

Trust Modelling in E-Commerce through Fuzzy Cognitive Maps

Christian Schläger and Günther Pernul

Department for Information Systems, University of Regensburg, Germany

christian.schlaeger@wiwi.uni-regensburg.de, guenther.pernul@wiwi.uni-regensburg.de

Abstract

Trust and its role in e-commerce is a major topic for researchers, clients, and service providers alike. However, questions of origin and practical usage of trust in e-commerce are still not answered. Two eminent obstacles in the integration of information on trust and reputation are limited data about customers, and a missing fine grained access control model. The first hindrance is shrinking as users generate personal data in the Web 2.0 as they go (or rather surf). The aim of this paper is to show potentials for e-commerce federations using an attribute-based authentication and authorisation infrastructure to use customer information for the derivation of metric trust and reputation values. Using Fuzzy Cognitive Maps and trust metrics, a prototype integrates a federation's user data within an easy to use service provider interface for reputation management. To assure user privacy the data is categorised and stored distributedly.

1. Introduction and Motivation

A trust decision in the online-world can so far only take into consideration a subset of the information available in traditional business transactions. For electronic transactions trust must be assessed metrically. This poses another challenge on the derivation of such values as trust is normally given in a qualitative manner only. The origin of trust values has been addressed in many research fields, ranging from psychology to mathematics without having a common understanding [3]. All of them agree, however, that dynamic changes and a large information base are needed to compute any kind of "trust" [1]. Trust will gain momentum for e-commerce providers if it can be used as a tool for enhanced IT security and personalisation. Consequently, an interface is needed that lets vendors decide on what "trust" means for them or in other terms what attributes a user needs to present if he wants access on reserved goods and services. Two typologies of trust are especially helpful for defining trust in e-commerce: The work by McKnight and

Chervany from 2001 [1] and a more technical study by Viljanen from 2005 [4].

Coetzee and Eloff introduced in [5] how trust can be used to administer web service access. They used Fuzzy Cognitive Maps (FCMs) to compute a metric trust value from the client's information artefacts. Such information artefacts originate at large in Web 2.0 applications connecting various service providers and their applications. Technologies like attribute-based access control (ABAC) can make use of such values. Infrastructures enforcing such access control decisions and managing trust calculation and assessment will be the key to integrate trust in modern e-commerce. E-commerce service providers are familiar with such infrastructures usually referred to as AAI (Authentication and Authorisation Infrastructures).

This work proposes an enhancement of attribute-based AAI for e-commerce federations. Using FCMs and a federation's data a metric trust value is computed based on the approach by Coetzee and Eloff [5]. The needed metric trust value is derived by an adopted trust definition for e-commerce by McKnight and Chervany [1]. As a basis, an AAI with attribute-based access control is used as presented by Schläger et al. in 2006 [2].

This paper is structured as follows. In section 2 related work is given. Section 3 explains how FCMs can be used for trust computation. Consecutively, the use for e-commerce applications is explained. An enhancement of AAI with these trust values and the corresponding prototype are introduced in section 5. The paper finishes with a conclusion and an outlook.

2. Related Work

In the course of previously published work on XACML (eXtensible Access Control Modelling Language) and especially attribute-based access control in e-commerce such as [2] or [6], questions of origin and meaning of user attributes were raised. Trust clearly is an influencing factor that plays an important role in brick-and-mortar business as well as in all personal transactions. If attribute-based access control

aims to enable e-commerce transactions with fine grained, flexible, and user tailored privileges it is imperative for ABAC to replicate “trust” as a dynamic information artefact.

2.1 Trust

In 2001 McKnight and Chervany started a conceptualisation and typology of trust definitions over various research fields ranging from sociology, over psychology to economics. Sixteen characteristics of trust were identified. The various trust definitions and assessment methods used attributes from categories such as competence, predictability, or integrity. Mapping concepts and categories they accordingly built an interdisciplinary model consisting of four trust constructs (see grey shaded boxes in Figure 1): *Disposition to Trust*, *Institution-based Trust*, *Trusting Beliefs*, and *Trusting Intention*. “Disposition to Trust” is an entity’s general intent to trust someone.

All of the mentioned trust constructs influence each other [7] and result in a “Trusting Intention”. “Trusting Intention” for [1] sums up to a person’s tendency to trust a specific counterpart in a specific situation to behave without malicious intent.

