Review Paper

A glimpse of Semantic Web trust

Sam Rahimzadeh Holagh[1] · Keyvan Mohebbi[2]

Received: 20 May 2019 / Accepted: 31 October 2019 / Published online: 30 November 2019

Abstract

Trust management plays a significant role in the Semantic Web for combining authoritative information, fitting the services and increasing data security and user privacy. It helps people to overcome mistrust and fear of risk (for selecting the services) as well as providing reliability for the user to use the Semantic Web services. This paper tries to give an insight regarding different dimensions of Semantic Web trust layer. It will look at trust from four different perspectives, namely policies which can be applied, contents that should be proven, in addition to origins of acquired information or services. Finally, due to emergence of Semantic Web of things, the trust model and management within distributed systems will be reviewed.

Keywords Semantic Web · Trust · Policy · Reputation · Content · Semantic Web of things

1 Introduction

In the era of Information, by transformation of Internet into Internet of things and Semantic Web, cooperation of human and computers is the prime solution for social challenges. The main purpose of Semantic Web creation was to assist not only the human interactions with machines but also to help the machines interactions with each other. In fact, the Semantic Web can be viewed as a network of linked information, which facilitates machine processing globally. Semantic Web also can be considered as sets of relationships between entities on the Web, these connections can also be seen as graphs where the predicates are taken as edges and classes as nodes [1].

From the beginning, it was clear that the reliability and security of information in an immense and open information space such as Web would become a challenge. Almost unsupervised and uncontrolled, it is the nature of Web that allows one to say anything over a certain subject on the Web, and this makes the Web a unique source of information. However, it is the user's responsibility to distinguish right from wrong. On the other hand, in an agent based environment, where computers have to make choice over multiple and alternative sources to the requested queries, this would be achieved through harder and computationally intense processes [2]. Therefore, necessity of a mechanism to provide secure data interaction, identify the trueness of content and trustworthiness of the origin is obvious.

Getting information from Web become common every day, and users acquire their information through various sources ranging from personal Web pages, governmental institutions to scientific portals, human users tend to make decision regarding to trust a source using different methods, such as relying on their previous experiences or other user's opinions, but as we know the Semantic Web seek different goal and that is to give computer agents the ability to interact with the Web content and other agents, make decisions over choosing the right service or information provider. In this case, how will be a computer agent able to trust an information source? How can it identify the correctness of acquired information? And how it can achieve a secure communication?

✉ Keyvan Mohebbi, k.mohebbi@mau.ac.ir | [1]Department of Management, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran. [2]Department of Electrical and Computer Engineering, Mobarakeh Branch, Islamic Azad University, Mobarakeh, Isfahan, Iran.

SN Applied Sciences (2019) 1:1732 | https://doi.org/10.1007/s42452-019-1598-6

This paper provides an overview on the research works related to the Semantic Web security and trust layers of the Semantic Web stack. Section 2 studies various definitions of trust and reputation. Section 3 categorizes trust from different perspectives. Section 4 reviews the prominent approaches in the distributed trust. Section 5 presents different trust and reputation test beds. Section 6 introduces open challenges. Section 7 concludes the paper.

2 Definitions

This section reviews the definitions two preliminary concepts, namely trust and reputation.

2.1 Trust

Trust carries different meaning depending on the context and the area it is used. In computer network it refers to mechanisms that insure the security and access control. In distributed systems and agent based systems it is considered as a tool to measure reliability. In game theory and policies, it is viewed as the rate of correct decisions made by system under uncertain condition [3]. Trust can be clustered in two main categories, namely reliability trust and decision trust, each with different descriptions. When person A asks person B to perform a certain task, the reliability (probability) of trusted person B as seen by trusting person A depends on the performance of expected tasks [1].

Trust in decisions is the degree that trusting party is willing to depend on trusted party under certain circumstances to acquire sense of security, even against the possibility of odds. Decisions made under this class, depends on the degree of risk accepted by trusting party and the previous negative or positive experiences it had toward trusted party [2]. Trust is also defined as the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context [3].

Trust is not a new topic in computer systems, but it is among the vital issues within the computer science scope. Figure 1 shows the amount of published articles related to trust topics in Semantic Web as reported by the Google Scholar.

2.2 Reputation

General thoughts regarding a person or thing are called reputation. Reputation can be based on accumulated ratings or scores given by community members to a person. Different approaches can be implemented in order to calculate rating of an entity, such as average; for example, it is possible to calculate the average of reputation scores given by community members toward the attitude of an entity. Usually members of certain group receive almost the same rating from other users, when a group is well known in certain subject, all the members of that group usually receive the same credit as their group [4].

