International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 08 Special Issue 01 | 2023

Trust Management in Social Internet of Things (SIoT): A Review

Yogesh B. Jadhao[1]

[1] Padm. Dr. V. B. Kolte College of Engineering, Malkapur

ABSTRACT

A review on trust management in the Social Internet of Things (SIoT) is provided, beginning with a discussion of SIoT architectures and relationships. Using a variety of publication databases, we describe efforts that focus on various trust management aspects of SIoT. Trust management models cover three themes: trust computation, aggregation, and updates. Our review presents a detailed discussion of all three steps. Trust computation and trust aggregation depend upon Trust Attributes (TAs) for the calculation of local and global trust values. Our paper discusses many strategies for aggregating trust, but ``Weighted Sum'' is the most frequently used in the relevant studies. Our paper addresses trust computation and aggregation scenarios. Our work classifies research by TAs (Social Trust, Quality of Service).We've categorized the research (reputation-based, recommendation-based, knowledge-based) depending on the types of feedback/opinions used to calculate trust values (global feedback/opinion, feedback from a friend, trusts own opinion considering the trustee's information). Our work classifies studies (policy-based, prediction based, weighted sum-based/weighted linear combination-based) by trust computation/aggregation approach. Two trust-update schemes are discussed: time-driven and event-driven schemes, while most trust management models utilize an event-driven scheme. Both trust computation and aggregation need propagating trust values in a centralized, decentralized, or semi-centralized way. Our study covers classifying research by trust updates and propagation techniques. Trust models should provide resiliency to SIoT attacks. This analysis classifies SIoT attacks as collaborative or individual. We also discuss scenarios depicted in the relevant studies to incorporate resistance against trust-related attacks in SIoT. Studies suggest context based or context-free trust management strategies. Our study categorizes studies based on context-based or context-free approaches. To gain the benefits of an immutable, privacy-preserving approach, a future trust management system should utilize Block-chain technology to support non-repudiation and tracking of trust relationships.

Keyword: ***- Social Internet of Things, SIoT, trust, architecture, attacks, future direction, application areas, event-driven, time-driven, context-based, trust attributes.***

1. INTRODUCTION

The Internet of Things (IoT) provides a platform to integrate a large number of distributed heterogeneous systems. Ubiquitous computing is the backbone of IoT, indicating a network of uniquely identify able interconnected smart objects using standard communication protocols [2]. These resource-constrained smart devices communicate and collaborate in various contexts. However, IoT is not just a global network of smart devices, but also encompasses a group of supporting technologies along with the necessary services and set of applications [3]. IoT can be seen as a network whose prime objective is to include devices or nodes which can request or provide services. Moreover, nodes can collaborate to provide a single service [4]. Since the inception of IoT, there has been progress in this paradigm at an unprecedented rate resulting in the innovation of many different visions and contexts such as ``Social IoT'' (SIoT), industrial IoT, and IoT in the healthcare domain. User-to-Object Relationships and Object-to-Object Relationships are both possible in a SIoT system, depending on their respective affiliations. Relationship types play a critical role in inter-SIoT communication and the application domain [11]. When ``things'' discover that they have a social nature, they begin to form connections with one another. Based on factors like specifications of entities or nodes, activity patterns, programs installed, services rendered, etc. social links between objects can be constructed [12], [13]. Social relationships in the SIoT can be classified as

- Parent-object relationship: refers to objects or nodes belonging to the same manufacturer [5], [13] i.e., under the same batch. Mostly the nodes owned by the same manufacturer are homogeneous.
- Co-location relationship: this relationship exists between objects belonging to the same location [5], [13]. Objects can be located in the same city or same workplace depending on their physical location.
- Co-work relationship: objects actually cooperate with each other towards a common application/ goal [5], [13] The relationship is established between homogenous or heterogeneous objects.
- Ownership object relationship: present among objects belonging to the same owner. The objects need not be homogeneous [5].