Obviously, the deducted model is still fuzzy in the definitions of trust and cannot be assigned metrical values. In addition, it is too general to be used without major alterations for e-commerce environments. Without going further into detail, McKnight and Chervany extended their model by e-commerce specific information resulting in changes for the two concepts of “Trusting Belief” and “Trusting Intention” affecting, finally, the behaviour of an e-commerce entity. The e-commerce adaptations are shown in Figure 1 in the white boxes.

In [1] trust is defined generally as trust between two entities, regardless of their role. Implicitly, however, McKnight looks at trust in e-commerce from a customer side rather than from an impartial side. This

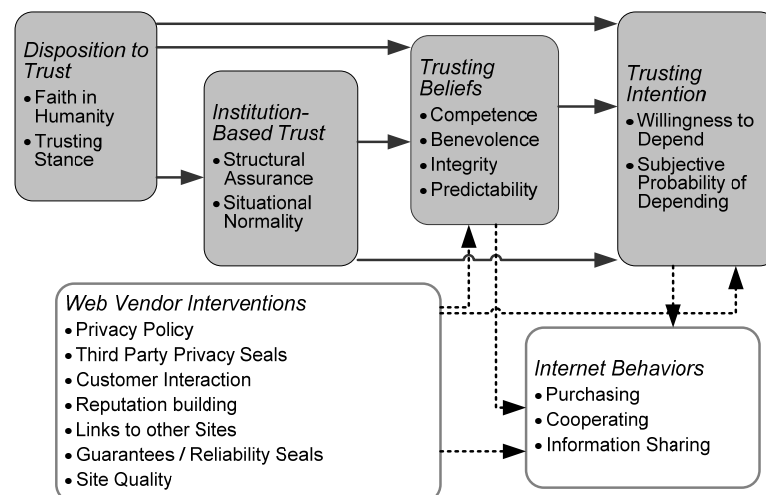


Figure 1: Interdisciplinary trust constructs model (shaded) with e-commerce relations by [1]

“Institution-based Trust” indicates the security given by the environment. This can be influenced by legal assurance because of applying contracts, laws, and warranties. In addition to legal institutions contributing to this definition of trust, McKnight and Chervany also subsume the effects of familiar situations. A situation is more trusted if processes and appearance are known and users are accustomed to a good outcome. Where “Institution-based Trust” aims at the situation, “Trusting Beliefs” refers to the person one is interacting with. Influencing factors are integrity, competence, benevolence, and especially predictability.

is obvious looking at the behavioural options in Figure 1 and in line with previously published work [8]. In this article, trust is defined as trust between vendors and customers, where a vendor needs a certain level of trust in the customer to grant certain privileges. Our view of trust is closely connected to reputation. A customer with a higher reputation is more trusted.

2.2 Fuzzy Cognitive Maps

Concentrating on the practical relevance of trust, Coetzee and Eloff [5] define trust simply by three requirements. Firstly, trust needs to reduce a decision’s

complexity. Secondly, trust is built of different concepts. All concepts and corresponding elements need to be mathematically processable. All connections and relations need to be defined. Thirdly, trust results from a computation of objective information.

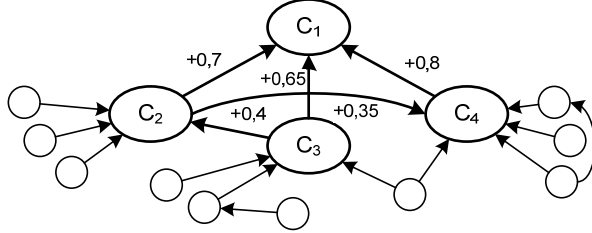


Figure 2: Fuzzy Cognitive Map

Using these three axioms Coetzee and Eloff are able to map trust in Fuzzy Cognitive Maps (FCM). FCMs consist of nodes, connected by signed and weighted arcs [9]. The root of an FCM can be seen as the final trust value (C_1 in Figure 2). Each node resembles the information needed to compute that value or an already computed subset of the final trust value (e.g. $C_2 - C_4$).

information can be assessed in an ordinal value ranging in an interval between 0 and 1. This information can be computed by FCMs. [5] have used FCMs for the computation of web service trust.

2.3 Authentication and Authorisation Infrastructures in E-Commerce

In 2006 [2] have introduced an attribute-based authentication and authorisation infrastructure usable for e-commerce providers and customers. The AAI is able to form a federation of service providers in which attributes about customers can be exchanged. Unlike existing frameworks like Microsoft's .Net Passport or Liberty's ID-FF the proposed architecture uses user, resource, and environmental attributes together with policies to come to an access control decision. The authors presented a reference model able to mediate between user and provider demands [11] and gaining functionalities on existing solutions. The security sub-services and the access process are depicted in Figure 3.

