CertainLogic: A Logic for Modeling Trust and Uncertainty (Short Paper)

Sebastian Ries[1], Sheikh Mahbub Habib[1], Max Mühlhäuser[1], and Vijay Varadharajan[2]

[1] Technische Universität Darmstadt, CASED
Darmstadt, Germany
[2] Macquarie University
Sydney, Australia

Abstract. The evaluation of the trustworthiness of complex systems is a challenge in current IT research. We contribute to this field by providing a novel model for the evaluation of propositional logic terms under uncertainty that is compliant with the standard probabilistic approach and subjective logic. Furthermore, we present a use case to demonstrate how this approach can be applied to the evaluation of the trustworthiness of a system based on the knowledge about its components and subsystems.

1 Introduction

The evaluation of the trustworthiness of complex systems is one of the major challenges in current IT research, as – following the visions of the Internet of Services, the Future Internet and Cloud Computing – IT systems become highly distributed, dynamically composed, and hosted and managed by multiple parties. For example, in the field of Cloud Computing, people and enterprises are still hesitating to *move to the Cloud* due to missing transparency and security concerns. However, it is not only the users who are interested in evaluating the trustworthiness of a service, infrastructure, or platform, but also the providers and accreditation authorities.

Currently, there are several approaches supporting those stakeholders in assessing the trustworthiness of such kind of systems, e.g., from the field of trusted computing, experience-based trust and reputation models, and security [1]. However, for complex systems there is a lack of models that provide means for deriving the trustworthiness of the overall system considering (1) the trustworthiness of the subsystems and atomic components (independently from how these trust values are assessed), (2) the uncertainty associated to this information. For example, reputation values might be based on insufficient information and current solutions from the field of trusted computing cannot effectively capture dynamic changes in trust [2]. Also when considering the recent advances in the field of property-based attestation (e.g., [3]), there is a need for modeling trust and uncertainty in order to deal with the fact that (1) the state of the system that was measured at the time of booting does not necessarily reflect the state of the

system at the time of attestation and (2) that the authority that provides the property certificates might only be trusted to a certain degree [4].

As the core contribution of this paper, we define operators for AND, OR, and NOT for the evaluation of propositional logic terms under uncertainty and we give the properties of these operators. The operators have been designed to be compliant to the standard probabilistic approach and subjective logic [5, 6], which also provides the justification for the mathematical validity of the model. Furthermore, we introduce a use case to show how this approach could be used for evaluating the trustworthiness of a system in a Cloud Computing scenario and to show how the evaluation of the trustworthiness of a complex system relates to the evaluation of propositional logic terms. The paper is structured as follows: Sec. 2 presents the related work, Sec. 3 introduces a use case and Sec. 4 presents the model. Finally, we draw our conclusions in Sec. 6.

2 Related Work

In the field of trust modeling – for a definition of trust see [7] – there is a number of approaches modeling the (un-)certainty of a trust value, well-known approaches are given in [8–11]. However, those approaches do not tackle the issue of deriving the trustworthiness of a system based on the knowledge about its subsystems and components, instead the challenge of these approaches is to find good models for deriving trust from direct experience of a user, recommendations from third parties, and sometimes additional information, e.g. social relationships. Especially, those models aim on providing robustness to attacks, e.g., misleading recommendations, re-entry, Sybil attacks. For those tasks they usually provide operators for combining evidence from different sources about the same target (also called consensus) and for weighting recommendations based on the trustworthiness of the source (also called discounting).

Although, there are researchers in the field of trust focusing on modeling (un-)certainty [5, 9, 12, 13], they do not provide operators for the evaluation of propositional logic terms, except for "subjective logic" [5, 6].

Furthermore, there are well-known approaches for modeling uncertainty outside the trust field. At first, there is the standard probabilistic approach. However, this approach only allows to deal with the uncertainty of the outcome of the next event, but probabilities are assumed to be known.

Fuzzy logic [14] seems to be related, however, it models another type of uncertainty, which could be typed as linguistical uncertainty or fuzzyness.

There is the field of (Dempster-Shafer) belief theory, which again leads to "subjective logic" [5]. The main drawback of this model is that the parameters for *belief*, *disbelief*, and *uncertainty* are dependent on each other, which introduces an unnecessary redundancy from the perspective of modeling and prevents one from re-assign just a single parameter.

Beyond subjective logic there are numerous other approaches for probabilistic reasoning, see e.g. [15]. However, as we argue for the mathematical validity of our model based on its compliance to subjective logic and the standard probabilistic approach, we do not provide a discussion of probabilistic reasoning in general.

