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

# Trust Based Service Management for Social Internet of Things: A Review

Prof. Y. B. Jadhav[1], Ms. Farisa Fatema [2],Ms. Vaishnavi D. Chaudhari [3], Ms. Aarti G. Khodke [4], Ms. Samruddhi J Pol[5]

[1] *Assistant Professor, Department of Computer Science & Engineering, Padm. Dr.V.B.K.C.O.E.Malkapur, Maharashtra, India*
[2] *Student , Department of Computer Science & Engineering, Padm. Dr.V.B.K.C.O.E.Malkapur, Maharashtra, India*
[3] *Student , Department of Computer Science & Engineering, Padm. Dr.V.B.K.C.O.E.Malkapur, Maharashtra, India*
[4] *Student , Department of Computer Science & Engineering, Padm. Dr.V.B.K.C.O.E.Malkapur, Maharashtra, India*
[5] *Student , Department of Computer Science & Engineering, Padm. Dr.V.B.K.C.O.E.Malkapur, Maharashtra, India*

**ABSTRACT**

***A social internet of things (iot) system can be seen as a combination of normal peer-to-peer networks and social networks, where "things" independently establish the social relationships according to the owners' social networks, and seek trusted "things" that can provide services stand in need of when they come into contact with each other opportunistically. We have suggested and analyze the design notion of many easily adaptable trust management system for social Internet of Things systems in which social relationships evolve are not constant but they are variable among the owners of Internet of Things devices. We have been reveal the planned trade-off between trust convergence vs. trust variation in our old easily adaptive trust management protocol design. With our regular fluently adaptable trust operation headliners, the social Internet of effects( SIOT) operations can fluently elect the stylish trust parameter settings in response to changing Internet of effects social parameters similar that not only trust assessment is accurate but also the application performance is enhanced. We have propose a table-lookup method to apply the analysis results dynamically and demonstrate the practicability of our proposed adaptive trust management scheme with two real-world social IoT service composition applications.***

***Index items/ keywords–Trust Management, Internet of Things, Social Networking , Performance Analysis, Adaptive Control, Security .***

## 1. INTRODUCTION

The Internet of Things (IoT) provides a platform to integrate a large number of distributed heterogeneous systems. common computing is the backbone of IoT, indicate a network of uniquely identifiable interconnected smart objects using standard communication protocols . 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 . IoT can be treated as a network whose prime goal is to include devices or nodes which can request or provide services. Moreover, nodes can work together to provide a single service . Since the initiation 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 Internet of Things’’ (SIoT), industrial IoT, and IoT in the healthcare sector. IoT enables various various devices to communicate and cooperate while providing or acquiring different services. However, this collaborative interaction can lead to trust challenges between devices, requiring a decentralized, mobile, cost-effective, low latency, lightweight and scalable trust management framework. The merging of ‘‘social networks’’ and the ‘‘internet of things’’ leads to the realization of SIOT , which has been characterized by the heterogeneity of the software and hardware components and a variety of hardware architectures. In SIoT these different devices collaborate and cooperate with each other to achieve a common target . Social Internet of Things is a broad term that includes connection entirely between people, between ‘‘things’’, or between people and things . Geographically circulate different objects can be efficiently detect through the use of SIOT. Social IoT includes both peer-to-peer networks and social relationships amongst multiple self-governing systems, where nodes act as

service providers (SPs) or service requesters/ consumers (SRs or SCs).

