New Concepts for Trust Propagation in Knowledge Processing Systems

Markus Jäger and Josef Küng

Institute for Application Oriented Knowledge Processing (FAW)
Faculty of Engineering and Natural Sciences (TNF)
Johannes Kepler University Linz (JKU), Austria
{markus.jaeger, josef.kueng}@jku.at

Abstract. Everybody has a sense of trusting people or institutions, but how is trust defined? It always depends on the specific field of research and application and is different most of the time, which makes it hard to answer this question in general at a computational level.
Thinking on knowledge processing systems we have this question twice. How can we define and calculate trust values for the input data and, much more challenging, what is the trust value of the output? Meeting this challenge we first investigate appropriate ways of defining trust. Within this paper we consider three different existing trust models and a self developed one.
Then we show ways, how knowledge processing systems can handle these trust values and propagate them through a network of processing steps in a way that the final results are representative. Therefore we show the propagation of trust with the three existing trust models and with a recently self developed approach, where also precision- and importance-values are considered. With these models, we can give insights to the topic of defining and propagating trust in knowledge processing systems.

Keywords: Trust; Propagation; Knowledge Processing Systems; Trust Metrics; Trust Models; Precision; Fusion; Knowledge; Provenance;

1 Introduction

The main subject of our research is the topic of how knowledge processing systems can work with trust values. While going deeper into this research field, several questions arise.

In our work, we try to figure out, **how trust can be defined and measured** and in particular the question of **how knowledge processing systems can deal with trust?** Furthermore we investigate the topic of **how several trust values can be combined (in general and in knowledge processing)** and **how can trust values be propagated through several steps of a knowledge processing system?**

We try to give answers to these questions by investigating possibilities of trust measurement, combination and propagation and try to propose a sound and all-encompassing way of handling these topics.

The rest of this paper is structured as following: section 2 defines common terminologies and shows related work in our field of research.

As the term "trust" has a significant high importance in our research, we dedicated an extra section for defining trust in knowledge processing - section 3. In this section, we investigate different models of measuring or determining trust. We briefly introduce our recently developed and already published approach, where trust- and precision values are handled, processed and propagated by taking into account several importances in section 4.

Section 5 examines the question, how trust can be propagated through knowledge processing systems. Here we cover the different trust measuring models, which were introduced in section 3 and 4 and how trust can be propagated in these different models. Section 6 shows the application of the presented trust propagation models in a scenario. We close this paper with section 7 by giving a summary of our work and an outlook for further research.

2 Related Work

In this section we provide some insights into important terms which are relevant to our work.Furthermore we discuss the fusion of sensor precision values.

2.1 Trust

The meaning of the term "Trust" always depends on the specific environment and field of research and application. In a recent publication about trust, we state: *"The question of 'How can we trust anything/anybody?' is discussed since the beginning of mankind, but what does this topic mean in context to today's technology age and especially for the information technology?"* [11].

The three main types of applicable trust by Rousseau et al. [18] are (1) trusting beliefs, (2) trusting intentions, and (3) trusting behaviours, where these three types are connected to each other.

Another point of view is the similarity of trusting people and trusting technology, especially information technology, where the main difference is within the application of trust in the specific area [16].

Also a very interesting publication about trust in information sources is from Hertzum et al. [9]. They compare the concept of trust between people and virtual agents, based on two empirical studies. Some relational aspects concerning trust in the industrial marketing and management sector can be found in "Concerning trust and information" from Denize et al. [8].

2.2 Provenance

When we come into trust concerning trusting in data and trusting the sources of data, the term "Data Provenance" comes into account. It means the origin and complete processing history of any kind of data. A quite good introduction and overview can be found in [2] and [3].

Several problems concerning data provenance are covered in [5].

Recent research work on provenance can be found in the following literature: "Trust Evaluation Scheme of Web Data Based on Provenance in Social Semantic Web Environments" [19] and "Transparently tracking provenance information in distributed data systems" [4].

