A Taxonomy of Trust Models for Attribute Assurance in Identity Management

Andreas Grüner, Alexander Mühle, Michael Meinig and Christoph Meinel

Abstract Attribute providers are trusted third parties in decentralized and federated identity management patterns. Service providers evaluate trust in delivered attributes with attribute assurance techniques because user properties are highly important for service provisioning. Levels of assurance define verification measures forming common ground for trust in attributes delivered by a particular provider. Beyond that, trust models that are tailored to attribute assurance in identity management enable flexible trust decisions that consider multiple attribute providers. Over time, various trust schemes for attribute assurance that address different characteristics have been proposed. We present existing models in this domain and analyze them with regard to trust scale, trust applicability, attribute aggregation, trust composition and centralization of trust. Based on the results, we create a taxonomy to arrange the trust models. Supported by this classification scheme, we devise gaps in the model coverage and propose associated future research directions.

1 Introduction

Identity management models have advanced from being isolated to centralized, and later on to a federated and decentralized scheme. This progression has lead to the separation of the identity provider from the service provider [1]. As a distinct trusted third party, the identity provider manages digital identities, their attributes and respective processes for instance, authentication. These functions are used by a wide range of service providers and users.

The attributes of a digital identity are of significant importance to the service provider. In particular, service provisioning strongly depends on correct and valid attributes. For example, accurate address information of a user enables the service

Andreas Grüner, Alexander Mühle, Michael Meinig and Christoph Meinel
Hasso Plattner Institute (HPI), University of Potsdam, 14482 Potsdam, Germany, e-mail: {andreas.gruener|alexander.muehle|michael.meinig|christoph.meinel}@hpi.uni-potsdam.de

provider to deliver ordered goods to the right person. Additionally, valid billing information ensures proper invoicing.

Therefore, the service provider trusts certain identity providers to assure correct attributes. Strong attribute verification procedures, which are implemented by the identity provider, build the foundation of assurance. To enable comparability, levels of assurance are defined that target a common understanding for verification procedures [2]. Furthermore, a service provider may use several identity providers for the same attribute to increase the assurance or selectively choose different providers for specific properties in situations with a varying risk profile. Various trust models that concentrate on attribute assurance try to optimize trust decisions. Additionally, service providers are able to flexibly choose the right attribute provider.

In this paper, we outline trust models for attribute assurance in identity management and analyze them based on defined properties. The evaluated characteristics enable a comparative view of the trust models within this domain. As a result, we can identify gaps in the taxonomy and derive open areas for research.

The remainder of this paper is organized as follows. In Section 2, related research work is presented. Afterwards, we outline properties of the trust models in Section 3. Subsequently, in Section 4, we present, analyze and compare the trust models for attribute assurance. Based on the comparison, we provide insights into open research areas in Section 5 and conclude the paper in Section 6.

2 Related Work

The determination of trust and reputation between parties in online services is a longstanding research area. Related research work focuses on summarizing different models in a survey or providing a taxonomic classification.

In 2000, Grandison et al.[3] created a survey of trust in internet applications by defining trust itself, creating different trust categories and classifications. Furthermore, trust management solutions for applications are presented and contexts where trust is necessary (e.g. medical information systems, information retrieval, mobile code) are outlined.

Sabater and Sierra [4] published a comprehensive review in 2005 on computation trust and reputation models. The schemes are differentiated in two categories: cognitive and game-theoretic. Additionally, all reviewed models are analyzed with regard to information sources, visibility types, model granularity and agent behaviour.

The trust management survey by Ruohomaa and Kutvonen[5], published in 2005, provides an overview of phases within trust management frameworks. Trust management follows a sequence of events: initialization of the trust relationship, observation of new information relevant for the relationship and, finally, evolution of the reputation and trust based on the observations.

In 2007, Jøsang et al.[6] created a survey of trust and reputation systems for online service provision. The models are clustered according to the underlying

methodology of trust or reputation aggregation: summation, Bayesian systems, discrete models, belief patterns or flow schemes.

Yan et al.[7], published in 2014 a survey on trust management for the Internet of Things. Within the survey, different objectives of trust, e.g. data perception trust, identity trust, are outlined. Based on these objectives, trust areas in the Internet of Things are described and evaluated.