Every object or node on a social network acquires valid responses to their requests as compared to the objects or nodes working severally , The primary goal of Social IoT is to couple on things from people and allow them to self-organize – to share computational resources, information, and services. Every Entity must decide on the type of connection it has with other objects. Social IoT applications are likely balanced toward a service oriented architecture where each thing plays the role of either a service provider or a service requester, or both, according to the rules set by the owners. Unlike a traditional service-oriented Peer-to-peer network, social networking and social relationship plays an important role in a social IoT, since things (real or virtual) are essentially operated by and work for humans. Therefore, social connection among the owners must be taken into account during the preparing phase of social IoT applications. A social internet of things system thus can be seen as a P2P owner-centric community with devices (owned by humans) request and give services on behalf of the owners. IoT devices establish social relationships autonomously with other devices based on social rules set by their owners, and interact with each other excessive as they come into contact. It is out of our imagination that the future social Internet of things will be connect large amount of smart Objects in our physical world including RF identification (RFID) tags sensors ,actuators ,Personal Digital Assistance and smartphones as well as virtual objects in cyber space such as data & virtual Desktop on the different cloud. The Emerging paradigm of the social Internet of things has attracted a large amount of variety of application running on the top of it including Smart Home, Smart City ,E-health and smart community. We will have to use the term things objects and device interchangeably in the paper .

Such future social internet of things applications are likely oriented towards a service oriented architecture where each thing plays the role of either a particular service provider and a service requester (the person who request the service) or both , according to the principles set by the owners .Not likely a traditional service oriented Peer to Peer network , social networking and social relationship play an vital role in a social internet of thing , since things (virtual or real ) are essentially operate by the work for us (Humans). Therefore , Social relationship among the users or owners must be taken into account during the design phase of social internet of things application.

A Social IOT system thus can be seen as the Peer to peer owner-centric community with the devices (acquired by human ) requesting and providing different services on the behalf of the owners . Internet of things devices based on the social principles set by their owners , and interact with one another opportunistically as they come into contact . to best satisfy the service requester and maximize application performance , it is crucial to evaluate the trustworthiness of service provider in social internet of things environment .

## 2. LITERATURE SURVEY

We have Served recently proposed trust management protocols for IOT systems. We have contrast and compare our work with old/existing work so as to make difference in our work from the existing work and identify unique features and contributions of our trust management protocol design and trust based sevice management design for the Internet of things systems. There is a small work on trust management in Internet of Things in environments for security enhancement ,especially for dealing with misbehaving owners of Internet of things devices that provides different services to other Internet of things devices in the system.[14] proposed a trust management model which is based on the fuzzy reputation for the Internet of Things environment populated with the wireless sensor only , so they will only considered Quality of Service trust metrics like the packet forwarding /delivery ratios and energy consumption for measuring trust of sensors. On the other hand our , work will consider both QoS trust deriving from communication networks And social trust deriving from social networks which give to th social relationship of owners of IoT devices in the social Internet of things environment . Said et al .[**36**] proposed a context aware and multi-service approach for the trust management in IoT environments . Relative[**36**] to our trust protocol is totally distributed without requiring ant centralized trusted entity. Bao and Chen [5] proposed a trust management protocol considering both social trust metrices and use both direct observation and indirect recommendation to update in Internet Of Things systems .

However the adaptivity issue adjusts trust evaluation in response to dynamically changing as to cope with misbehaving node and maximize the IOT applications performance running on the top of trust management was not addressed related to cited above[5] we do not only consider multiple trust properties for Social Internet Of Things (SIOT) environment, but also analyze the tradeoff between the speed of trust convergence and fluctuation of trust to identify the best protocol parameter setting for trust propagation and aggregation to best exploit this tradeoff fot minimize the trust bias.