"Research of Data Resource Description Method oriented Provenance" [20] and "A semantic Foundation for Provenance Management" [17] provide more theoretical and conceptual foundations for the usage of provenance.

2.3 Risk

Risk in general addresses the potential of losing something with a special personal value. It is also seen as an intentional interaction with uncertainty, where the outcome is hard to predict.

Rousseau et al. [18] say that *"Risk is the perceived probability of loss, as interpreted by a decision maker [...]. The path-dependent connection between trust and risk taking arises from a reciprocal relationship: risk creates an opportunity for trust, which leads to risk taking."*

2.4 Precision & Multi Data Sensor Fusion

The link on related work of fusion precision values in sensor networks can be found in our recent publication "Focussing on Precision- and Trust-Propagation in Knowledge Processing Systems" [12]. The concluding findings are, that sensor fusion is motivated to avoid problems which come from the use of single sensors (e.g. sensor deprivation, limited spatial and temporal coverage, imprecision and uncertainty). Fusion processes in the sensor domain are often categorized in three levels: (1) raw data fusion (low level), (2) feature fusion (medium level), and (3) decision fusion (high level).

3 Defining Trust in Knowledge Processing

The main question in our work is, how knowledge processing systems can handle and work with trust. In this context, the first step is to find a definition of trust, which is suitable for this scientific domain. In this section we investigate different applicable models of measuring or determining trust. Therefore we describe three existing ways: the binary trust model, the probabilistic trust model and the opinion-space trust model.

3.1 Trust, Certainty and Precision in Knowledge Processing

To the best knowledge of the authors, there is no related work dealing with this topic directly – neither for processing trust and certainty, nor for the aggregation of trust, (un)certainty or precision. A good approach for measuring trust is given in [7]. Recent research on modeling uncertainty is given in [15] and in [6].

The propagation/fusion of (sensor) precision values has been evaluated in recent publications, as stated in section 2.4. Some of the investigated propagation/fusion methods of sensor precision values seem quite promising also for the application on trust. Nevertheless we focus on models that cover only trust values, as presented in the following sections.

Another approach is the refactoring of a trust value from a given precision, which will be covered in our future work.

3.2 Binary Trust Model

One of the easiest ways to represent trust values in an understandable and applicable way is the usage of a binary trust model. In this model the possible trust values can either be 0 or 1. Therefore the only differentiation is to fully trust a subject (trust = 1) or not (trust = 0).

In our opinion, the model is very hard to apply in a real world domain because it is very hard to get a trust value of 1 anyway. The definition of possible states in the binary trust model, can be seen in formula 1.

$$T = 0 \ \vee \ 1 \tag{1}$$

Formula 1: Boundaries for the scope of trust in the binary trust model.

3.3 Probabilistic Trust Model

A very application oriented and realistic way of representing trust is the usage of a probabilistic trust model. In this model the possible trust values range from 0 to 1 and can, for example be seen as a type of percentage view. The value of not trusting a subject (trust = 0) and fully trusting a subject (trust = 1 or 100%) is like in the binary trust model, but here the grading can be more precise, as there are (theoretically) infinite states of trust between 0 and 1 (or 100%). The range of possible states of trust in the probabilistic trust model can be seen in formula 2.

$$0 \leq T \leq 1 \tag{2}$$

Formula 2: Boundaries for the scope of trust in the probabilistic trust model.

3.4 Opinion-Space Trust Model

A very well developed model for measuring trust values is the opinion-space model by Audun Jøsang and S.J. Knapskog from 1998: "A Metric for Trusted Systems" [14].

They introduce an *evidence space* and an *opinion space* which are two equivalent models for representing human beliefs, which can be summarized as trust in their model. We focus on the opinion-space trust model, which consists of the values *belief b*, *disbelief d*, and *uncertainty u*. These three values represent

the trust, which is determined. The sum of the three values is always 1, so the interpretation of trust has to be clarified for the current domain of application. The opinion-space trust model can be seen in figure 1.