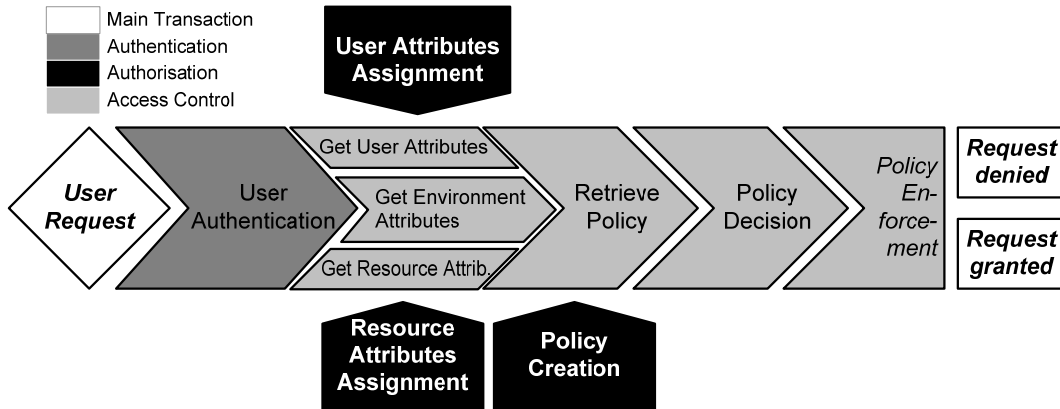


Figure 3: AAI security sub-services [2]

Each node represents a value in the interval $[0, 1]$. The arcs are weighted according to the impact of one node on another. Normally, this impact must be in the interval $[-1, +1]$.

Let A be the value assigned to one node and e_{ij} the weighted arc between A_i and A_j with A_j being the predecessor of A_i . The value of A_i can be computed with the help of (1) [10].

$$A_i = f\left(\sum_{j=1}^n A_j e_{ij}\right) \quad (1)$$

However, information that affects trust can often not be specified in a metrical value. Mostly, trust

As explained in detail in [12] AAI's are able to respect the user's privacy by successfully separating identity information and attributes through special sub-service allocation. Open questions in the proposed work were the origin and computation of user attributes. User attributes could entitle a trust or reputation value resulting from user data and buying behaviour gathered in a federation of providers.

3. Using FCM for Trust Computation

As the proposed reference model in [2] uses XACML policies the trust attribute can either be a

binary or a metrical value. In the first case the existence or non-existence of “trust” would grant or deny access. For the second case more complex policies like categories or thresholds would be possible. With FCMs a metrical value can be computed.

Taken the scenario of an e-commerce transaction in an AAI, we first have to define what information is available on the subject (in this case the user or customer). Attributes range in three categories: mere identifiers, explicit user data, and inferred user data. The latter cannot be given by the user himself but needs to be computed from his customer history [see for example 13].

Fuzzy Cognitive Maps can use attributes ranging in the category of explicit and implicit data to compute an individual trust value. Before computation every value needs to be categorised in the interval [0, 1]. Metrical input data (like “Turnover in EUR in this time period”) must be normalised, ordinal or by nature fuzzy data (e.g. “Classification of Housing Region” or “Customer Loyalty”) must be assigned normalised metrical values in the interval. Binary data (e.g. “Ongoing Insolvency”) is valued as 1 or 0.

Using the trust typology of [1] as explained in

in the notion of “Trusting Beliefs”. Figure 4 depicts these four sub-categories and included user attributes. Attributes have been chosen as examples only. The given list of 15 user attributes is neither mutual exclusive nor exhaustive. Ideas for attributes were taken from [1, 5, 13-18].

Most attributes are self-explaining. Among the metrical values that need to be normalized are turnovers or household income. Note that one might consider an attribute like “ongoing insolvency” - if positive - as an exclusionary factor. Indeed, recently published work by McKnight and Chervany [17] suggest that such exclusion criteria might lead to a disposition to distrust and that such a disposition might be far more relevant for e-commerce scenarios. However, the notion of negative attributes is not realistic for an open scenario. As explained in [19] a user misbehaving in a federation would do so intentionally and thus know about the negative attributes he or his pseudonym carries. As a consequence a malicious user would change his pseudonym or identity immediately afterwards. Accordingly, the idea of distrust is not useful as such in open e-commerce environments.