Finally, it is possible to model uncertainty using Bayesian probabilities [16], this usually leads to probability density functions, e.g., the Beta probability density function. For the approaches in [5, 13], it has been shown that there are bi-directional mappings between the representations proposed in those papers and the Beta probability density function. It is possible to apply the propositional standard operators to probability density functions, however, this leads to complex mathematical operations and multi-dimensional distributions, which are also hard to interpret and to visualize. In our proposed approach, we will not increase the dimensions when calculating AND and OR.

3 Use Case

We introduce a scenario from the field of Cloud Computing, and show how the evaluation of the trustworthiness of the overall system can be carried out, if there is an appropriate approach for the evaluation of propositional logic terms (see also [17]). We evaluate the trustworthiness of a simple Customer Relationship Management (CRM) system focusing on the availability of the system.

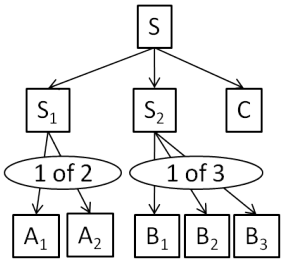

Fig. 1. System architecture (incl. information about redundant components)

In the example (see Fig. 1), the CRM system S directly relies on two subsystems, S_1 providing authentication capabilities, S_2 offering storage capacity for sales data and data mining capabilities, and an atomic component C for the billing. Subsystem $S1$ consist of two authentication servers (A_1 and A_2), where at least one of the servers has to be available. Similarly, subsystem $S2$ is composed of three redundant databases servers (only one needs to be available).

Based on the description above and assuming that the information about the trust values of the atomic components is known, the evaluation of the trustworthiness of the complete system in the context of availability, can be carried out by evaluating the following propositional logic term:

$$(A_1 \vee A_2) \wedge (B_1 \vee B_2 \vee B_3) \wedge C$$

where A_1 is a proposition that is true if the component A_1 behaves as expected (e.g., the component replies to requests within a certain time limit); the interpretations of the other propositions are assigned in the same way. Although, we restricted the scope of our example to availability, please note that it is possible to model statements about the fulfillment of other relevant properties (e.g., attested / self-evaluated security properties or reputation of a component or subsystem) as propositions and to consider them in the evaluation of the overall trustworthiness of the system using propositional logic terms. However, as the knowledge about the fulfilment of the propositions is subject to uncertainty, the evaluation method has to take this uncertainty into account when calculating the trustworthiness of the overall system.

4 CertainLogic

In the following, we introduce a novel model, which we call *CertainLogic*, for evaluating propositional logic terms that are subject to uncertainty. Especially, we define the standard operators of propositional logic: AND, OR, and NOT. However, before introducing these operators, we have to introduce a way for modeling probabilities and uncertainty.

4.1 CertainTrust - Representation

The model for expressing opinions, this is how we call the construction for modeling probabilities that are subject to uncertainty (in accordance with [5]), is called *CertainTrust* [13]. CertainTrust (CT) bas been designed as a representation for evidence-based trust, but may also serve as a representation for uncertain probabilities. Additionally, it supports users with a graphical, intuitively interpretable interface (see [13, 18]).

Definition 4.1 (Representation CertainTrust)
In CertainTrust, an opinion o_A about the truth of a proposition A is given as $o_A = (t, c, f)$ where the parameters are called average rating $t \in [0, 1]$*,* certainty $c \in [0, 1]$*, and* initial expectation value $f \in]0, 1[$*. If it holds $c = 0$ (complete uncertainty), the expectation value (see Def. 4.2) depends only on f, however, for soundness we define $t = 0.5$ in this case.*

The following introduces the basic semantics of the parameters[3]. The *average rating* t indicates the degree to which past observations (if there are any) support the truth of the proposition. It can be associated to the relative frequency of observations supporting the truth of the proposition. The extreme values can be interpreted as follows:

- average rating = 0: There is only evidence contradicting the proposition.
- average rating = 1: There is only evidence supporting the proposition.

The *certainty* c indicates the degree to which the average rating is assumed to be representative for the future. It can be associated to the number of past observations (or collected evidence units). The higher the certainty of an opinion is, the higher is the influence of the average rating on the expectation value in relation to the initial expectation. When the maximum level of certainty ($c = 1$) is reached, the average rating is assumed to be representative for the future outcomes. The extreme values can be interpreted as follows:

- certainty = 0: There is no evidence available.
- certainty = 1: The collected evidence is considered to be representative.