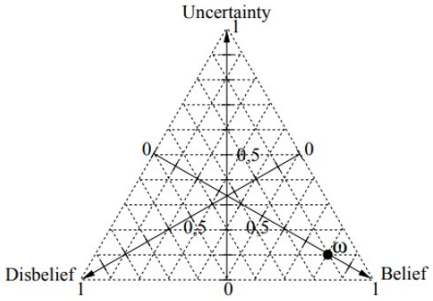

Fig. 1: The opinion-space trust model / opinion triangle from [14].

$$b + d + u = 1, \{b, d, u\} \in [0, 1]^3 \tag{3}$$

Formula 3: Boundaries for the scope of trust in the opinion-space model.

4 Specification of our Approach

In our recent research, we designed a convenient approach for propagating trust and precision values through multi-step knowledge processing systems, where also a factor importance was introduced and considered in the calculation. Our approach was evaluated and published in several conferences before e.g. in [10, 12, 13] and tested on some artificial and real world scenarios.

4.1 Principle Idea

Following, we describe the idea of our approach. The main components are:

- any Source (S), which provides data; there can be multiple sources.
- any Data (D), which is provided by one source; for our model, every source usually provides one or more data (elements).
- any Knowledge Processing System (KPS), which processes data from one or more sources; each KPS itself produces new data as output.

The main values in our approach are:

- Trust value (T) of source (S), which defines how trustable the source is. The system has to be seen as a whole environment, hence the trust level for one source should always be the same.

– Precision value (P) of data (D), which describes how precise, reliable, confident or steady the provided data is.
– Importance value (I) of one input data (D), decided by the current knowledge processing system (KPS) for the current step of computation.

Our approach is sketched in figure 2.

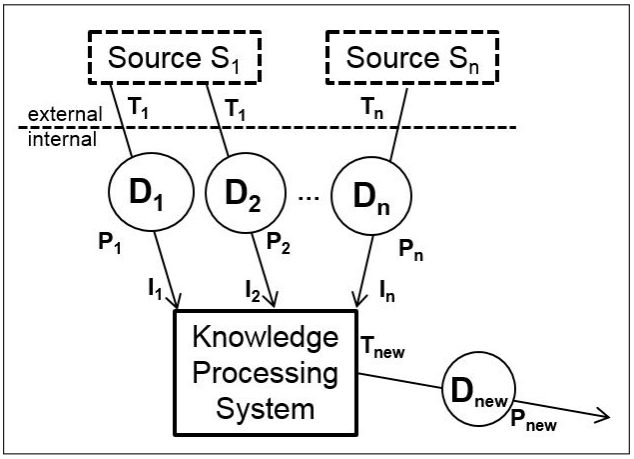

Fig. 2: Graphical description of our approach.

4.2 Scopes & Calculation

In our approach, the scopes of possible values are fixed as following:

– Trust T of source S, for each S, has to be greater than 0 and less or equal than 1, where each value of T for each S has to be the same (if used multiple times) - a higher value represents higher trust:

$$0 < T \leq 1 \tag{4}$$

– Precision P of data D, for each D, has to be greater than 0 and less or equal than 1, where each value of P for each D has to be the same (if used multiple times) - a higher value represents higher precision:

$$0 < P \leq 1 \tag{5}$$

– Importance I of data D, decided by the knowledge processing system:
  • 0.5 for values which are not very important
  • 1.0 for regular values, where no special impact on importance is given
  • 1.5 for very important values, concerning the current data processing

$$I = 0.5 \mid 1 \mid 1.5 \tag{6}$$

5 Propagation of Trust in Knowledge Processing Systems

In this section we compare different methods of fusing and propagating trust values in knowledge processing systems.

5.1 Propagating Trust in the Binary Trust Model

As simple the determination of trust in the binary trust model is, as simple is the propagation of of these values. The only way of a reasonable propagation of binary trust values, is to take the results of the logical conjunction over all values. This means, if only one input value is 0, the output is 0 as well. This can be explained, because it is not justifiable to trust an output of a processing where one input value wasn't trusted.

$$T_{new} = \bigwedge_{i=1}^{n} T_i \tag{7}$$

Formula 7: Calculating T_{new} over all $T_{1\text{-}n}$ in the binary trust model.