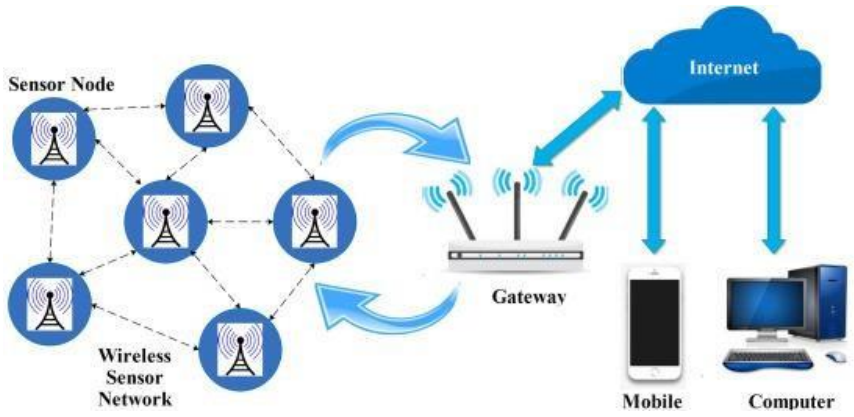


**Fig-1:** Social Internet Of Things (SIOT) Structure

Further more .it addresses the issue of trust formation for application performance maximization using service composition as an application example. Recently, Nitti *et al.* [32] had considered social relationships of owners of Internet of Things devices for trust management S IoT systems. They are proposed two models for trustworthiness management. First one ,*subjective model* deriving from social networks, with each node compute the trustworthiness of its friend on the basis of its own experience and on the opinion of friendly recommenders, and second is *objective model* derived from Peer 2Peer communication networks with each node stores and retrieves trust information towards its peers in a distributed hash table structure, so that any node can make use of the same information. Their objective model requires a pre-trusted nodes be in place for maintaining the hash table,which is questionable in IoT environments. Their subjectivemodel is also similar in spirit to our trust model taking into consideration for the social relationships between owners of IoT devices. The fundamental main difference is that our model of *objective trust* is based on ground truth or actual status, and our trust protocol dynamically adapts to changing environments by adjusting the best protocol settings to minimize trust bias (it is the difference between subjective trust and objective trust) and to maximize application performance. Security has taken the attention in IoT research [14, 15,34, 35, 42]. Roman *et al.* [35] Has discussed about threats to IoT, such as compromising botnets trying to hinder services and the domino effect in between intertwined services and userprofiling .Traditional network approaches to the network security ,ie data and privacy management ,to identify management and fault tolerance wii no be accommodate the requirement of IOT due to the scalability lack and inability to cope with a high variety of relationship and identity type[35].There is a possible solution proposed for each security problem, but specific protocols and analysis was not given. Ren proposed [34]a compromise-resilient key management scheme for heterogeneous wireless IoT. The proposed key managementprotocol includes key agreement schemes and key evolutionpolicies (forward and backward secure key evolution). The author also designed a quality of service (QoS) aware enhancement to the proposed scheme. However, the proposed scheme doesn't take social relationships among IoT identities into consideration. Chen and Helal [15 ] proposed a device-centric approach to enhance the safety of Internet Of Things. They were design a device description language i.e. DDL in which each device can specify its own safety concerns, constraints and knowledge .Nevertheless, their approach is specifically designed for sensor and actuator device, and does not consider social relationships among device owners. Zhou and Chao [42]proposed a architecture on media-aware traffic security for IOT .First ,the authors designed multimedia traffic classification and then develop this media aware traffic security architecture to achieve good trade-off between efficiency and flexibility of the system. A limitation of their work is that they only considered direct observations to traffic without considering indirect recommendations. Relative to the security and design/mechanism cited above ,our approach is to use trust to implement security against malicious attacks .We note that our trust system can work orthogonally with this security designs and mechanism to further enhance security of Social Internet Of Things(SIOT) systems.

## 3. CONCLUSION

We have study and provides a comprehensive analysis in the field of Social Internet of Things based on the trust management framework/models. Different social Internet of Things architectures are covered in the introduction section. Social relationships are the pillars of any Social Internet of Things architecture in any context. Therefore, this study also covers various social relationships which play an important role in the development of trust management frameworks as part of the introduction section. Our focus is on the examination of the trust management facets in social internet of thing that's why this study covers all different facets of trust in detail. Each trust management framework comprises Trust Attributes whose features are broadly classified as general trust properties and trust properties particularly related to the social aspects in the social internet of thing domain.