Furthermore, in 2015, Cho et al.[8] published a generic survey on trust modelling. Within the survey, the concept of trust and underlying factors, respectively rationale, are described. Additionally, different techniques to model trust in various scientific disciplines are outlined.

Besides these surveys, focused research work about trust models in public key infrastructures have been published [9] [10]. These overviews present single certificate authorities, multiple certificate authorities, top-down and bottom-up schemes.

Attribute assurance is specifically about trust in the correctness of properties of a digital identity and how trust is achieved and modelled for relying parties. In contrast to the previous work, we focus our taxonomy on trust models for attribute assurance in identity management. In addition to that, we analyze the models according to defined characteristics.

3 Characteristics of Trust Models in Attribute Assurance

The foundation of a taxonomy is based on characteristics that enable a comparative classification of objects. We apply the properties trust scale and trust applicability. Furthermore, we consider attribute aggregation, trust composition and centralization of trust as major differentiating factors of trust models within the attribute assurance domain. In the following paragraphs, we outline a definition of each characteristic and possible values.

- **Trust scale:** The decision to trust an attribute can be evaluated according to different scales of trust. We differentiate in general a *discrete* or a *continuous* scale. A discrete scale has a finite number of levels that specify trust in an attribute. The *binary* scale is a specific case of a discrete range that differentiates solely between trusted and not trusted. It is the most coarse grained categorization. A continuous scale has infinite increments to express levels of trust. Thereby, it enables a very fine grained representation of trust. Additionally, a continuous scale requires thresholds to define trust levels.
- **Trust applicability:** The meaning of trust applicability is twofold. On the one hand, it relates to the trust rating itself. On the other hand, the applicability refers to an acceptance value of the rating by the party that consumes the attribute. For both contexts, we differentiate the characteristic as a *predefined* or an *individual* value. The applicability of a trust rating for a specific attribute can be globally *predefined* the same or *individually* different. A globally *predefined* trust value is at least initially the same for all actors. An *individual* trust value is not globally

alike predefined, but specific to each party or group of parties that evaluate the trust rating. In a comparable manner, the acceptance level is global *predefined* if it is the same for all actors or *individual* to each party.

- **Attribute aggregation:** Attribute aggregation refers to the combined usage of attributes from different attribute providers. We differentiate the category attribute aggregation in the following clusters: *completing*, *trust-enhancing* and *none*. An attribute assurance model can use aggregation for *completing* a set of required attributes if a dedicated attribute provider cannot deliver all demanded properties. In case the same attribute from different providers is used to increase assurance in the attribute value, the application is *trust-enhancing*. A *trust-enhancing* pattern may also be used to complete the attribute set. Otherwise, *none* aggregation methodology is used.
- **Trust Composition:** The category composition describes the depiction of trust value. We distinguish a *simple* representation in case trust is derived from one factor. A *structured* composition involves the combination of several factors. For instance, a probabilistic aggregation of one attribute from different attribute providers or the joining of several requirements from one provider. Furthermore, a detailed breakdown of underlying trust factors is also considered as *structured*.
- **Centralization of Trust:** Centralization refers to a *central* or *decentral* origination of trust in the attributes of an identity. If the trust does not originate from any trusted third parties, the schema is *decentralized*. Otherwise, the trust model is *centralized*.

4 Trust Models for Attribute Assurance

In identity management, various attribute assurance models have been proposed to determine and increase trust in a digital identity's attributes by a service provider in particular or a user in general. We describe the contextual setting of the trust model and the trust model itself. As the main contribution, we evaluate each trust model according to the criteria outlined in the previous section. Finally, we compare the different models.

4.1 Public-key Infrastructure based on X.509

Public-key infrastructures (PKI) establish identities for entities by the issuance of certificates. Therefore, PKIs are a foundational component for securing communication, e.g. network traffic, over untrusted networks. Especially on the internet, certificates that are issued by certificate authorities are used to secure the communication between the user's browser and web servers. A standard for these public-key infrastructures is X.509 [11].

A certificate binds a public key to additional attributes. Usually, a certificate includes the name of the owner of the public key. Additionally, further properties including permissions can be contained. A certificate authority issues a certificate by cryptographically signing the corresponding data structure with its own private key. Certificate authorities are organized in a hierarchy that forms a chain of trust. At the top, there are a few authorities that delegate roles to intermediate authorities. A functional delegation is at the same time a delegation of trust. Finally, certificates are issued to principals such as user devices or servers. A user or service provider trusts a certificate if the verification succeeds up to the top certificate authority. Additionally, general trust in all involved certificate authorities is required. In case a specific authority in the chain of trust is not trusted, the verification process fails.