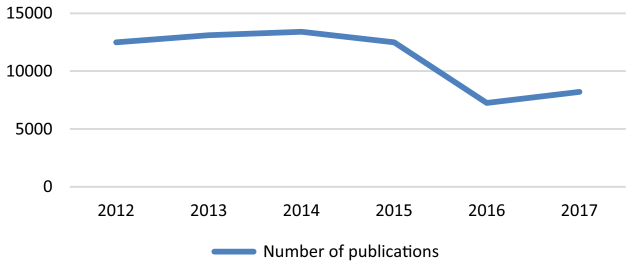

Fig. 1 The number of publications regarding semantic web trust layer

In addition, reputation can be considered as the personal beliefs or experiences of an entity regarding to performance of other entity over certain subjects. In this case, reputation ratings should be based on firsthand experiences or based on a weighted measure divided by the total amount of references provided by single individual such as the approach used by Google's page rank. A reputation approach can be either centralized and be given by an authority, or it can be distributed and based on knowledge of crowd [5].

3 Categorization of the trust

This section categorizes the trust and the providing approaches, based on three perspectives.

3.1 Policy-based trust

The only vertical layer of Semantic Web stack, which is called digital signature, utilizes the XML digital signature ability such as signed references, info's and digestion values to mark any Web content. Along with proof, logic and trust layer itself; these layers are responsible for trustworthiness of Semantic Web processes [3]. As the structure of XML Documents are like graphs, the main challenge is to designate which parts of the documents be accessible by which users through enforcing policies on users and documents. In other words, Semantic Web agents are required to ensure the safety of information and Web services from unauthorized access. To satisfy this need, there are broad range of security policies, such as authentication, data integrity and privacy, access control, authorization and confidentiality existing.

XML nature of Semantic Web gives it the advantage of using meta data instead of data itself. There are many advantages in using information regarding data instead of whole data itself. One is the relatively small size of meta data, in addition to the ability to make data more discoverable. Besides many benefits of meta data, it has disadvantages. It can be created by number of resources, such as automated tools, data owner itself and other users on the Web, therefore because of non-uniform trustworthiness of meta data generators on the Web, it is imperative for each user to understand the trustworthiness level of each Meta data in order to get the full advantage of it [2].

Currently, our Web is equipped with variety of tools to ensure security of information exchange. Tools such as digital signature, public key, Web certificate and encryption. Several security standards have been introduced to guarantee safety of contents exchanging in Web of trust between business partners. For example, WS-security policy introduced by W3C for XML-based Web services, which describes ways of attaching signatures and encryption headers or security tokens to a SOAP message, or SAML policy provided by OASIS security services which is providing a means to authorize and authenticate, but it is unable to give any suggestion regarding trust [6].

Kerberos ticket issuing system, which is originally created by MIT for project Athena, is one of the widely used trusted third-party authentication technologies. WS-trust as an extension to previously mentioned WS-security, designates the ways of acquiring trust through authorization, identity proof and entity performance [7].

Another challenge in establishing trust is to provide a means to reveal credential but prevent loss of privacy and control over information. To deal with this issue, different mechanisms and policies are introduced, such as TrustBuilder which was designed to provide mechanism for credential tradeoffs in a way that would not be causing loss of privacy [8]. As trust decisions are type of actions that require acceptance of certain amount of risk of revealing credentials in return to getting advantage of earning trust. Other system suggested to facilitate negotiation of credential exchange is called PeerTrust, which is a more recent policy and trust negotiation language [9, 10].

The prominent standards and technologies to implement policies are depicted in Table 1.

3.2 Reputation-based trust

The purpose of reputation-based trust is to make trust decisions through personal- or others-experiences or in some cases through combination of personal and global experiences. In reputation-based trust, members in the community judge about other members in their network based on their transactions, quality of product and service consistency [17, 18]. In other words, members of community would implement a collaborative sanctioning in a team effort to give incentive to poor quality service providers in the network to provide better services. A trust-based network can be considered as a graph in which the members are nodes with weighted edges according to amount of trust performance perceived from other users by members. Through trust network, users will be able to trust the resources directly by personal experiences or indirectly by other trusted users using trust propagation methods [19, 20].

Reputation network can be viewed from different viewpoints. It can be divided into centralized and distributed architectures. In centralized reputation system, information related to quality and performance of any member is collected from other users who had direct experience with that particular node in network. Then a central authority usually called reputation center collect all the ratings and calculates a score for every member of the node and publicize the scores. Members of community can use the distributed reputation score in their decisions of making transactions with other members in network. The idea behind this system is that, transactions with members with higher reputation score usually yields better results [2]. Figure 2, shows the schema of a centralized model.