Our survey includes the classification of studies on the types of Trust Attributes ‘‘Social Trust’’ or ‘‘Quality of Service (QoS)’’ are used.
Any trust management framework is based on there three general steps: trust computation, trust aggregation, and trust updates. the trust management framework is based on there are three general types trust computation, trust aggregation, and trust updates.The three general steps make use of Trust Attributes to perform the estimation. a local trust values are accumulated or aggregated to form an overall or global trust by using various trust aggregation schemes. Our research work also covers many distinguished trust computation and trust aggregate techniques in detail. The weighted Sum technique is one of the generally. Used techniques because of its low cost and easily operated.

## 4. References

[1] Adali et al., "Measuring Behavioral Trust in Social Networks," *IEEE International Conference on Intelligence and Security Informatics*, Vancouver, BC, Canada, May 2010.
[2] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A Survey,” *Computer Networks*, vol. 54, no. 15, Oct. 2010, pp. 2787- 2805.
[3] 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,” *Computer Networks*, vol. 56, no. 16, Nov. 2012, pp. 3594-3608.
[4] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Computer Communications, vol. 54, 2014, pp. 1- 31.
[5] F. Bao, and I. R. Chen, “Dynamic Trust Management for Internet of Things Applications,” *2012 International Workshop on Self-Aware Internet of Things*, San Jose, California, USA, September 2012.
[6] F. Bao, Dynamic Trust Management for Mobile Networks and Its Applications, ETD, Virginia Polytechnic Institute and State University, May 2013.
[7] F. Bao, I. R. Chen, M. Chang, and J. H. Cho, “Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-Based Routing and Intrusion Detection,” *IEEE Trans. on Network and Service Management*, vol. 9, no. 2, 2012, pp. 161-183.
[8] F. Bao, I. R. Chen, and J. Guo, “Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems,” *11th IEEE International Symposium on Autonomous Decentralized System*, Mexico City, Marc———h 2013.
[9] N. Bui, and M. Zorzi, “Health Care Applications: A Solution Based on The Internet of Things,” *the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, Barcelona, Spain, Oct. 2011, pp. 1-5.
[10] B. Carminati, E. Ferrari, and M. Viviani, *Security and Trust in Online Social Networks*, Morgan & Claypool, 2013.
[11] . R. Chen, F. Bao, M. Chang, and J.H. Cho, “Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, 2014, pp. 1200-1210.
[12] I. R. Chen, F. Bao, M. Chang, and J.H. Cho, “Trust-based intrusion detection in wireless sensor networks,” *IEEE International Conference on Communications*, Kyoto, Japan, June 2011, pp. 1-6.
[13] I.R. Chen, F. Bao, M. Chang, and J. H. Cho, “Trust management for encounter-based routing in delay tolerant networks,” *IEEE Global Telecommunications Conference (GLOBECOM 2010),* 2010, pp. 1-6.
[14] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, “TRM-IoT: ATrust Management Model Based on Fuzzy Reputation for Internet of Things,” *Computer Science and Information Systems,* vol. 8, no. 4, Oct. 2011, pp. 1207-1228.
[15] C. Chen, and S. Helal, “A Device-Centric Approach to a Safer Internet of Things,” *the 2011 International Workshop on Networking and Object Memories for the Internet of Things*, Beijing, China, Sep. 2011, pp. 1-6.
[16] J.H. Cho, I.R. Chen, and P. Feng “Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile AdHoc Networks,” *IEEE Trans. on Reliability*, vol. 59, 2010, pp. 231- 241.
[17] J. H. Cho, A. Swami, and I. R. Chen, “Modeling and Analysis of Trust Management for Cognitive Mission-Driven Group Communication Systems in Mobile Ad Hoc Networks,” *International Conference on Computational Science andEngineering*, vol. 2, 2009, pp. 641-650.
[18] J. H. Cho, A. Swami, and I. R. Chen, “Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks,” *Journal of Network and Computer Applications*, vol. 35, no. 3, 2012, pp. 1001-1012.
[19] K. Dar, A. Taherkordi, R. Rouvoy, and F. Eliassen, “Adaptable Service Composition for Very-Large-Scale Internet of ThingsSystems,” *ACM Middleware*, Lisbon, Portugal, Dec. 2011.
[20] T. Dubois, J. Golbeck, and A. Srinivasan, "Predicting Trust and Distrust in Social Networks," *IEEE 3rd International Conference on Social Computing*, Boston, MA, USA, Oct. 2011, pp. 418-424.