The scale of a PKI trust model is of type discrete. The values trusted and not trusted are solely differentiated. A relying party might trust or does not trust a single certificate authority or the chain of trust overall. Thus, the discrete scale is additionally binary. Concerning trust applicability, the trust rating and the acceptance of attributes contained in a certificate is globally predefined to all users and service providers. Within the PKI trust model, the rating and acceptance is also the same. A user can solely trust a certificate authority, and if the certificate authority is trusted, the certificates are accepted. For all entities using the PKI the certificate authority has the same rating. Furthermore, different users do not have the possibility to define distinct levels of acceptance. The PKI trust model does not apply attribute aggregation in the defined sense. A certificate can contain several attributes. However, these properties are attested by the same certificate authority. There is no aggregation from different authorities. Besides that, no trust-enhancing aggregation occurs. The composition of factors to achieve a trust rating is simple. There is no structured composition of different trust factors for a certain certificate authority. Finally, the PKI trust model is centralized towards the certificate authorities as trusted third parties.

4.2 Pretty Good Privacy

Phil Zimmermann created Pretty Good Privacy (PGP)[12] as a decentralized email address scheme. An email address is bound to a public key and the name of the holder based on a peer-to-peer attestation scheme. PGP was created as a counter project against hierarchical email address schemes (compare subsection 4.1). These patterns require trust in a trusted third party that confirms the public key to the email address as respectively name binding.

The PGP trust model [13] differentiates the trustworthiness of a public key certificate and the trustworthiness of an introducer. An introducer is an entity that confirms the certificate. The public key certificate contains the email address, the owner and the public key to verify ownership. The trustworthiness of the certificate is categorized as undefined, marginal and complete. From status undefined no conclusion about the trustworthiness of the certificate is possible. The status marginal reflects an

intermediate trust status. Finally, the classification complete reflects a fully trusted certificate. The trust classification of the certificate is distinct to each participant. It is based on the number of required fully or marginally trusted introducers. The trust rating of an introducer can be full, marginal, untrustworthy or simply unknown. If a certificate reaches numbers that signify fully or marginally trusted introducers, it is completely trusted. In case there is at least one fully or marginally trusted introducer, the certificate is marginally trusted. Otherwise, the trust status of the certificate is undefined. The trust classification of the introducer is distinct to the user.

The trust scale of the PGP trust model is discrete. The trust levels complete, marginal and undefined are used to evaluate a certificate. The trust applicability is individual for both the rating and the acceptance. The rating of an introducer is specific to each user. Even if a certain introducer is not trusted by a user, the PGP trust model still enables a trust decision. The acceptance of a certificate depends on the user defined number of required marginal or fully rated introducers. Attribute aggregation techniques to complete a set of attributes from different providers are not used. However, the delivery of the same attribute by different providers is done implicitly by the confirmation of the certificate by different introducers. Therefore, we classify the attribute aggregation category as trust-enhancing. The characteristic composition of the PGP trust model is simple. Each introducer is classified as marginal or fully trusted. The number of introducers of both categories is compared to threshold. The PGP trust model is decentralized as it does not depend on trusted third parties. Every user can act as an introducer to provide trust for a certificate and therefore, for the included attributes.

4.3 A Probabilistic Trust Model for GnuPG

Jonczy et al.[14] proposed a new trust model for GnuPG resp. PGP to remediate deficiencies that have been seen in the default trust model (compare subsection 4.2). A coarse grained discrete trust scale that differentiates marginal and fully trusted introducer has been named as the major drawback [14].

The foundation of the trust model is aligned to network reliability theory and depicted as a directed graph-based network. Such a network exists per user. A node represents an introducer with an assigned probability. The probability value reflects the trustworthiness of being an honest introducer. Paths between the nodes outline certificate relationships. If a user wants to evaluate the trustworthiness of a certificate for another user it determines all paths between them. In case no path exists, trustworthiness cannot be evaluated. Otherwise, the probabilities of all paths with minimum length are combined. The probability of a specific path is the product of the independent probabilities of each introducer on the path.