Table 1 Prominent trust policies and systems

Subject area	Suggested method	References
Credential exchange	Kerberos system	Kohl and Neuman [7]
Trust negotiation	TrustBuilder	Winslett et al. [8]
	RT0	Li et al. [11]
	PeerTrust	Leithead et al. [9]; Nejdl et al. [10]
	PROTUNE	Bonatti et al. [12]
Access control	SAML	OASIS [13]
	WS-Trust	IBM [14]
Distributed trust management	PolicyMaker	Blaze et al. [15]
	KeyNote	Blaze et al. [16]

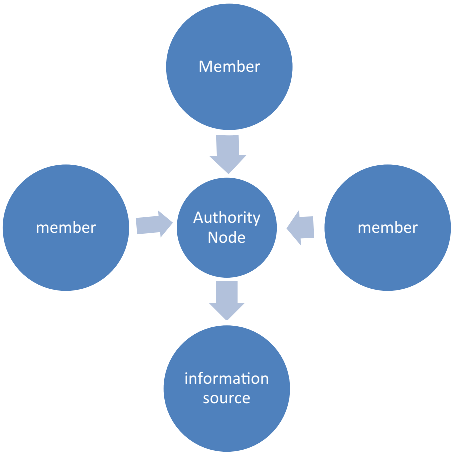

Fig. 2 The schema of a centralized model

In a distributed system, there is no reputation center, instead there are multiple reputation bases where each member can submit its experience regarding other members, or even members can get information they need related to a certain member of community from different user who had previous experience regarding that particular member. A peer-to-peer system is an example of distributed system [21].

In some of the research works, the distributed architecture is divided into two subcategories, namely global and local. Within global model, reputation is based on degree of popularity of members of society. Each member of society creates a profile for every other member of network after the first interaction and saves the experiences regarding each transaction. One may make decision about trusting a source using other neighbor's experience profile. However, because of the nature of Web, distinguishing between right information from wrong is rather a sophisticated process. Therefore, as calculation of reputation based on total score given by users of network might not be completely correct, one might try to trust to scores calculated by certain nodes in the network, those nodes that may also act as authority nodes on society, may get their competencies through their high social network scores. The more links a node has, the better it can be trusted. The EigenTrust algorithm is an example for global trust performance ranking [22]. Figure 3, shows the schema of a distributed model.

In a local model, the idea is based on transitivity nature of reputation, although under conditions in this model trust is personal and varies from node to node, but in any case a node didn't have any information regarding a new trustee, it can rely on closed trusted nodes experience. If someone doesn't have any information regarding someone else usually his/her trusts to his friends and relatives more than unknown people or sources. According to small world hypothesis, there would be a path from trustor to trustee through chain of trusted close friends [3, 23].

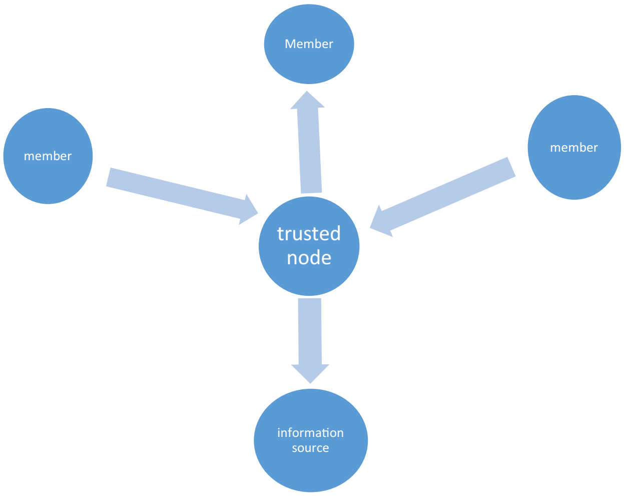

Fig. 3 The schema of a distributed model

In the following, some of the reputation calculation models are reviewed:

Subtraction or ratings average One of the simplest ways of reputation calculation is the subtraction of aggregation of positive and negative ratings given by users. These methods are also known as simple summation and average methods. The advantage of this method is its simplicity, but it also suffers from imperfect reflection of user's opinion regarding a particular member or information resource due to its primitive mathematics [19]. An advanced version of this method is calculation of average of ratings or weighted average of ratings based on certain factors each with a weight assigned to them [1].