5.2 Propagating Trust in the Probabilistic Trust Model

In the probabilistic trust model, several trust values can be fused by multiplying them, presupposed the providing sources are independent.

$$T_{new} = \prod_{i=1}^{n} T_i \tag{8}$$

Formula 8: Calculating T_{new} over all $T_{1\text{-}n}$ in the probabilistic trust model.

5.3 Propagating Trust in the Opinion-Space Trust Model

In this model, a reasonable way of propagation is to consider all input values in the opinion-space trust model. This means that the values of belief, disbelief and uncertainty have to be propagated through the system in a way that the output can again be identified with separate belief, disbelief and uncertainty values again. We propose a very clear way of propagating the three values through a knowledge processing system: using the arithmetic mean for all three separated values to gain the new output values.

$$b_{new}|d_{new}|u_{new} = \frac{1}{n}\sum_{i=1}^{n}(b_i|d_i|u_i) \tag{9}$$

Formula 9: Calculating bdu_{new} over all bdu_{1-n} in the opinion-space trust model.

5.4 Propagating Trust in the Arithmetic Mean Trust Model

This model of propagation is based on our approach, which is presented in section 4. It calculates the propagated trust value based on the input values from the sources, weighted with different important values, which are decided by the knowledge processing system itself individually for every step of processing.

$$T_{new} = \frac{1}{n} \sum_{i=1}^{n} (T_i \times I_i) \tag{10}$$

Formula 10: Calculating T_{new} over all $T_{1\text{-}n}$ related to $I_{1\text{-}n}$ in the arithmetic mean trust model.

6 Scenarios

6.1 Artificial Scenario

The scenario is a complex environment and consists of several knowledge processing systems, where multiple processing steps are taken and where some output values are used as new input values. We introduce six sources (S_1 to S_6) with different trust values (T_1 to T_6), each providing one or two data with different precision values for multiple knowledge processing systems (KPS_A to KPS_E), which weight the different importances. All following calculated propagation models consider the trust values. The usage of the precision- and importance values is only considered in the arithmetic mean trust model of our approach.

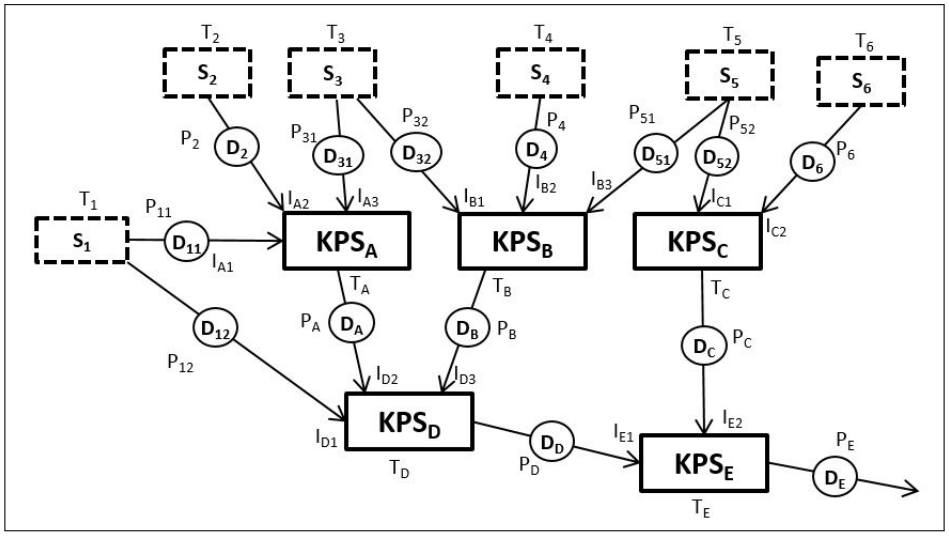

Fig. 3: Artificial Scenario.