Jonczy et al.'s trust model has a continuous trust scale based on probability values between 0 and 1 for a certificate. The trust applicability is individual both for rating and acceptance. Each user can rate its known introducers with a probability that indicates trustworthiness. Similarly, a threshold for the probability determines

if a certificate is trusted or not. That threshold might be differently defined between different users. Attribute aggregation method is trust-enhancing as the trustworthiness of several introducers is combined to achieve an overall increase in trust. The composition of trust information is structured as the setting and combination of trust values is aligned to modelling in network reliability theory. Finally, the trust model is decentralized based on its origin of the decentralized PGP scheme.

4.4 Thomas et al.'s logic-based Assurance Framework

In service-oriented architectures, identity federations are applied to use identities and attributes across trust domains. Thomas et al.[15] noticed that common assurance frameworks only allow to specify trust in the identity provider for the identities and all of its attributes. However, an attribute-specific trust determination gives an opportunity to make a finer grained trust decision. Therefore, Thomas et al.[16] defined a logic-based assurance framework that enables a trust specification in the provider and the delivered attributes.

The formalized trust model consists of service and identity providers as well as additional participants. Furthermore, it encompasses a set of organizational trust levels, attributes and their types and attribute verification classes as distinct objects. In addition to that, the model contains relationships between the different elements. Attributes are assigned to a specific type and a verification class. The identity provider can only assert particular attributes and support specific verification classes for these properties. Besides that, an identity provider has assigned characteristics. The organizational trust rating is a special characteristic of an identity provider. The rating is specific to a service provider. A certain configuration of the model is stored as a knowledge base. This knowledge base is used by participants that rely on it. Thomas et al. outlines an example where identity providers are classified with a three-ary organizational trust rating and an additional federation categorization. Additionally, rules are stored that define the trusted attributes and originating identity provider.

The trust scale of Thomas et al.'s model is discrete because the acceptance of an attribute depends on rules that utilize the organizational trust rating and federation property of the identity provider. Additionally, the rule encompasses the asserted attribute itself and may contain a restriction on the verification class. Within the trust applicability, the rating and acceptance are individual to all participants if each participant has a distinct knowledge base and rules. The characteristic attribute aggregation has the value completing because different identity providers can deliver distinct attributes. However, the same attribute from different providers is not used to enhance the trust rating. Thomas et al.'s assurance model is structured in the category composition because of different factors, e.g. organizational trust, federation, verification class, are used to obtain a final trust decision. The trust scheme is central due to the usage of identity providers as trusted third parties.

4.5 AttributeTrust

Mohan et al.[17] proposed the AttributeTrust framework. It applies a reputation system to determine trust in provided properties of an identity. Disadvantages of attribute-based access control schemes, including the bundling of several attributes to credentials, serve as motivation for the assurance framework.

The AttributeTrust framework is modelled as a weighted directed graph with nodes and edges. The nodes represent the actors that are comprised of users, relying parties and attribute providers. The edges reflect confidence paths between the different entities. Nodes and edges have weights that express confidence values in range 0 to 1. For a new node joining the network, the default confidence value is zero. The confidence value of a node is the product of the in-degree of the node with the average of the confidence values leading to the node. In case a user wants to consume a service, the user presents attributes of an attribute provider to a service provider. The service provider evaluates all known confidence paths to the attribute provider up to a certain depth. Subsequently, the confidence value of the attribute provider is calculated by the service provider. The overall value is used to decide if the attributes from the respective attribute providers are accepted or rejected.

The trust scale of the AttributeTrust framework is of type continuous. Values of the trust scale lie between 0 and 1. A value is calculated as the product of the in-degree of a node and the average value of all received confidence paths. The trust applicability in the form of rating and acceptance is individual to the entities of the trust model. Entities can define their own confidence paths. Additionally, an actor as a service provider can define its own thresholds for acceptance of a confidence value. Besides that, the maximum length of confidence paths that are considered for calculating the value is another entity specific adjustment option. AttributeTrust acts in a completing manner with regard to attribute aggregation. A user can forward attributes from different attribute providers to a service provider to complete the required set. As trust is derived from different confidence values, the characteristic composition is evaluated to simple. There are no structured underlying factors specified in the AttributeTrust framework. Finally, the scheme is centralized as specific attribute providers are the origin of trust in the properties.