Bayesian model This model gets positive and negative ratings and using probability density function (PDF) tries to update the trust scores. New scores are calculated using previous scores and new ratings. This method can be advantageous because of its theoretical bases, but also has the disadvantage of being so complex for to understand it [1]. Formula utilized to calculate interaction based trust during exploratory stage is:

$$Tinter(A,B) = \frac{\text{number of correct replies}}{\text{total number of replies}}$$

Opinion model In this method, it is suggested to use belief as a representative for reputation. Here, there are only two possible conditions: If agents are trustworthy or not (A,Ac), and the trustworthiness of an agent T(A) would be calculated through subtraction of accumulation of beliefs (M(A), M(Ac)).

$$T(A) = M(A) - M\left(A^{c}\right)$$

where $M(A)$ & $M(A^{c}) \in [0, 1]$ and $T(A) \in [-1, 1]$.

Because opinions can also be mapped into Beta PDFs and hence the opratores are the same as bayesian method, therefore this model can be named both opinion- and bayesian-based [3].

Fuzzy logic based model In this method, using linguistically fuzzy concepts repution of members of network is indicated, meaning that the amount of membership function illustrates almost how much agents are fit into concepts of trustworthiness. Reasoning in this method is done through fuzzy logic and fuzzy measures [2].

Flow model In flow method, reputation is calculated using the transitive itraton through chain of members in the network. Some of models assume a constant reputaton weight for how trust network which can be distributed between members of network, even or unevenly. Each member reputation can only be increased at the cost of other members, since the total weight of network is constant. Therefore, the degree of increase and decrease of each node reputation is a function of input and output flow of the reputation score within the network [2]. Table 2, summarizes the reputation calculation models and their prominent examples.

Multi context models Since Trust and reputation are multi-context in nature, therefore creation of multi-dimensional models to calculate trust and reputation has importance. Multi-dimensional models have modular structure, agents created in such an architecture are capable of utilizing several logics in a way that increases its representational power to maximum [21]. Some of well-known multi-dimensional models are REGRET, SPORAS and HISTOS.

REGRET model Within REGRET model it is possible to calculate multi-dimensional reputation systems, it is possible to take into account dimensions such as social, ontological hierarchy and individual dimensions. This model is actually the natural extension of previous widely used models and is flexible enough to be implemented on societies with different social structure, and agents that belong to more than one group at a time [21].

SPORAS and HISTOS models As an evolved version of online reputation models in which are utilizing simple summation and average methods, within SPORAS only the most recent rating between users is considered and also users with higher reputation values receive very smaller rating changes in compare to the users with low reputation values after each update iteration. Although SPORAS have the same characteristics of simple summation and average models but still has more robustness to user behavior changes and hence is more reliable. HISTOS was introduced as a response to lack of personalization within SPORAS model. HISTOS can deal with direct information as well as witness information [24].

AFRAS model The main Idea behind this model is to utilize fuzzy values for designation of reputation values. This method aggregates the old satisfaction value and new reputation values using weighted aggregation method. This calculation is done once the new fuzzy set in which shows the degree of satisfaction of the latest interaction between two nodes is created [24].

3.3 Content-based trust

Web contents are represented as axioms and ontologies within the Semantic Web. In the following, the possibilities of using content of Web transactions to gain trust are explored. Content of information exchanged on the Web was never considered in Semantic Web trust layer. This issue is solved by authentication, identification and proof checking. However, Semantic Web makes it possible to interact and utilize Web content directly. Thus, it provides a unique opportunity to use the content of Web resources as a means to judge regarding the identity of their creators.

While all other types of trust assessment methods are concerned with information provider's legitimacy based on their reputation, behavior and implemented policies, content-based trust is more involved with the nature of the contents given on the Web. In real life, one

Table 2 Prominent examples of reputation calculation models

Calculation model	Example	References
Subtraction or ratings average	Ebay reputaion forum	Resnick and Zeckhauser [5]
	Amazon	Schneider et al. [4]
Multi-dimentional	REGRET, HISTOS	Sabater and Sierra [21]; Carbo et al. [24]
Bayesian	Institutionalized trust	Esfandiari and Chandrasekharan [25]
Opinion	Epinions	Shekarpour and Katebi [3]
Fuzzy	AFRAS	Carbo et al. [24]
Flow	Google's PageRank	Page et al. [26]
	Appleseed algorithm	Ziegler and Lausen [27]
	Advogato's reputation scheme	Levien [28]

may choose to trust information provided by a trusted resource, however if the information that is provided by many low trusted resources are the same and it conflicts with the information given by the trusted resource, then people might choose to believe the information comes from the many, even if they may not look legit. Therefore, it can be said that each of the reputation and certification is just one of the dimensions that would create a phenomenon called trust.