[3]There are additional parameters defined in [13], i.e., the *weight* w of the initial belief, the *number of expected evidence units* N, and a parameter for considering the *age* of evidence. When deriving the parameters (t, c, f) from past evidence, one could assume $w = 1$ and $\lim N \to \infty$. The param. *age* is not directly relevant for this paper.

Table 1. Definition of the operators

OR	$c_{A\vee B} = c_A + c_B - c_A c_B - \frac{c_A(1-c_B)f_B(1-t_A) + (1-c_A)c_B f_A(1-t_B)}{f_A + f_B - f_A f_B}$ $t_{A\vee B} = \begin{cases} \frac{1}{c_{A\vee B}}\left(c_A t_A + c_B t_B - c_A c_B t_A t_B\right) & \text{if } c_{A\vee B} \neq 0\ , \\ 0.5 & \text{else}\ . \end{cases}$ $f_{A\vee B} = f_A + f_B - f_A f_B$
AND	$c_{A\wedge B} = c_A + c_B - c_A c_B - \frac{(1-c_A)\,c_B\,(1-f_A)\,t_B + c_A\,(1-c_B)\,(1-f_B)\,t_A}{1-f_A f_B}$ $t_{A\wedge B} = \begin{cases} \frac{1}{c_{A\wedge B}}\left(c_A c_B t_A t_B + \frac{c_A(1-c_B)(1-f_A)f_B t_A + (1-c_A)c_B f_A(1-f_B)t_B}{1-f_A f_B}\right) & \text{if } c_{A\wedge B} \neq 0, \\ 0.5 & \text{else}\ . \end{cases}$ $f_{A\wedge B} = f_A f_B$
NOT	$t_{\neg A} = 1 - t_A$, $c_{\neg A} = c_A$, and $f_{\neg A} = 1 - f_A$

The *initial expectation* f expresses the assumption about the truth of a proposition in absence of evidence.

The assessment of those parameters can be achieved in multiple ways, e.g., direct assessment by an expert, or derived from a Bayesian reputation system, subjective logic, or a Beta probability distribution.

Definition 4.2 (Expectation value of CT)
The expectation value *of an opinion* $E(t, c, f) \in [0, 1]$ *is defined as* $E(t, c, f) = t * c + (1 - c) * f$.

It expresses the expectation about the truth of the proposition taking into account the initial expectation, the average rating and the certainty.

4.2 Logical Operators

Having introduced the representational model, we define the operators of propositional logic (OR, AND, and NOT). These operators are defined in a way that they are compliant with the evaluation of propositional logic terms in the standard probabilistic approach. However, when combining opinions, those operators will especially take care of the (un-)certainty that is assigned to its input parameters, and reflect this (un-)certainty in the result.

Operator *OR* The operator OR is applicable when opinions for two independent propositions need to form a new opinion reflecting the degree of truth for at least one out of both propositions.

Definition 4.3 (Operator OR)
Let A and B be two independent propositions and the opinions about the truth of these propositions be given as $o_A = (t_A, c_A, f_A)$ and $o_B = (t_B, c_B, f_B)$, respectively. Then, the resulting opinion is denoted as $o_{A\vee B} = (t_{A\vee B}, c_{A\vee B}, f_{A\vee B})$ where $t_{A\vee B}$, $c_{A\vee B}$, and $f_{A\vee B}$ are defined in Table 1 (OR). We use the symbol $'\vee'$ to designate the operator OR and we define $o_{A\vee B} \equiv o_A \vee o_B$.

Operator *AND* The operator AND is applicable when opinions for two independent propositions need to be aggregated to produce a new opinion reflecting the degree of truth of both propositions simultaneously.

Definition 4.4 (Operator AND) *Let A and B be two independent propositions and the opinions about the truth of these propositions be given as $o_A = (t_A, c_A, f_A)$ and $o_B = (t_B, c_B, f_B)$, respectively. Then, the resulting opinion is denoted as $o_{A\wedge B} = (t_{A\wedge B}, c_{A\wedge B}, f_{A\wedge B})$ where $t_{A\wedge B}$, $c_{A\wedge B}$, and $f_{A\wedge B}$ are defined in Table 1 (AND). We use the symbol $'\wedge'$ to designate the operator $'AND'$ and we define $o_{A\wedge B} \equiv o_A \wedge o_B$.*

Operator *NOT* The operator NOT is applicable when an opinion about an proposition needs to be negated.