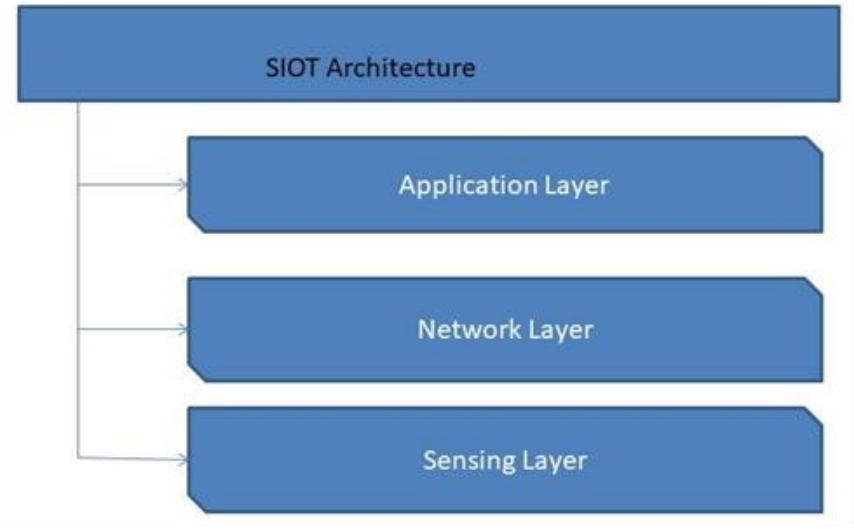

Fig -1: SIOT Architecture

1.1 RELATED WORK

Trust properties and models are presented in reviews [1], however, the associated trust management systems, simulation tools, and components are not described. These reviews do not include challenges, future directions, and potential trust aggregation schemes.
In [1] a limited number of studies are considered, and analysis is based on various performance metrics. These reviews do not cover trust update schemes, trust properties and trust propagation schemes. The surveys [1] describe SIoT trust and ``friendliness" techniques, in which the concept of SIoT is examined for supporting cloud computing, multi agent systems and Industry 4.0. A contrast of various trust and friendliness techniques in SIoT is provided. There is however no discussion of trust management strategies, notably for SIoT. In [1] a holistic perspective of the SIoT domain is provided, including recent research developments in SIoT, such as the discovery of services and their composition, management of relationships between services, and trust management frameworks. Subjective/ objective and dynamic trust management schemes are described, but a contrast of the most recent trust management frameworks/ models in the SIoT domain is not included. Another survey [1] contrasts and evaluates trust management approaches in various fields, including Wireless Sensor Networks (WSN) and the Internet of Things (IoT), followed by a description of various trust management aspects. However, the comparison is not limited to SIoT trust management processes; it also incorporates IoT trust management. The survey [1] presents a comparative evaluation of trust models for SIoT and Online Social Networks (OSN). In [1]
the key components and parameters needed to create a realistic trust model specific to MOOC platforms are described, aimed to provide an appealing learning environment for learners. Trust models are compared based on their architecture, the initial value of trust, trust updates, a trust decay factor, context/ risk, resistance to attack, and scalability. The survey [1] investigates common themes between IoT and SIoT domains; SIoT-related architectures are examined, and SIoT trust management platforms are compared, along with a discussion of future research challenges in SIoT. This work lacks an assessment of trust in SIoT-based applications, SIoT platforms, and potential research challenges in trust assessment for SIoT.

1.2 METHODOLOGY

This section provides the methodological process, as shown in Figure 2, for conducting the literature review. Figure 3 represents the structure of our review.

A. SELECTION OF RELEVANT STUDIES

The query used for the selection of papers is ((``SIoT'' OR ``Social internet of things'') AND (``trust'' OR ``TMS'' OR ``DTMS'')) Where: DTMS distributed trust management schemes; TMS Trust Management Schemes.

B. INCLUSION/EXCLUSION OF RESEARCH STUDIES

1) INCLUSION

Only research articles, over the time period 2012-2022, related to trust management in the domain of SIoT are considered. These research articles are published as journal articles, conference papers or book chapters.