Propagation with the binary trust model Table 1 shows the initial trust values in the scenario for propagation with the binary trust model.

Table 1: Artificial Scenario, Binary Trust Model

S_1: T_1=1	S_2: T_2=1	S_3: T_3=1	S_4: T_4=1	S_5: T_5=1	S_6: T_6=0

$$T_A = T_1 \wedge T_2 \wedge T_3 = 1 \wedge 1 \wedge 1 = 1 \quad (11)$$
$$T_B = T_3 \wedge T_4 \wedge T_5 = 1 \wedge 1 \wedge 1 = 1 \quad (12)$$
$$T_C = T_5 \wedge T_6 = 1 \wedge 0 = 0 \quad (13)$$

Applying formula 7 in the calc. 11-13 we get the results for T_A, T_B and T_C.

$$T_D = T_1 \wedge T_A \wedge T_B = 1 \wedge 1 \wedge 1 = 1 \quad (14)$$
$$T_E = T_D \wedge T_C = 1 \wedge 0 = 0 \quad (15)$$

By applying formula 7 in the calculations 14 and 15 from the propagation of trust in the binary trust model, the result is T_{new}=0. Here we notice again the problem of the binary trust model, where only one untrusted input (T_6) ruins the trust in the overall system.

Propagation with the probabilistic trust model Table 2 shows the initial trust values in the scenario for propagation with the binary trust model.

Table 2: Artificial Scenario, Probability Trust Model

S_1: T_1=0.95	S_2: T_2=0.87	S_3: T_3=0.75	S_4: T_4=0.66	S_5: T_5=0.50	S_6: T_6=1.00

$$T_A = T_1 \times T_2 \times T_3 = 0.95 \times 0.87 \times 0.75 = 0.6198 \quad (16)$$
$$T_B = T_3 \times T_4 \times T_5 = 0.75 \times 0.66 \times 0.50 = 0.2475 \quad (17)$$
$$T_C = T_5 \times T_6 = 0.50 \times 1.00 = 0.50 \quad (18)$$

Applying formula 8 in the calc. 16-18 we get the results for T_A, T_B and T_C.

$$T_D = T_1 \times T_A \times T_B = 0.95 \times 0.619 \times 0.247 = 0.1457 \quad (19)$$
$$T_E = T_D \times T_C = 0.14575 \times 0.50 = 0.07287 \quad (20)$$

By applying formula 8 in the calculations 19 and 20 from the propagation of trust in the probabilistic trust model, the result is T_{new}=0.07287 or 7.287%. Again, we recognize the problem of inputs with "lower" trust values (T_4 and T_5) which lead to very low overall trusting outcome, especially in multi step knowledge processing systems.

Propagation with the opinion-space trust model Table 3 shows the initial values for belief, disbelief and uncertainty in the scenario for propagation with the opinion-space trust model.

Table 3: Artificial Scenario, Opinion-Space Trust Model

S_1:	b = 1	d = 0	u = 0
S_2:	b = 0	d = 1	u = 0
S_3:	b = 0	d = 0	u = 1
S_4:	b = 0.3	d = 0.4	u = 0.3
S_5:	b = 0.5	d = 0.5	u = 0
S_6:	b = 0.8	d = 0	u = 0.2

$$b_A = (1+0+0)/3 = 0.\overline{33} \quad (21)$$
$$d_A = (0+1+0)/3 = 0.\overline{33} \quad (22)$$
$$u_A = (0+0+1)/3 = 0.\overline{33} \quad (23)$$
$$b_B = (0+0.3+0.5)/3 = 0.2\overline{66} \quad (24)$$
$$d_B = (0+0.4+0.5)/3 = 0.\underline{3} \quad (25)$$
$$u_B = (1+0.3+0)/3 = 0.4\overline{33} \quad (26)$$
$$b_C = (0.5+0.8)/2 = 0.65 \quad (27)$$
$$d_C = (0+0.5)/2 = 0.25 \quad (28)$$
$$u_C = (0+0.2)/2 = 0.1 \quad (29)$$