Definition 4.5 (Operator NOT)
Let A be a proposition and the opinion about the truth of this proposition be given as $o_A = (t_A, c_A, f_A)$. Then, the resulting opinion is denoted as $\neg o_A = (t_{\neg A}, c_{\neg A}, f_{\neg A})$ where $t_{\neg A}$, $c_{\neg A}$, and $f_{\neg A}$ are given in Table 1 (NOT). We use the symbol $'\neg'$ to designate the operator NOT and we define, $o_{\neg A} \equiv \neg o_A$

The operators for AND and OR are commutative and associative. The proofs for Theorem 4.1 and Theorems 4.2 are given in [19].

Theorem 4.1 (Commutativity)
It holds $o_{A\wedge B} = o_{B\wedge A}$ and $o_{A\vee B} = o_{B\vee A}$

Theorem 4.2 (Associativity)
It holds $o_{A\wedge(B\wedge C)} = o_{(A\wedge B)\wedge C}$ and $o_{A\vee(B\vee C)} = o_{(A\vee B)\vee C}$.

The operators are *not distributive*, i.e., it does not hold that $o_{A\wedge(B\vee C)} = o_{(A\wedge B)\vee(B\wedge C)}$, as $A \wedge B$ and $A \wedge C$ are not independent propositions. Finally, it can be shown that the evaluation of the operators is compliant to the standard probabilistic approach as well as to subjective logic (see [19]).

5 Evaluation of the Use Case

In this section, we show how the operators of CertainLogic can be applied to the use case presented in Section 3. The propositional logic term for evaluating the trustworthiness of the system in the use case has been given as $(A_1 \vee A_2) \wedge (B_1 \vee B_2 \vee B_3) \wedge C$.

For the evaluation, we assume that we have good knowledge about the components of subsystem S_1 (consisting of A_1 and A_2) and subsystem S_2 (consisting of B_1, B_2, and B_3) and that the components are highly available. The opinions for the components as well as for the resulting subsystems are given in table 2. In both cases, the subsystems are highly trustworthy ($E(o_{S_1}) = 0.9963$ and $E(o_{S_2}) = 0.9964$) and the certainty for both systems is high.

Table 2. Resulting opinions for S_1 (left) and S_2 (right)

o_{A_1}	$(0.90, 0.98, 0.5)$
o_{A_2}	$(0.99, 0.95, 0.5)$
$o_{A_1 \vee A_2} = o_{S_1}$	$(0.9974, 0.9956, 0.75)$

o_{B_1}	$(0.9, 0.8, 0.5)$
o_{B_2}	$(0.95, 0.8, 0.5)$
o_{B_3}	$(0.9, 0.9, 0.5)$
$o_{B_1 \vee B_2 \vee B_3} = o_{S_2}$	$(0.9978, 0.9894, 0.875)$

We show the advantage of the new operators presenting different scenarios regarding the trustworthiness of the atomic component C. Depending on whether the component is hosted by the owner of the overall system or by a third party, the certainty about the behavior of this component might be higher or lower. Here we consider two cases:

Case 1: We assume that the trustworthiness of C is given as $o_C = (0.9, 0.9, 0.5)$ [*high certainty*] or as $o_C = (0.9, 0.1, 0.5)$ [*low certainty*]. For this case, the trustworthiness of the overall system S (consisting of S_1, S_2, and C) are given in Table 3 (left). In the first row, we see that the *high certainty in* o_C is also reflected in the resulting opinion ($c_S = 0.9229$), whereas the *low certainty in* o_C is reflected in the resulting opinion ($c_S = 0.3315$) in the second row. In this example, we have different expectation values for o_C (depending on the certainty), and thus also different expectation values for o_S.

Case 2: We assume that the trustworthiness of C is given as $o_C = (0.9, 0.9, 0.9)$ [*high certainty*] or as $o_C = (0.9, 0.1, 0.9)$ [*low certainty*]. Here, both opinions lead to the same expectation value. The expectation value for the trustworthiness of the overall system is also the same (due to the compliance with the standard probabilistic approach). However, in our approach the different values for the certainty in the input parameters are still visible in the final result, for the certainty it holds $c_S = 0.9704$ [*high certainty*] and $c_S = 0.7759$ [*low certainty*] (see Table 3 (right)).