2) EXCLUSION

All other studies not related to trust management aspects of SIoT domain are filtered out. The studies which are not in English and research studies for which full text is not available are excluded.

C. FORMATION OF RESEARCH QUESTIONS

The research questions in Table 1 are for analysis purposes, to comprehend the three general steps of the Trust Management Framework (Sec IV).

D. ABBREVIATIONS WITH FULL FORM

Table 2 contains a list of the abbreviations which is used frequently in the succeeding sections.

2. TRUST MANAGEMENT FRAMEWORK IN SIoT AND FINDINGS

2.1 CONCEPT OF TRUST

Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work A deep belief in the dependability, honesty, sincerity, justice, and good confidence of others to carry out a deal, transaction, commitment, agreement, etc. in line with established principles, norms, laws, expectations, and undertakings is referred to as trust [1]. The concept of trustworthiness can be explained in terms of the relationship among entities in trusting exchanges. Trustworthiness, therefore, depends on the attributes of the trustees in the given context [1].

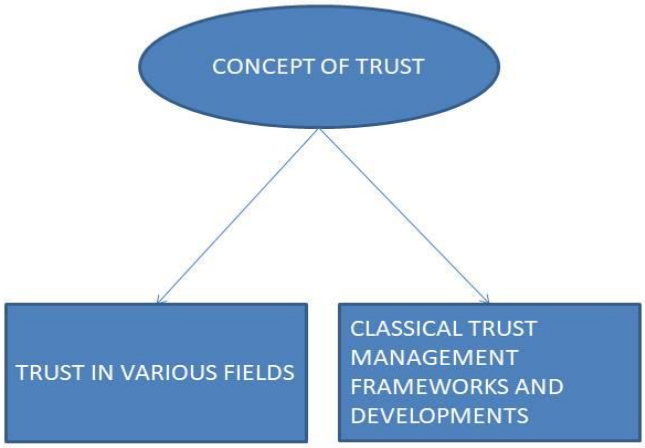

Fig -2: CONCEPT OF TRUST

Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction

2.1 GENERAL STEPS IN TRUST MANAGEMENT FRAMEWORK

The general steps in trust management frameworks are depicted in Figure 4. It is to be noted that trust values are propagated for the computation of global trust / overall trust either in a centralized or decentralized manner.