Various factors are suggested that affect user's decision in choosing trusted resources, as follows:

Authority Trusted information providers for particular subject may not be trusted on other subject areas. People may trust information provided by world health organization about diseases, but economical information is provided by the same organization will not be trusted by the users [29].

Transitivity of legitimation Having relation with highly trusted and authorized entities on the network can transfer some of trust to other entities in relation with them. For example, certificates provided by universities to medical students [29].

Pedigree Contents generated by entities may receive credit and trust from their creators. Information provided by a scientific web site is more likely to be accepted by user in compare to anonymous resources [30].

Bias Sometimes information provided by resources may be incomplete or insufficient under certain condition, for example a drug production factory may ignore side effects related to certain treatment condition and focus on trial outcomes. Designation of bias requires expertise and profession [16].

Motivation in providing accurate information If there is motivation and interest in information provider to provide more accurate information, then it is more likely that users believe to that information [29].

Deceptive behavior Encountering with information resource with sinister goals is natural event on the Web, therefore users should be alerted about the fact that resources and their associates may not be what they appear to be [31].

Based on what mentioned regarding content-based trust, this method tries to introduce new metrics for trust, using the content of information provided by the trusted suppliers. In a Semantic-enabled Web, not only humans will need to make decisions, but also agents should be able to choose to trust certain resources while facing with many other alternatives. This process is happening by human users on everyday life. People choose resources and information in their everyday Web activities but the rationale behind their decision is unknown due to complexity of human behavior, therefore it would be advantageous for automated systems and agents to utilize the capabilities of Semantic Web and make trust judgments based on content of information provided by resources [32].

4 Trust in Semantic Web of things

Another environment in which trust bares importance is the distributed systems and to be more accurate Semantic web of things. While speaking about security solutions in the area of distributed systems, the terms trust model and trust management plays a key role. The difference between trust management and trust model is that the trust management can be considered as potential solution for a distributed system security concerns, while the trust model is a special perception from the trust management which explains the techniques and approaches. It is possible to explain the trust model of distributed systems in 6 phases, as depicted in Fig. 4.

In the literature, Li et al. [11] introduced a new language for management of trust based on behavior and constructed a hypothetical meaning for them. In addition, they illustrated that utilization of graphs in credentials are functioning accurately [11]. Ghorbanimoghaddam [33] highlighted the advantages of using trust in distributed systems and explored weaknesses of different related introduced trust methods. According to research works

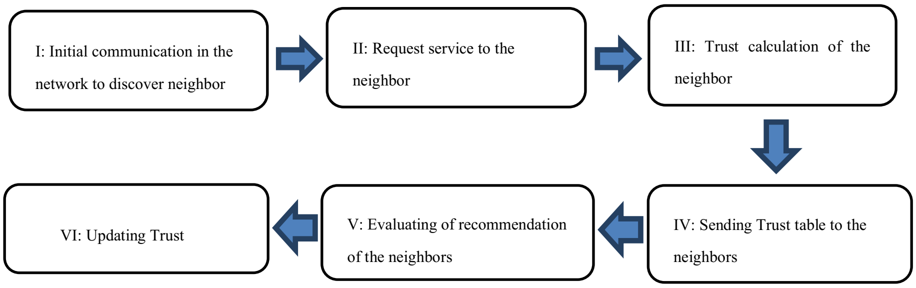
I: Initial communication in the network to discover neighbor
II: Request service to the neighbor
III: Trust calculation of the neighbor
IV: Sending Trust table to the neighbors
V: Evaluating of recommendation of the neighbors
VI: Updating Trust