Table 3. Resulting opinions for S – Case 1 (left) & Case 2 (right)

	o_C	$o_{S_1 \wedge S_2 \wedge C} = o_S$
high certainty	$(0.9, 0.9, 0.5)$	$(0.8978, 0.9229, 0.3281)$ $E(o_S) = 0.8538$
low certainty	$(0.9, 0.1, 0.5)$	$(0.9556, 0.3315, 0.3281)$ $E(o_S) = 0.5361$

	o_C	$o_{S_1 \wedge S_2 \wedge C} = o_S$
high certainty	$(0.9, 0.9, 0.9)$	$(0.9028, 0.9704, 0, 5906)$ $E(o_S) = 0.8935$
low certainty	$(0.9, 0.1, 0.9)$	$(0.981, 0.7759, 0.5906)$ $E(o_S) = 0.8935$

6 Conclusion

In this paper, we proposed a novel model for the evaluation of propositional logic terms under uncertainty. The operators for AND and OR can be shown to be associative and commutative, which is essential for the evaluation of propositional logic terms. Additionally, the operators can be shown to be compliant with the standard probabilistic evaluation of propositional logic terms and with subjective logic, which finally provides the justification for the mathematical validity of our model. However, the proposed approach is more expressive than the standard probabilistic approach, and although it is as expressive as subjective logic, it provides a simpler representation since it is based on independent parameters and it provides a more intuitive and more expressive graphical representation.

Finally, we have briefly indicated how the model can be applied when evaluating the trustworthiness of a system in a Cloud Computing scenario. The model provides a means (1) to derive the trustworthiness of the overall system based on the knowledge about its components, (2) to take into account multiple criteria (modeled by propositions), and (3) to explicitly model the uncertainty associated to the truth of a proposition. Thus, we consider this approach an appropriate, expressive, and well-founded tool for the evaluation of the trustworthiness of complex systems.

While we have used the Cloud Computing scenario as a descriptive example, the model could also be used for reasoning under uncertainty in other fields such as those involving contextual information. Such information is also subject to uncertainty; for instance, information collected by sensors.

References

1. Schneier, B.: Attack trees: Modeling security threats. Dr. Dobb's journal **24** (1999)
2. Varadharajan, V.: A note on trust-enhanced security. IEEE Security and Privacy **7** (2009) 57–59
3. Sadeghi, A., Stüble, C.: Property-based attestation for computing platforms: caring about properties, not mechanisms. Workshop on New security paradigms, (2004)
4. Nagarajan, A., Varadharajan, V.: Dynamic trust enhanced security model for trusted computing platform based services. Future Generation Comp. Sys. (2010)
5. Jøsang, A.: A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems **9**(3) (2001) 279–212
6. Jøsang, A., McAnally, D.: Multiplication and comultiplication of beliefs. International Journal of Approximate Reasoning **38(1)** (2005) 19–51
7. Gambetta, D.: Can we trust trust? In Gambetta, D., ed.: Trust: Making and Breaking Cooperative Relations. Basil Blackwell, New York (1990) 213–237
8. Buchegger, S., Le Boudec, J.Y.: A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks. In: P2PEcon 2004. (2004)
9. Teacy, W., et al.: Travos: Trust and reputation in the context of inaccurate information sources. Aut. Agents and Multi-Agent Systems **12**(2) (2006) 183–198
10. Jøsang, A., Ismail, R.: The beta reputation system. In: Proceedings of the 15th Bled Conference on Electronic Commerce. (2002)
11. Ries, S., Heinemann, A.: Analyzing the robustness of CertainTrust. In: 2nd Joint iTrust and PST Conf. on Privacy, Trust Management and Security, (2008) 51 – 67
12. Wang, Y., Singh, M.P.: Formal trust model for multiagent systems. In: Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI). (2007)
13. Ries, S.: Extending bayesian trust models regarding context-dependence and user friendly representation. In: ACM Symp. on Applied Computing, (2009) 1294–1301
14. Zadeh, L.A.: Fuzzy logic and approximate reasoning. Synthese **30** (1975) 407–428
15. Haenni, R.: Towards a unifying theory of logical and probabilistic reasoning. In: 4th Int. Symp. on Imprecise Probabilities and Their Applications. (2005) 193–202
16. Bolstad, W.M.: Introduction to Bayesian Statistics. John Wiley & Sons, Inc (2004)
17. Schryen, G., Volkamer, M., Ries, S., Habib, S.M.: A formal approach towards measuring trust in distributed systems. In: ACM Symp. on Applied Comp. (2011)
18. Ries, S.: Trust in Ubiquitous Computing. PhD thesis, Technische Universität Darmstadt (2009)
19. Ries, S., Habib, S.M., Mühlhäuser, M., Varadharajan, V.: CertainLogic: A Logic for Modeling Trust and Uncertainty. Technical report, Technische Universität Darmstadt (2011)