Applying formula 9 in the calc. 21-29 we get the results for T_A, T_B and T_C.

$$b_D = (1+0.\overline{33}+0.2\overline{66})/3 = 0.5\overline{33} \quad (30)$$
$$d_D = (0+0.\overline{33}+0.\underline{3})/3 = 0.2\overline{11} \quad (31)$$
$$u_D = (0+0.\overline{33}+0.4\overline{33})/3 = 0.2\overline{55} \quad (32)$$
$$b_E = (0.5\overline{33}+0.65)/2 = 0.591\overline{66} \quad (33)$$
$$d_E = (0.2\overline{11}+0.25)/2 = 0.230\overline{55} \quad (34)$$
$$u_E = (0.2\overline{55}+0.1)/2 = 0.1\overline{77} \quad (35)$$

By applying formula 9 in the calculations 30-35 from the propagation of trust in the opinion-space trust model, the result is b_{new}=$0.591\overline{66}$, d_{new}=$0.230\overline{55}$, and d_{new}=$0.1\overline{77}$. A very mean and realistic result in particular, when we observe the well distributed input values. In our opinion, the outcome is very representative.

Propagation with the arithmetic mean trust model Table 4 shows the initial trust values in the scenario for propagation with the weighted arithmetic mean trust model.

Table 4: Artificial Scenario, Arithmetic Mean Trust Model

S_1: T_1=1.0	D_{11}: P_{11}=0.9	KPS_A: I_{A1}=0.5
S_2: T_2=0.4	D_2 : P_2 =0.3	KPS_A: I_{A2}=1.0
S_3: T_3=0.8	D_{31}: P_{31}=0.8	KPS_A: I_{A3}=1.5
	D_{32}: P_{32}=0.5	KPS_B: I_{B1}=1.0
S_4: T_4=0.2	D_4 : P_4 =0.2	KPS_B: I_{B2}=1.5
S_5: T_5=0.5	D_{51}: P_{51}=1.0	KPS_B: I_{B3}=0.5
	D_{52}: P_{52}=0.7	KPS_P: I_{P1}=1.0
S_6: T_6=0.9	D_6 : P_6 =1.0	KPS_C: I_{C2}=1.0

The calculation steps for this scenario can be found in [10]. The results are T_{new}=0.6625 and P_{new}=0.6875, which are very promising and realistic.

6.2 Agricultural Scenario

Because the scenario from the last subsection is completely artificial, we applied our approach in the course of a project in the agricultural domain funded by the European Union, to have comparable computations.

Therefore, we are now referring to the DPM (Disease Pressure Model, used in the Project CLAFIS [1]) for calculating an accurate daily risk value. This shows how certain a specific disease outbreak for a specific agricultural field can be. The DPM uses input values from a FMIS (farm management information system), which stores information such as this year's and last year's crop as well as the used tillage method. The needed weather data comes from several weather stations, which gathers information, such as temperature, relative humidity, amount of rainfall, and wind speed is gathered. This was a very practical scenario for the application of our approach, where several different trustable sources where used as input. This application of our approach (the weighted arithmetic mean trust propagation model) was evaluated by experts from the agricultural domain and showed very good results. The detailed calculation and evaluation can be found in [10].

7 Summary & Outlook

We addressed the question of how to determine trust values in general and how knowledge processing systems can handle these values in particular. Additionally, we investigated several models for the definition of trust and presented our recently developed approach. Furthermore we showed ways to propagate trust values from the investigated trust models through multi step knowledge processing systems and also a new way of trust propagation from our approach. We gave example calculations on a scenario with all propagation models and compared the results.

Our approach was evaluated in a real world scenario in the frame of a cooperation project with colleagues from practice. An evaluation was done by interviewing experts from this scientific and application domain and the results were encouraging. Our aim is to develop a complete model for incorporating trust, precision and importance values into knowledge processing systems. This approach then could be applied to all other processing systems as well. Such a system, which could be used in a broad variety of applications, definitively would be very useful in practice.