Fig. 4 Trust phases within distributed systems

Table 3 Prominent works in distributed trust

Author	Methodology	Performance/trust evaluation metrics	Trust property	Result	Trust management model
Bao and Chen [36]	Update trust value using direct observations and Indirect recommendations	Social trust and QOS metrics	Honesty, cooperativeness, and community-interest	Effectiveness of our trust management Protocol by a service composition application in comparison with Ideal service composition (upper bound) and Random service composition (lower bound)	Community-based social environment
Jingpei Wang et al. [37]	Fuzzy set theory and formal semantics-based language	Quality of service (Qos)	(1) Extracting trust information (2) Decision-making based on trust (two types of decision-making based on trust: access Control policy, based on trust and self-organized decision)	Providing a service of self-organizing a set of items based on their trust status to take an informed decision	Based on a service model (layered)
Dong Chen et al. [17]	Direct observations and indirect reputation-NS-3 simulator	(1) End-to-end packet forwarding ratio (EPFR) (2) AEC: the energy consumption (3) The package delivery ratio (PDR)	Confidentiality integrity, availability	(PDR) Package Delivery Ratio (DP) Detection Probability (CS) Convergence speed Better performance In comparison with two reputation model DRBTS [26] and BRTM-WSN [27]	Based on fuzzy reputation model (TRM)
Ben Saied et al. [38]	Assigns dynamic trust scores to cooperating nodes according to different contexts and different functions	Trust values updated by events and time	–	Deter a class of common attacks designed to target trust management systems	A context-aware and multiservice approach
Ray Chen et al. [30]	Direct user satisfaction experiences of past interaction experiences and recommendations from others.	Social relationships: friendship, social contact, and community of interest	Scalability	–	SOA-based service oriented architecture
Hui Xia [19]	Direct trust, recommendation trust, incentive function and active degree Netlogo Simulator	Incentive function and active degree	Network interaction quality, adaptability, malicious node identification, attack resistance	Lesser attack effects on introduced model in compare to TSF2 and CFStrust	Based on fuzzy approach
Yinan [39]	Both direct observations and indirect recommendations in NS-3.17 network simulator	–	Effectiveness	Delay-tolerant MANET	Using social network theory (social hierarchy is structured using balanced connectivity criteria and a K-mean clustering algorithm)

Table 3 (continued)

Author	Methodology	Performance/trust evaluation metrics	Trust property	Result	Trust management model
Nitti and Atzori [40]	Past direct (direct interactions) or indirect (through intermediate nodes) Experiences	Credibility and centrality	–	Isolation of almost any malicious node in the network	Social Internet of Things (SIoT) paradigm basis of the behavior of the objects

around On and OFF attacks, using an adaptive oblivious pattern instead of using oblivious factors themselves is more effective [33]. Nitti et al. [34] introduced a protocol for dynamic management of trust, a solution to deal with nodes that acting wrong and functioning dynamically. This protocol also was able to designate the suitable parameters for each conditions of network in which dynamically changing [34]. Liu et al. [35] first explored failure reasons of traditional security mechanisms in managing trust, and then introduced a holistic model to manage trust within distributed system such as the one used in distributed systems [35].

Table 3 summarizes the prominent works in the distributed environment for trust management within distributed systems.

5 Trust and reputation test beds

In order to observe the performance and behavior of introduced trust and reputation models, it is required to test them within certain environment called testbed. Since each model tries to cover certain aspects of reputation and trust, therefore there is no test bed that offers an environment to compare all of presented models with each other hence making comparison process more twisted and complicated. Each proposed model is presented by particular testing environment exclusively designed to that model. There are test beds created based on prisoner's Dilemma such as the playground designed by Marsh [41]. In this test bed agent have freedom of movement and interactions are saved using prisoner's dilemma whenever agent make a move. Schillo et al. [42] suggested a disclosed iterated prisoner's dilemma using partner selection and standard payoff matrix [42]. Castelfranchi et al. [43] in their research presented a test bed designed to observe the effects of interactions between artificial agent populations following different criterions for aggregation control purposes. ART test bed presented by Fullam et al. [44], as a respond to existing shortcomings among previously introduced test beds, within ART test bed researchers are capable of comparing different subjective metrics and conduct their research using flexible parameters [44].

6 Open challenges and issues

After reviewing the literature, we have recognized many open challenges and issues in the scope of this research. In summary, there are still the need for:

1. Performance improvement for Semantic Web trust algorithms.

2. Seamless integration and cooperation of various trust management models for achieving holistic trust management in Semantic Web.
3. Power efficient trust management models, as well as faster and less energy consuming mechanisms to support semantic enabled devices within IoT.
4. Approaches to overcome difficulties of transmission and computation of trust among different networks.
5. Privacy of the human and confidentiality of the business processes.
6. Autonomic trust management algorithms.
7. Trustworthy data fusion.

7 Conclusion

This paper tried to give an insight regarding different dimensions of Semantic Web trust layer. How intelligent agents should trust different resources on the Web when more than one choice is available depends on reputation metrics and calculation methods that mentioned here. How to decide whether the content supplied is relevant using the nature of Semantic Web is explored in this research. In addition, different policies that can be imposed on network to facilitate and secure information exchange has been reviewed. As for the distributed systems, in order to achieve robust trust management, trust properties should be improved. Valid ratings for comments provided by nodes, honesty of the provided recommendation by each node within semantic networks and evaluation of the past experience with a particular node that is intended to communicate with, could be solved utilizing fuzzy logic approaches, also the context aware approaches are good to deter malicious information within Semantic Web space. As a result, it seems that the combination of the context aware and fuzzy approaches could be useful in designing an effective trust management model in this scope.