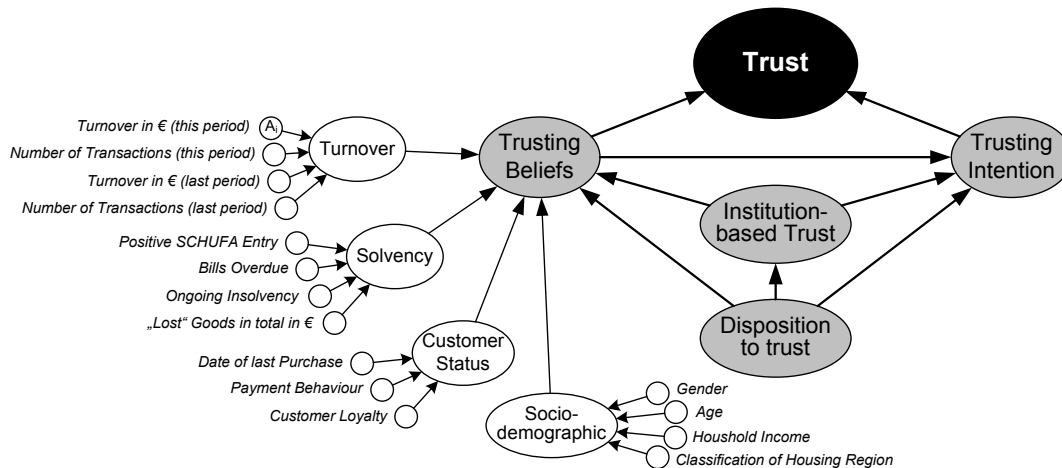


Figure 4: Adapted trust typology for e-commerce with FCM computation

section 2.1 and transforming it into an FCM a tree evolves as given in Figure 4. The different trust constructs are shaded in grey. Relations are given by yet unweighted arcs.

Making the abstract model usable for e-commerce environments and using data that can be gathered in an AAI federation the authors enhance the constructs by four sub-constructs: customer turnover, solvency, customer status, and socio-demographic factors. In accordance with [1] these sub constructs are weighted

4. Using Trust Values in E-Commerce Service Providing

In contrast to [17], the author’s idea of trust-attributes rather is that of an incentive system. Vendors and service providers have an intrinsic mistrust of customers that can be changed to a positive trust level by provided attributes and meta-information. A user that earned an SP’s trust or has a good reputation is

able to access a higher service level - such as special terms of payment or a discount. This system of reputation is already in use at service providers with a large customer base. However, this data is not exchanged with others. A federation of service providers offers the chance to exchange data over the federation in specified formats and semantics. A suitable standard is SAML [20], as used in the reference model of [2].

4.1 Attribute-based Access Control with XACML

Attribute-based access control can be set into practice by the OASIS' open standard XACML [21] – the extensible access control modelling language. XACML uses rules, aggregated to policies, to decide with resource, environment, and user attributes on access. A policy decision point (PDP) uses the service provider's policy together with the accumulated attributes for the access control decision. The enforcement is handled by the PEP- the policy

he could issue a policy ruling that a turnover up to 5.000 EUR qualifies for the bronze category. Turnover up to 10.000 EUR would qualify as silver category and so on. Each category is then assigned a value in the interval of [0, 1]. The node A_i "Turnover in EUR (this period)" in Figure 4 would hence be initiated with this value (e.g.: $A_i(\text{bronze}) = 0.3$, $A_i(\text{silver}) = 0.5$, ...). In addition to this categorisation the company needs to specify the weighted arcs in a FCM. Depending on the weight the information of A_i is valued in the final trust value. Let $e_{\text{Turnover}, \text{TrustingBeliefs}}$ be the weight of the arc from A_{Turnover} to $A_{\text{TrustingBeliefs}}$. e must be in the interval of [0, +1].