Acknowledgment

The research leading to these results, has received funding partly from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no.604659 in the project CLAFIS and partly from the federal county of Upper Austria.

References

1. CLAFIS: Crop, livestock and forests integrated system for intelligent automation, 2013-2016. EU Seventh Framework Programme NMP.2013.3.0-2.
2. Peter Buneman and Susan B Davidson. Data provenance–the foundation of data quality, 2010.
3. Peter Buneman, Sanjeev Khanna, and Wang-Chiew Tan. Data provenance: Some basic issues. In Sanjiv Kapoor and Sanjiva Prasad, editors, *FST TCS 2000*, volume 1974 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2000.
4. P.C. Castro, M. Pistoia, and J. Ponzo. Transparently tracking provenance information in distributed data systems, August 7 2014. US Patent App. 13/761,916.
5. Wang chiew Tan. Research problems in data provenance. *IEEE Data Engineering Bulletin*, 27:45–52, 2004.
6. Gianpaolo Cugola, Alessandro Margara, Matteo Matteucci, and Giordano Tamburrelli. Introducing uncertainty in complex event processing: model, implementation, and validation. *Computing*, 97(2):103–144, 2015.
7. Chenyun Dai, Dan Lin, Elisa Bertino, and Murat Kantarcioglu. An approach to evaluate data trustworthiness based on data provenance. In *Proceedings of the 5th VLDB Workshop on Secure Data Management*, SDM '08. Springer-Verlag, 2008.
8. Sara Denize and Louise Young. Concerning trust and information. *Industrial Marketing Management*, 2007.
9. Morten Hertzum, Hans H.K Andersen, Verner Andersen, and Camilla B Hansen. Trust in information sources: seeking information from people, documents, and virtual agents. *Interacting with Computers*, 14(5):575 – 599, 2002.
10. Markus Jäger and Josef Küng. Introducing the factor importance to trust of sources and certainty of data in knowledge processing systems - a new approach for incorporation and processing. In *Proceedings of the 50th HICSS*, 2017.
11. Markus Jäger, Stefan Nadschläger, and Nhan Trong Phan. Towards the trustworthiness of data, information, knowledge and KPS in smart homes, IDIMT 2015.
12. Markus Jäger, Jussi Nikander, Stefan Nadschläger, Van Quoc Phuong Huynh, and Josef Küng. Focussing on precision- and trust-propagation in knowledge processing systems. 4th Future Data and Security Engineering. Springer, 2017.
13. Markus Jäger, Trong Nhan Phan, Christian Huber, and Josef Küng. Incorporating trust, certainty and importance of information into knowledge processing systems - an approach. 3rd Future Data and Security Engineering. Springer, 2016.
14. Audun Jøsang and S.J. Knapskog. A metric for trusted systems. 1998.
15. Alexander Karlsson, Björn Hammarfelt, H. Joe Steinhauer, Göran Falkman, Nasrine Olson, Gustaf Nelhans, and Jan Nolin. Modeling uncertainty in bibliometrics and information retrieval: an information fusion approach. *Scientometrics*, 2015.
16. D. Harrison McKnight. *Trust in Information Technology.* The Blackwell Encyclopedia of Management: Operations management. Blackwell Pub., 2005.
17. Sudha Ram and Jun Liu. A semantic foundation for provenance management. *Journal on Data Semantics*, 1(1):11–17, 2012.
18. Denise Rousseau, Sim Sitkin, Ronald Burt, and Colin Camerer. Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 1998.
19. Sangwon Yoon, Kitae Choi, Jaeyeol Park, Jongtae Lim, Kyoungsoo Bok, and Jaesoo Yoo. Trust evaluation scheme of web data based on provenance in social semantic web environments. *Journal of KIISE*, 43(1):106–118, 2016.
20. Yan-peng Zhao, Chao-fan Dai, and Xiao-yu Zhang. Research of data resource description method oriented provenance. In *Proceedings of the 22nd Int. Conf. on Industrial Engineering and Engineering Management 2015*. Springer, 2016.