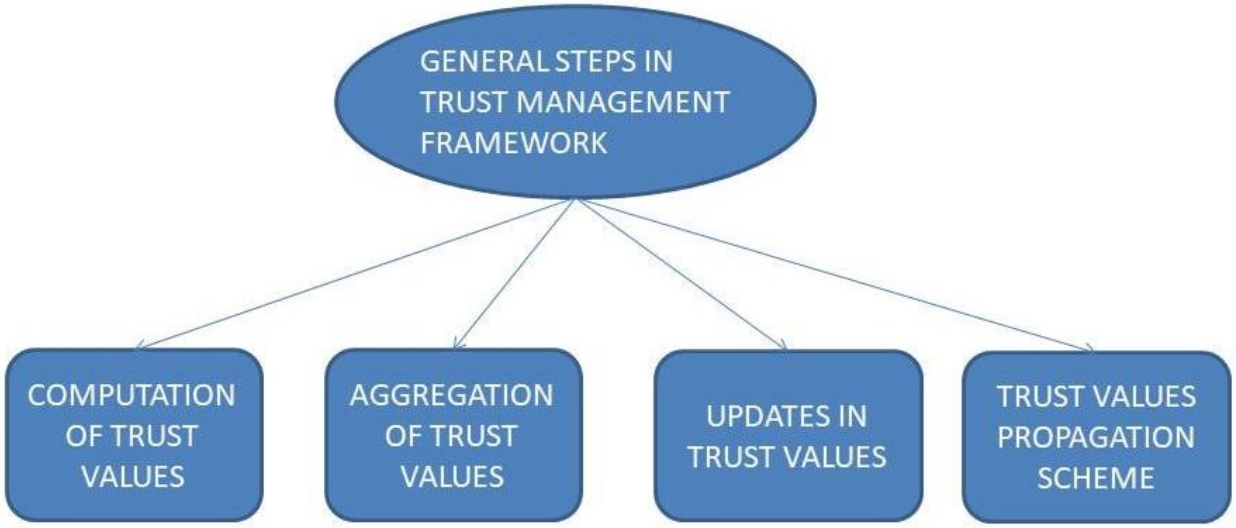

Fig -3: GENERAL STEPS IN TRUST MANAGEMENT FRAMEWORK

2.2 TRUST RELATED ATTACKS IN THE SIoT DOMAIN

A node or object can use its social connections with other nodes to nd the services it needs, but only if there is enough trust between them. The SIoT environment is made up of multiple social objects or devices with different characteristics. Misbehaving objects can take advantage of social interactions for launching attacks on a SIoT system as these malevolent nodes have ulterior motives. These misbehaving nodes or their owners want to get benefits from resources or services, but they do so at the expense of other nodes that can provide such services [1]. Thus, malicious nodes launch attacks on other nodes.

A malevolent node is dishonest and non-cooperative in a social context with the tendency to break the basic functionality of SIoT by executing attacks on various nodes [1]. In this context, trust management is crucial and assists SIoT nodes in overcoming perceptions of ambiguity and the risk of coming into contact with malevolent objects. In order to reduce the impact of malevolent devices, trust management systems for the SIoT encourage objects to collaborate honestly and constructively. These systems also forecast the most trustworthy trustee for a given trustor.

Due to the nature of cyber-physical systems, a successful attack on a SIoT system has the potential to be just as disastrous as the biggest industrial disasters to date [1]. Attacks are broadly categorized into two types: collaborative attacks and individual attacks [13]. These attacks are specifically
related to SIoT, hence the attacks listed below are ``Intrinsic
Attacks".

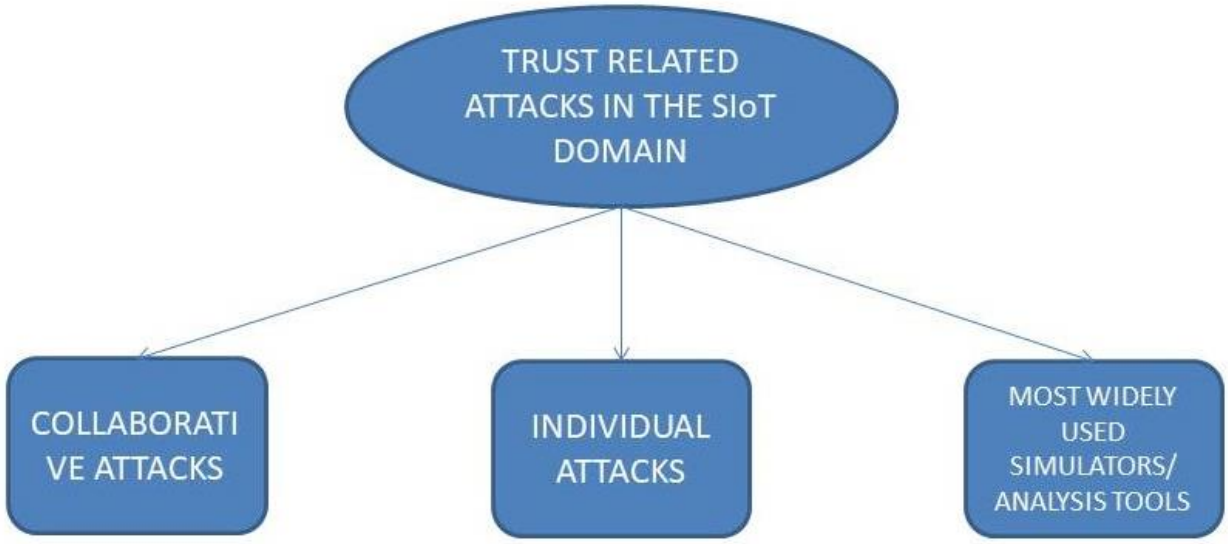

Fig -4: TRUST RELATED ATTACKS IN THE SIoT DOMAIN

3. APPLICATION AREAS OF SIoT CONCERNING TRUST MANAGEMENT

A description of application areas of trust management in the SIoT domain as shown in Figure 5 as follows:

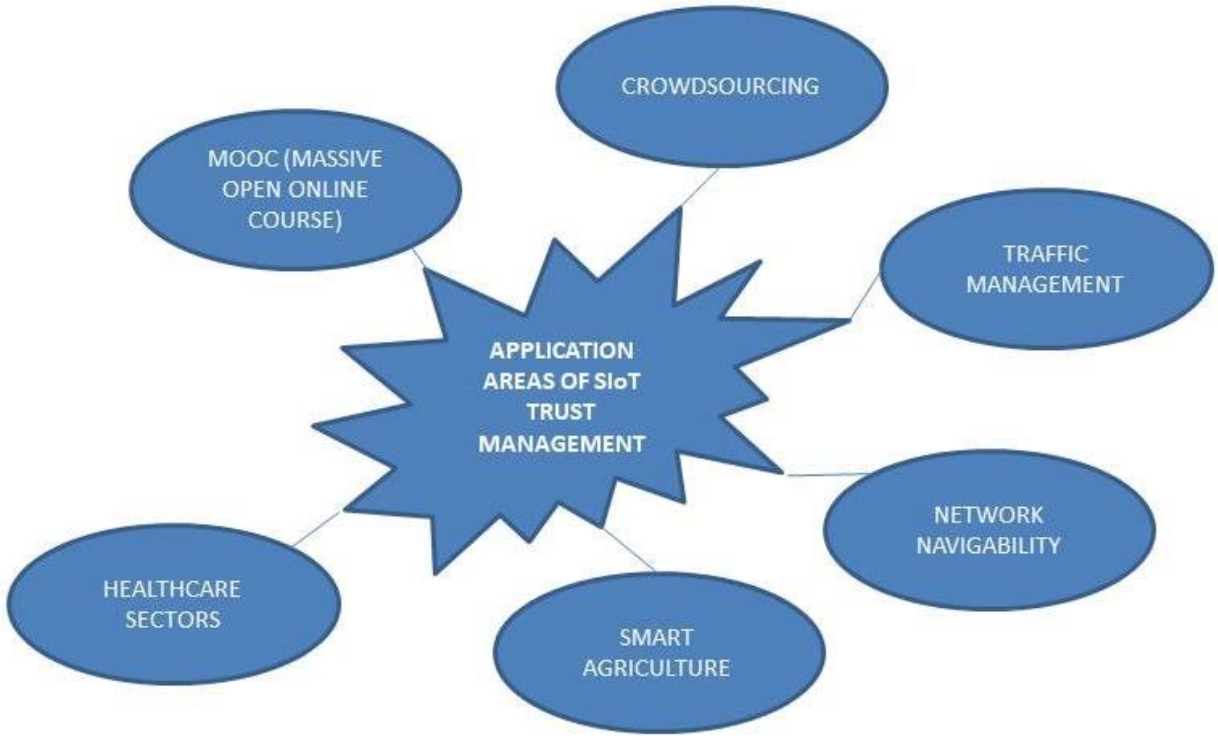

Fig -5: APPLICATION AREAS OF SIoT TRUST MANAGEMENT

4. CONCLUSIONS

Our research study provides a comprehensive analysis in the field of SIoT based on the trust management framework/ models. Different SIoT architectures are covered in the introduction section. Social relationships are the pillars of any SIoT architecture in any context. Therefore, this study also covers various social relationships which play an important role in the development of trust management frameworks