For our prototype an interface has been constructed depicting all possible information artefacts of users in the federation. A company can assign categories for each artefact and weight the FCM's arcs accordingly. Of course a standard categorisation is provided. The evolving policy is stored as an XML file at the computing server. The trust value of user α would be computed as given in (2) – (5).

$$A_{\text{Turnover}(\text{thisPeriod})}^{\alpha} = \begin{cases} 0.3 & \text{for } \text{Turnover}(\text{thisPeriod}) \leq 5.000 \\ 0.5 & \text{for } 5.000 < \text{Turnover}(\text{thisPeriod}) \leq 10.000 \\ 0.7 & \text{for } 10.000 < \text{Turnover}(\text{thisPeriod}) \leq 15.000 \\ 1.0 & \text{for } \text{Turnover}(\text{thisPeriod}) > 15.000 \end{cases} \quad (2)$$

$$A_{\text{Turnover}}^{\alpha} = A_{\text{Turnover}(\text{thisPeriod})}^{\alpha} \cdot e_{\text{Turnover}(\text{thisPeriod}), \text{Turnover}} + \dots \quad (3)$$

$$A_{\text{TrustingBeliefs}}^{\alpha} = A_{\text{Turnover}}^{\alpha} \cdot e_{\text{Turnover}, \text{TrustingBeliefs}} + \dots \quad (4)$$

$$A_{\text{Trust}}^{\alpha} = A_{\text{TrustingBeliefs}}^{\alpha} \cdot e_{\text{TrustingBeliefs}, \text{Trust}} + A_{\text{TrustingIntention}}^{\alpha} \cdot e_{\text{TrustingIntention}, \text{Trust}} \quad (5)$$

enforcement point. In an AAI as presented by [2] the PEP is located at the SP. It enforces the decision of the distributed PDP locally. The attributes are requested at all SPs knowing the user in question. For performance reasons not all user information should be transmitted but a classification of the user. This categorisation can be e.g. by a scale of bronze, silver, gold, to platinum users. Such a categorisation can be done via an FCM. In addition to performance issues user privacy can be protected by such a categorisation as well.

4.2 Trust Value Computation

Provided enough user data exists in the federation the FCM in section 3 needs to be initiated for computation. The requested SP uses a policy of his own to decide on the meaning of abstract information artefacts. Taken the example of turnover in this period

4.3 Privacy Issues

Obviously user data is computed that is highly personal and must be protected. The idea of freely distributing user information like buying patterns or other personal information artefacts without limitations must be rejected from a legal as well as from a privacy and data security perspective. Privacy enhancing technologies (PET) can be used to respect privacy issues. In accordance with [22] we use trust computation mechanism as a PET, relying on categorisation, distribution, and filtering.

The prototype computes the trust value at the PDP. The PDP is only aware of the information artefacts and the SP's policy. Attributes are separated from the user's identity. More privacy can be achieved by letting each Service Provider compute a trust categorisation (e.g. categorising the customer as

bronze, silver, etc.) by itself and exchanging categorisations only. However, this approach would require a strong trust relationship between all federation members.

5. Enhancing AAI with FCM Trust Values

Building on the work of [11] and [2] we use the prototype of an attribute-based AAI providing services as depicted in Figure 3. The prototype's UML sequence diagram is given in Figure 5. Process steps are labelled using SAML and XACML nomenclature.

In this scenario at least four entities interact. User α requests resource ρ at SP-1 and is redirected to his

information artefacts of α are now processed using an FCM. SP-1's settings are derived from the appropriate XML file and a trust value is computed. This is used for the AC decision together with attributes on ρ and environment information ε . ρ and ε attributes are fetched from SP-1. The AC decision is enforced by the Policy Enforcement Point (PEP) of SP-1. Note that the user's identity is not revealed. Instead an opaque identifier β is used. This is another integrated PET.

In the course of our work a prototype was developed. SPs can personalise the initial set up of the FCM as well as the specific weight of the FCM's arcs. An according screenshot is given in Figure 6 at the end of this paper.