Compliance with ethical standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Jøsang A, Ismail R, Boyd C (2007) A survey of trust and reputation systems for online service provision. Decis Support Syst 43:618–644
2. Glimm B, Stuckenschmidt H (2016) 15 years of semantic web: an incomplete survey. KI-KünstlicheIntelligenz 30(2):117–130. https://doi.org/10.1007/s13218-016-0424-1
3. Shekarpour S, Katebi SD (2010) Modeling and evaluation of trust with an extension in semantic web. Web Semant Sci Serv Agents World Wide Web 8(1):26–36. https://doi.org/10.1016/j.Websem.2009.11.003
4. Schneider J et al (2000) Disseminating trust information in wearable communities In: Proceedings of the 2nd international symposium on handheld and ubiquitous computing (HUC2K)
5. Resnick P, Zeckhauser R (2002) Trust among strangers in internet transactions: empirical analysis of eBay's reputation system. In: Baye MR (ed) The economics of the internet and e-commerce, advances in applied microeconomics, vol 11. Elsevier Science, Amsterdam
6. Jøsang A (2001) A logic for uncertain probabilities. Int J Uncertain Fuzziness Knowl Based Syst 09(03):279–311. https://doi.org/10.1142/s0218488501000831
7. Kohl JT, Clifford Neuman B, T'so TY (1994) The evolution of the Kerberos authentication system. In: Distributed open systems. IEEE Computer Society Press, pp 78–94
8. Winslett M, Yu T, Seamons KE, Hess A, Jacobson J, Jarvis R, Smith B, Yu L (2002) Negotiating trust on the web. IEEE Internet Comput 6:30–37
9. Leithead T, Nejdl W, Olmedilla D, Seamons KE, Winslett M, Yu T, Zhang CC (2004) How to exploit ontologies for trust negotiation. In: ISWC workshop on trust, security, and reputation on the semantic web, volume 127 of CEUR workshop proceedings. Technical University of Aachen (RWTH), Hiroshima, Japan
10. Nejdl W, Olmedilla D, Winslett M (2004) PeerTrust: automated trust negotiation for peers on the semantic web. In: Jonker W, Petković M (eds) Secure data management. SDM 2004. Lecture notes in computer science, vol 3178. Springer, Berlin
11. Li N, Winsborough WH, Mitchell JC (2003) Distributed credential chain discovery in trust management. J Comput Secur 11(1):35–86
12. Bonatti PA, De Coi JL, Olmedilla D, Sauro L (2008) Policy-driven negotiations and explanations: exploiting logic-programming for trust management, privacy & security. In: Garcia de la Banda M, Pontelli E (eds) Logic programming. ICLP 2008. Lecture notes in computer science, vol 5366. Springer, Berlin
13. SAML (2005) http://www.oasis-open.org/committees/tchome.php?wgabbrev=security. Accessed 21 Mar 2019
14. WS-Trust (2005) http://www-128.ibm.com/developerworks/library/specification/ws-trust/. Accessed 23 Mar 2019
15. Blaze M, Feigenbaum J, Strauss M (1998) Compliance checking in the policymaker trust-management system. In: Proceedings of the financial cryptography '98. Lecture notes in computer science, vol 1465. Springer, Berlin, pp 254–274
16. Blaze M, Feigenbaum J, Ioannidis J, Keromytis A (1998) The KeyNote trust management system. http://www.cis.upenn.edu/~angelos/keynote.html
17. Chen D, Chang G, Sun D, Li J, Jia J, Wang X (2011) TRM-IoT: a trust management model based on fuzzy reputation for internet of things. Comput Sci Inf Syst 8(4):1207–1228
18. Riloff E, Wiebe J, Phillips W (2005) Exploiting subjectivity classification to improve information extraction. In: Proceedings of the 20th national conference on artificial intelligence
19. Hui Xia ZJ, Ju L, Li X, Zhu Y (2011) A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules. In: IEEE/ACM international conference on green computing and communications
20. Guha R, Kumar R, Raghavan P, Tomkins A (2004) Propagation of trust and distrust. In: WWW '04: Proceedings of the 13th international conference on world wide web. ACM Press, New York, pp 403–412
21. Sabater J, Sierra C (2005) REGRET: a reputation model for gregarious societies. In: Proceedings of the 4th international workshop on deception, fraud and trust in agent societies, in the 5th