[21] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A Survey on Facilities for Experimental Internet of Things Research," *IEEE Communications Magazine*, vol. 49, no. 11, Nov. 2011, pp. 58-67.
[22] A. Gutscher, "A Trust Model for an Open, Decentralized Reputation System," *IFIP International Federation for Information Processing*, vol. 238, 2007, pp. 285-300.
[23] A. J. Jara, M. A. Zamora, and A. F. G. Skarmeta, "An Internet of Things-Based Personal Device for Diabetes Therapy Management in Ambient Assisted Living (AAL)," *Personal and Ubiquitous Computing*, vol. 15, no. 4, 2011, pp. 431-440.
[24] A. Josang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," *Decision Support Systems*, vol. 43, no. 2, March 2007, pp. 618-644.
[25] T. Karagiannis, J.-Y. Le Boudec, and M. Vojnović, "Power Law and Exponential Decay of Intercontact Times between Mobile Devices," *IEEE Transactions on Mobile Computing*, vol. 8, no. 10, 2007, pp. 1377-1390.
[26] S. Lee, R. Sherwood, and B. Bhattacharjee, "Cooperative Peer Groups in NICE," *INFOCOM 2003*, vol. 2, pp. 1272-1282, SanFrancisco, March 2003.
[27] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart Community: An Internet of Things Application," *IEEE Communications Magazine*, vol. 49, no. 11, Nov. 2011, pp. 68-75.
[28] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," *IEEE Conference on Computer Communications*, San Diego, CA, March 2010, pp. 1-9.
[29] L. Liu, X. Liu, and X. Li, "Cloud-Based Service Composition Architecture for Internet of Things," *International Workshop on Internet of Things*, Changsha, China, August 2012, pp. 559-564.
[30] G. Liu, Y. Wang, M.A. Orgun, and H. Liu,"Discovering Trust Networks for the Selection of Trustworthy Service Providers in Complex Contextual Social Networks," *19th IEEE International Conference on Web Services*, 2012, pp. 384-391.
[31] R. Mitchell and I.R. Chen, "Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems," *IEEE Transactions on Reliability*, vol. 62, no. 1, March 2013, pp. 199-210.
[32] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness Management in the Social Internet of Things," *IEEE Transactions on Knowledge and Data Management*, vol. 26, no. 5, 2014, pp. 1-11.
[33] F. Paganelli and D. Parlanti, "A DHT-Based Discovery Service for the Internet of Things," *Computer Networks and Communications*, vol. 2012, Article ID 107041, 11 pages, 2012.
[34] W. Ren, "QoS-aware and compromise-resilient key management scheme for heterogeneous wireless Internet of Things," *International Journal of Network Management*, vol. 21, no. 4, July 2011, pp. 284- 299.
[35] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, Sep. 2011, pp. 51-58.
[36] Y.B. 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 and Security*, vol. 39, part B, Nov. 2013, pp. 351–365.
[37] A. A. Selçuk , E. Uzun , and M. R. Pariente, "A Reputation-based Trust Management System for P2P Networks," *Network Security*, vol.6, no.3, May 2008, pp. 235-245.
[38] W. Sherchan, S. Nepal, and C. Paris, "A Survey of Trust in Social Networks," ACM Computing Survey, Vol. 45, No. 4, Article 47, August 2013.