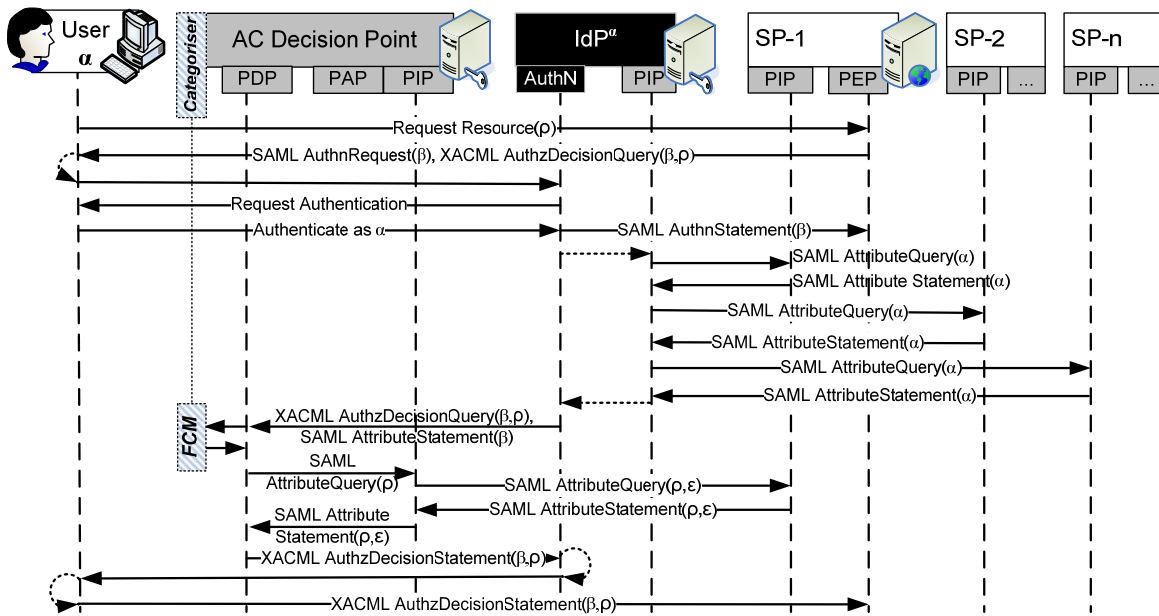


Figure 5: Attribute-based AAI by [2] enhanced with FCM categorisation

Identity Provider (IdP $^{\alpha}$). We assume that the user had the choice between various IdPs using the one he trusts. If authenticated, IdP $^{\alpha}$ accumulates the user's attributes. Every SP (including SP-1) is asked for information artefacts on α . The information exchange is done via SAML tokens (for more information on SAML in AAI see [19, 20, 23]) by the respective Policy Information Points (PIP). Finally, the IdP is in possession of all available information artefacts on α . The last entity involved is a central access control (AC) decision point, a trusted third party – TTP. The aforementioned PDP is hosted on this server together with the Policy Administration Point (PAP). As identity information and attributes were separated by IdP $^{\alpha}$ the PDP decides about the decision on attributes only. This can be seen as a powerful PET. The

Trust value computation is an example of the derivation of security related attributes. Neither [5] nor previously published work on AAI have given satisfying solutions on the problem of transferring general information artefacts into security related attributes. The AAI needs to transform these artefacts for an access control decision. Due to the distributed character of AAI this information needs to be accumulated and exchanged. These abstract processes in an AAI have been made tangible with specific standards and technologies.

Responsible for the user attributes are the SPs and the IdP. The exchange of security information and the semantics are provided by the AAI. The computation of the trust value is done at the AC decision point (being a TTP). The decision is computed by the PDP.

The enforcement is done by the SP.

6. Conclusion and Future Work

To our knowledge, this work presents the first integration of metrical trust values in attribute-based AAs for e-commerce. This is done by using fuzzy cognitive maps. The derivation of attributes bases on the work of [1]. Through the adoption of an infrastructure SP's on the Internet can exchange information artefacts of customers benefiting of the accumulated knowledge in the federation.

Our research answers the raised questions of attribute origins in AAs as well as of the impact of trust research on e-commerce. The usually limited information base is bypassed. In addition to trivial AC decisions like age attributes ruling access on rated materials, reputation can now be used for offers and personalisation. Additionally, categorisation and FCM computation can be used as PETs. The proposed architecture mediates between privacy issues and e-commerce security for Service Providers.

Future Work will encompass different allocation strategies, e.g. research on architectures categorising attributes at SP-level before the accumulation by the IdP.