6. REFERENCES

[1]. Sana Alam , Shehnila Zardari , Shaheena Noor , Shakil Ahmed ," Trust Management in Social Internet of Things (SIoT): A Survey", VOLUME 10, 2022, Digital Object Identifier 10.1109/access.2022.3213699
and haralambos mouratidis
[2]. L. Atzori, I. A. Iera, and M. Giacomo, ``The Internet of Things:Asurvey," Comput. Netw., vol. 54, pp. 2787 2805, May 2010.
[3]D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, ``Internet of Things: Vision, applications and research challenges," Ad Hoc Netw.,
vol. 10, no. 7, pp. 1497 1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.
[4] D. E. Kouicem, Y. Imine, A. Bouabdallah, and H. Lakhlef, ``A decentralized blockchain-based trust management protocol for the Internet of Things," IEEE Trans. Dependable Secure Comput., vol. 19, no. 2, pp. 1292 1306, Mar. 2022.
[5] L. Atzori, A. Iera, G. Morabito, and M. Nitti, ``The social Internet of Things (SIoT) When social networks meet the Internet of Things: Concept, architecture and network characterization," Comput. Netw., vol. 56, no. 16, pp. 3594 3608, Nov. 2012.
[5] B. Afzal, M. Umair, G. A. Shah, and E. Ahmed, ``Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges," Future Gener. Comput. Syst., vol. 92, pp. 718 731, Mar. 2019.
[7] S. K. Lakshmanaprabu, K. Shankar, A. Khanna, D. Gupta, J. J. P. C. Rodrigues, P. R. Pinheiro, and V. H. C. D. Albuquerque, ``Effective features to classify big data using social Internet of Things," IEEE Access, vol. 6, pp. 24196 24204, 2018.
[7] Z. Lin and L. Dong, ``Clarifying trust in social Internet of Things," IEEE Trans. Knowl. Data Eng., vol. 30, no. 2, pp. 234 248, Feb. 2018.
[8] B. K. Tripathy, D. Dutta, and C. Tazivazvino, ``On the research and development of social Internet of Things," in Internet of Things (IoT) in 5G Mobile Technologies. Cham, Switzerland: Springer, 2016, pp. 153 173.
[9] M. M. Rad, A. M. Rahmani, A. Saha , and N. N. Qader, ``Social Internet of Things: Vision, challenges, and trends," Hum.-Centric Comput. Inf. Sci., vol. 10, no. 1, pp. 1 40, Dec. 2020.
[10] S. Shahab, P. Agarwal, T. Mufti, and A. J. Obaid, ``SIoT (social Internet of Things): A review," in ICT Analysis and Applications (Lecture Notes in Networks and Systems), vol. 314, S. Fong, N. Dey, and A. Joshi, Eds. Singapore: Springer, 2022, doi: 10.1007/978-981-16-5655-2_28.
[11] L. Atzori, A. Iera, and G. Morabito, ``Social Internet of Things: Turning smart objects into social objects to boost the IoT," Newsletter, Nov. 2014. Accessed: Oct. 12, 2022. [Online]. Available: https://iot.ieee.org/newsletter/november-2014/social-internet-of-things-turning-smartobjects- into-social-objects-to-boost-the-iot.html?__hstc=77947915. ab7bf88e972fdd7a7debc8575bac5a80.1457222400146.1457222400147.1457222400148.1&__hssc=77947915.1.1457222400149&__hsfp= 3972014050
[12] R. K. Chahal, N. Kumar, and S. Batra, ``Trust management in social Internet of Things: A taxonomy, open issues, and challenges," Comput. Commun., vol. 150, pp. 13 46, Jan. 2020.
[13] L. Atzori, A. Iera, and G. Morabito, ``SIoT: Giving a social structure to the Internet of Things," IEEE Commun. Lett., vol. 15, no. 11, pp. 1193 1195, Nov. 2011.
[14] V. Beltran, A. M. Ortiz, D. Hussein, and N. Crespi, ``A semantic service creation platform for social IoT," in Proc. IEEE World Forum Internet Things (WF-IoT), Mar. 2014, pp. 283 286.
[15] A. M. Ortiz, D. Hussein, S. Park, S. N. Han, and N. Crespi, ``The cluster between Internet of Things and social networks: Review and research challenges," IEEE Internet Things J., vol. 1, no. 3, pp. 206 215, Jun. 2014.