international conference on autonomous agents (AGENTS'01). ACM Press, Montreal, Canada, pp 61–69
22. Kamvar SD, Schlosser MT, Garcia-Molina H (2003) The EigenTrust algorithm for reputation management in P2P networks. In: WWW'03: Proceedings of the 12th international conference on world wide web. ACM Press, New York, pp 640–651
23. Ziegler C-N, Lausen G (2005) Propagation models for trust and distrust in social networks. Inf Syst Front 7(4–5):337–358
24. Carbo J, Molina J, Dalliva J (2002) Comparing predication of SPORAS vs fuzzy reputation agent system. In: 3rd international conference on fuzzy system and fuzzy sets
25. Esfandiari B, Chandrasekharan S (2001) On how agents make friends: mechanisms for trust acquisition. In: Proceedings of the fourth workshop on deception, fraud and trust in agent societies, pp 27–34
26. Page L, Brin S, Motwani R, Winograd T (1998) The PageRank citation ranking: bringing order to the web. Technical report, Stanford Digital Library Technologies Project
27. Ziegler C-N, Lausen G (2004) Spreading activation models for trust propagation. In: Proceedings of the IEEE international conference on e-technology, e-commerce, and e-service (EEE'04), Taipei, March
28. Levien R (2004) Attack resistant trust metrics. Ph.D. thesis, University of California at Berkeley
29. Donovan A, Yolanda GA (2007) Survey of trust in computer science and the semantic web. Semant Sci Serv Agents World Wide Web 5(2):58–71
30. Chen IR, Guo J, Bao F (2014) Trust management for SOA-based IoT and its application to service composition. IEEE Trans on Serv Comput 99(1):1
31. Bonatti P, Olmedilla D (2005) Driving and monitoring provisional trust negotiation with metapolicies. In: POLICY '05: proceedings of the sixth IEEE international workshop on policies for distributed systems and networks (POLICY'05). IEEE Computer Society, Washington, DC, pp 14–23
32. Yu T, Winslett M, Seamons KE (2003) Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation. ACM Trans Inf Syst Secur 6(1):1–42
33. Ghorbanimoghaddam M (2015) Trust metrics in recommender systems, a survey. Adv Comput Intell Int J (ACII) 2(3):1245–1257
34. Michele Nitti RG, Atzori L, Iera A, Morabito G (2012) A subjective model for trustworthiness evaluation in the social internet of things. In: 23rd annual IEEE international symposium on personal, indoor and mobile radio communications
35. Liu L, Loper ML, Ozkaya Y, Yasar A, Yigitoglu E (2016) Machine to machine trust in the IoT era. TRUST@AAMAS
36. Bao F, Chen I-R (2012) Dynamic trust management for internet of things applications. Self-IoT'12, San Jose, California, ACM 978-1-4503-1753
37. Jingpei Wang SB, Yu Y, Xinxin N (2013) Distributed trust management mechanism for the internet of things. In: Proceedings of the 2nd international conference on computer science and electronics engineering (ICCSEE 2013)
38. Ben Saied Y, Olivereau A, Zeghlache D, Laurent M (2013) Trust management system design for the internet of things: a context-aware and multi-service approach. Comput Secur 39:351–365. https://doi.org/10.1016/j.cose.2013.09.001
39. Yinan X (2016) A study on trust management algorithms for the social internet of things. Xie yinan school of computer science and engineering, a dissertation submitted in partial fulfilment of the requirement for the degree of master of science in digital media technology
40. Nitti RGM, Atzori L (2014) Trustworthiness management in the social internet of things. IEEE Trans Knowl Data Manag 26(5):1253–1266
41. Marsh S (1994) Formalizing trust as a computational concept. PhD thesis, Department of mathematics and computer science, Sterling University
42. Schillo M, Funk P, Rovatsos M (2000) Using trust for detecting deceitful agents in artificial societies. Appl Artif Intell 14(8):825–848. https://doi.org/10.1080/08839510050127579
43. Castelfranchi C, Conte R, Paolucci M (1998) Normative reputation and the costs of compliance. J Artif Soc Soc Simul 1(3):1–3
44. Fullam KK, Klos T, Muller G, Sabater-Mir J, Barber KS, Vercouter L (2006) The agent reputation and trust (ART) testbed. In: Stølen K, Winsborough WH, Martinelli F, Massacci F (eds) Trust management. iTrust 2006. Lecture notes in computer science, vol 3986. Springer, Berlin

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.