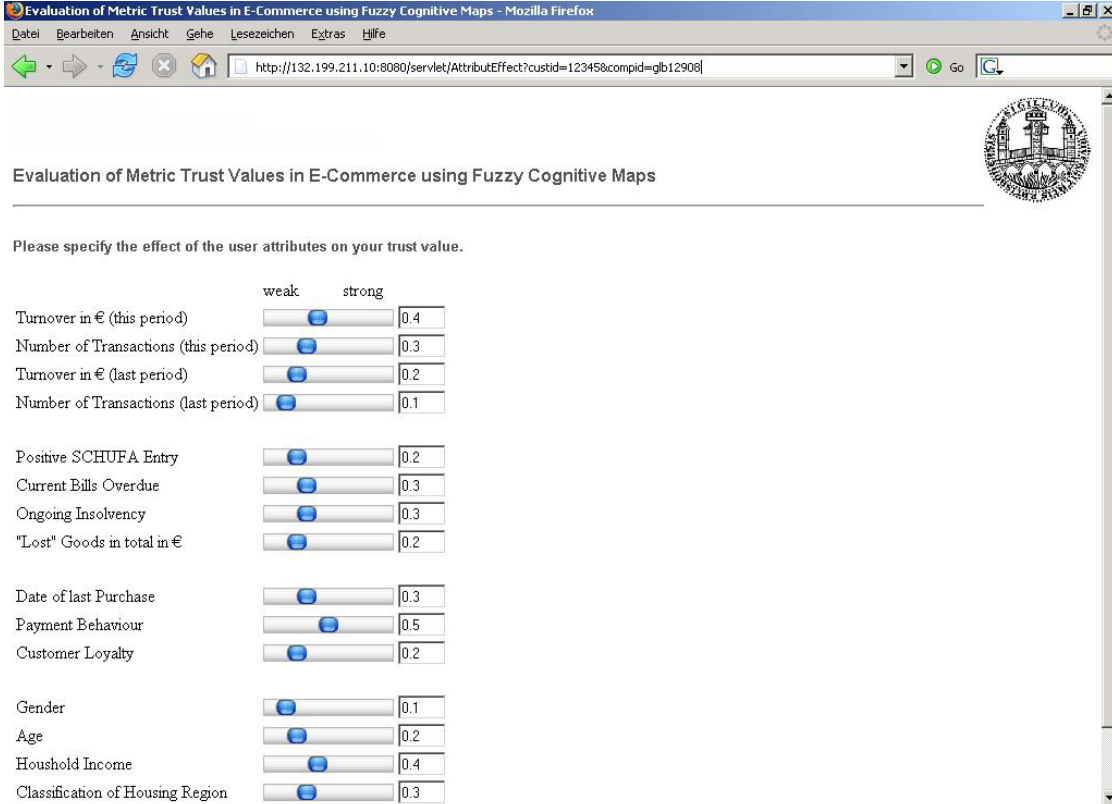
References

- [1] D.H. McKnight, and N.L. Chervany, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," Proc. of the 34th Annual Hawaii International Conference on System Sciences (HICSS 2001), IEEE, pp. 7022.
- [2] C. Schläger, M. Sojer, B. Muschall, and G. Pernul, "Attribute-Based Authentication and Authorisation Infrastructures for E-Commerce Providers," Proc. of the International Conference on E-Commerce and Web Technologies (EC-Web 2006), Lecture Notes in Computer Science (LNCS), Vol. 4082, Springer, pp. 132-141.
- [3] R.J. Lewicki, and B.B. Bunker, Trust in Relationships: A Model of Trust Development and Decline, Max M. Fisher College of Business, Ohio State University, 1994.
- [4] L. Viljanen, "Towards an Ontology of Trust.," Proc. of the International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2005), Lecture Notes in Computer Science (LNCS), Vol. 3592, Springer, pp. 175-184.
- [5] M. Coetzee, and J.H.P. Eloff, "A Framework for Web Services Trust," Proc. of the 21st IFIP TC-11 International Information Security Conference (SEC 2006): Security and Privacy in Dynamic Environments, Springer, pp. 74-86.
- [6] T. Priebe, W. Dobmeier, and N. Kamprath, "Supporting Attribute-based Access Control with Ontologies," Proc. of the 1st International Conference on Availability, Reliability, and Security (ARES 2006), IEEE, pp. 465-472.
- [7] D.H. McKnight, L.L. Cummings, and N.L. Chervany, "Initial Trust Formation in New Organizational Relationships," The Academy of Management Review, vol. 23, no. 3, 1998, pp. 473-490.
- [8] D.H. McKnight, V. Choudhury, and C. Kacmar, "Trust in E-Commerce Vendors: A Two-Stage Model," Proc. of the 21st International Conference on Information Systems (ICIS 2000), AIS, pp. 532-536.
- [9] B. Kosko, "Fuzzy Cognitive Maps," International Journal of Man-Machine Studies, vol. 24, no. 1, 1986, pp. 65-75.
- [10] B. Kosko, Fuzzy Engineering, Prentice Hall, 1997.
- [11] C. Schläger, and G. Pernul, "Authentication and Authorisation Infrastructures in b2c E-Commerce," Proc. of the International Conference on E-Commerce and Web Technologies (EC-Web 2005), Lecture Notes in Computer Science (LNCS), Vol. 3590, Springer, pp. 306-315.
- [12] C. Schläger, and M. Ganslmayer, "Effects of Architectural Decisions in Authentication and Authorisation Infrastructures," Proc. of the 2nd International Conference on Availability, Reliability and Security (ARES 2007), IEEE.
- [13] C. Schläger, T. Priebe, M. Liewald, and G. Pernul, "Enabling Attribute-Based Access Control in Authentication and Authorisation Infrastructures," Proc. of the 20th Bled eConference - eMergence (Bled 2007).
- [14] D. Gefen, V.S. Rao, and N. Tractinsky, "The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarifications," Proc. of the 36th Annual Hawaii International Conference on System Sciences (HICSS 2003), IEEE, pp. 192b.
- [15] S. Katsikas, J. Lopez, and G. Pernul, "Trust, Privacy and Security in E-Business: Requirements and Solutions," Proc. of the 10th Panhellenic Conference on Informatics (PCI 2005), Volas, Greece, Lecture Notes in Computer Science (LNCS), Vol. 3746, Springer, pp. 548-558.
- [16] A. Kini, and J. Choobineh, "Trust in Electronic Commerce: Definition and Theoretical Considerations," Proc. of the 31st Annual Hawaii International Conference on System Sciences (HICSS 1998), IEEE, pp. 51-61.
- [17] H.D. McKnight, C. Kacmar, and V. Choudhury, "Whoops...Did I Use the Wrong Concept to Predict E-Commerce Trust? Modeling the Risk-Related Effects of Trust versus Distrust Concepts," Proc. of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), IEEE, pp. 182.
- [18] C.P. Pfleeger, and S.L. Pfleeger, Security in Computing, Prentice Hall PTR, 2003.
- [19] C. Schläger, and T. Nowey, "On the Effects of Authentication and Authorisation Infrastructures on E-Commerce Environments," To be published in the

