEEE, Dec. 2019, pp. 1644–1648, ISBN: 978-1-7281-4743-7. DOI: 10.1109/ICCC47050.2019.9064242.
42. A. Kurniawan and M. Kyas, "A trust model-based Bayesian decision theory in large scale Internet of Things," in *2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, Singapore: IEEE, Apr. 2015, pp. 1–5, ISBN: 978-1-4799-8055-0. DOI: 10.1109/ISSNIP.2015.7106964.
43. N. B. Akhuseyinoglu, M. Karimi, M. Abdelhakim, and P. Krishnamurthy, "On Automated Trust Computation in IoT with Multiple Attributes and Subjective Logic," in *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, vol. 2020-Novem, Sydney: IEEE, Nov. 2020, pp. 267–278, ISBN: 978-1-7281-7158-6. DOI: 10.1109/LCN48667.2020.9314808.
44. A. Bhargava and S. Verma, "DEIT: Dempster Shafer Theory-based edge-centric Internet of Things-specific trust model," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, p. 25, Jun. 2021, ISSN: 2161-3915. DOI: 10.1002/ett.4248.
45. H. Xia, F. Xiao, S.-s. Zhang, C.-q. Hu, and X.-z. Cheng, "Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, vol. 2019-April, Paris: IEEE, Apr. 2019, pp. 838–846, ISBN: 978-1-7281-0515-4. DOI: 10.1109/INFOCOM.2019.8737491.
46. Z. Lin and L. Dong, "Clarifying Trust in Social Internet of Things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 2, pp. 234–248, Feb. 2018, ISSN: 1041-4347. DOI: 10.1109/TKDE.2017.2762678.
47. M. Bahutair, A. Bouguettaya, and A. G. Neiat, "Multi-Perspective Trust Management Framework for Crowd-sourced IoT Services," *IEEE Transactions on Services Computing*, vol. 15, no. 4, pp. 2396–2409, Jul. 2022, ISSN: 1939-1374. DOI: 10.1109/TSC.2021.3052219.
48. M. Nitti, V. Pilloni, and D. D. Giusto, "Searching the social Internet of Things by exploiting object similarity," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Reston: IEEE, Dec. 2016, pp. 371–376, ISBN: 978-1-5090-4130-5. DOI: 10.1109/WF-IoT.2016.7845506.
49. A. Khelloufi, H. Ning, S. Dhelim, *et al.*, "A Social-Relationships-Based Service Recommendation System for SIoT Devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1859–1870, Feb. 2021, ISSN: 2327-4662. DOI: 10.1109/JIOT.2020.3016659.
50. X. Wu, "Cross-domain trust management mechanism for internet of things systems," *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 933–947, Mar. 2021, ISSN: 1936-6442. DOI: 10.1007/s12083-021-01071-z.
51. EUROPEAN COMMISSION Directorate-General for Communications Networks Content and Technology, "Implementation of the European emergency number 112 – Results of the ninth data-gathering round," 2016.
52. European Emergency Number Association, "FALSE EMERGENCY CALLS," 2020. [Online]. Available: https://lumalilaresearch.com/2014/05/19/false-emergency/.
53. Z. Chen, R. Ling, C.-M. Huang, and X. Zhu, "A scheme of access service recommendation for the Social Internet of Things," *International Journal of Communication Systems*, vol. 29, no. 4, pp. 694–706, Mar. 2016, ISSN: 10745351. DOI: 10.1002/dac.2930.
54. J. Kim, J. Kong, M. Sohn, and G. Park, "Layered ontology-based multi-sourced information integration for situation awareness," *The Journal of Supercomputing*, vol. 77, no. 9, pp. 9780–9809, Sep. 2021, ISSN: 0920-8542. DOI: 10.1007/s11227-021-03629-3.
55. S. Dilek, K. Irgan, M. Guzel, S. Ozdemir, S. Baydere, and C. Charnsripinyo, "QoS-aware IoT networks and protocols: A comprehensive survey," *International Journal of Communication Systems*, vol. 35, no. 10, pp. 1–38, 2022, ISSN: 10991131. DOI: 10.1002/dac.5156.
56. M. Achir, A. Abdelli, L. Mokdad, and J. Benothman, "Service discovery and selection in IoT: A survey and a taxonomy," *Journal of Network and Computer Applications*, vol. 200, no. January, p. 103 331, 2022, ISSN: 10958592. DOI: 10.1016/j.jnca.2021.103331.