- International Journal of Computer Systems Science & Engineering (CSSE), vol. 22, 2007.
- [20] OASIS Security Services Technical Committee, "Security Assertion Markup Language (SAML)," 2005; <http://www.oasis-open.org/committees/security/>.
- [21] OASIS eXtensible Access Control Markup Language Technical Committee, "eXtensible Access Control Markup Language (XACML)," 2005; <http://www.oasis-open.org/committees/xacml/>.
- [22] H. Federrath, "Privacy Enhanced Technologies: Methods, Markets, Misuse," Proc. of the International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2005), Lecture Notes in Computer Science (LNCS), Vol. 3592, Springer, pp. 1-9.
- [23] A. Anderson, and H. Lockhart, "SAML 2.0 Profile of XACML v2.0 (OASIS Standard)," 2005; http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-profile-spec-os.pdf.

Acknowledgement

This work owes thanks to Birgit Gleißner who contributed to this research in her seminar thesis.



Evaluation of Metric Trust Values in E-Commerce using Fuzzy Cognitive Maps

Please specify the effect of the user attributes on your trust value.

Attribute	weak	strong	Value
Turnover in € (this period)	<input type="range"/>	<input type="range"/>	0.4
Number of Transactions (this period)	<input type="range"/>	<input type="range"/>	0.3
Turnover in € (last period)	<input type="range"/>	<input type="range"/>	0.2
Number of Transactions (last period)	<input type="range"/>	<input type="range"/>	0.1
Positive SCHUFA Entry	<input type="range"/>	<input type="range"/>	0.2
Current Bills Overdue	<input type="range"/>	<input type="range"/>	0.3
Ongoing Insolvency	<input type="range"/>	<input type="range"/>	0.3
"Lost" Goods in total in €	<input type="range"/>	<input type="range"/>	0.2
Date of last Purchase	<input type="range"/>	<input type="range"/>	0.3
Payment Behaviour	<input type="range"/>	<input type="range"/>	0.5
Customer Loyalty	<input type="range"/>	<input type="range"/>	0.2
Gender	<input type="range"/>	<input type="range"/>	0.1
Age	<input type="range"/>	<input type="range"/>	0.2
Household Income	<input type="range"/>	<input type="range"/>	0.4
Classification of Housing Region	<input type="range"/>	<input type="range"/>	0.3

Figure 6: Screenshot of SP's interface for specifying the FCM's weighted arcs