4.6 A Calculus of Trust and Its Application to PKI and Identity Management

Huang et al.[18] developed a calculus of trust based on trust in performance and belief. Additionally, the uncertainty is measured with regard to a specific trust rating. The trust model is applied to public-key infrastructures to determine the trustworthiness of certificates based on the certification paths between the principal and the certificate authorities.

The trust model shapes the network as a directed graph. Certificate authorities, intermediate authorities and the certificates are the nodes of the graph. The edges reflect a trust relationship. Trust is measured as a degree based on probabilities. The trust in a certificate is determined by sequentially aggregating the trust path from the certificate to the top-level certificate authority. Additionally, the trust degree of several parallel paths is combined to an overall probability value. A relying party can decide on their own at which rate the certificate is accepted as trustworthy.

The trust scale of the trust model is continuous due to the usage probabilities in range 0 to 1. With regard to trust applicability, the rating is individual for the participants in the model. That is a result of potentially subjective trust probabilities in the confidence in the certificate authorities. The acceptance of a trust rating is specific to each actor and therefore individual as well. The usage of several parallel certification paths enables a trust-enhancing aggregation of attributes. Underlying factors for the trust are structured due to the usage of trust in performance, trust in belief and uncertainty value. The model is centralized due to the usage of certificate authorities for attribute assurance.

4.7 A Quantifiable Trust Model for Blockchain-based Identity Management

Grüner et al. [19] developed a trust model for blockchain-based identity management. Blockchain enables the new self-sovereign identity management model. At the same time, it serves as an identity provider platform to connect attribute providers, relying parties and users. Attributes are modelled as verifiable claims that consist of claims and attestations.

The trust model is formed as a directed graph consisting of nodes and edges. Identities, claims and attestations are the entities that represent the nodes of the graph. The edges symbolize the trust flow from one object to another. An identity has a certain trust value. By issuing an attestation to a claim, trust is transferred to a claim by the attestation. The more attestations a claim has, the higher the trust value of the claim. The more claims with high trust values an identity has, the higher the trust value of the identity itself. The transition of trust between the different entities is specified by functions. The trust value is in the range of 0 to 1.

The trust scale of the scheme is continuous because the trust value lies between 0 and 1 and is calculated by trust functions. With regard to the trust applicability, the rating of a claim, respectively attribute, is globally predefined to all identities within the network. In contrast, a potential acceptance of an attribute is individual because the consumer of the attribute can specify a specific threshold. If the trust value exceeds the threshold, the attribute is accepted. The trust model focuses on a trust-enhancing attribute aggregation mechanism. A claim can hold several attestations by different issuers to increase its trust value. The composition of the trust value is structured because functions are used to combine different trust ratings al-

though no underlying factors are considered. Every entity can attest claims and act therefore as trust anchor. Thus, the model is decentralized.

4.8 Using Quantified Attribute Aggregation for Increasing Trust in Attribute Assurance

The quantified attribute aggregation trust model of Grüner et al. [20] is targeted towards verifiable claims that are used within self-sovereign identity solutions. Self-sovereign identity management solutions place the user in full control of its identity and have raised with the invention of blockchain technology.

Within the trust model, the attributes of users are modelled as verifiable claims that are comprised of claims and attestations. The trustworthiness of a claim is a probability between 0 and 1. This probability is derived from the combination of probabilities of all attribute providers that have attested the particular claim. Each attribute provider is rated with a probability for issuing correct and valid attributes by a relying party. Additionally, the relying party can define a threshold for each claim. If the calculated overall probability exceeds the threshold, the claim is accepted as a valid attribute of the user.

The trust model of Grüner et al. applies a continuous trust scale with probability values in the range between 0 and 1 for an attribute. With regard to trust applicability, the rating and acceptance are individual to all participants. All relying parties can define their own ratings of each attribute provider. Additionally, accepted providers can be set individually. Concerning the acceptance of the rating, the thresholds are also under control of the relying parties. The attribute aggregation type of the trust model is trust-enhancing because the acceptance of several attribute providers is used to increase the trustworthiness of the attribute. The composition of trust is structured as the rating takes into account the validity and correctness of an attribute of a certain provider as underlying factors. Furthermore, the trust model is decentralized because all participants can issue attestations.

4.9 Comparison

The evaluated trust models for attribute assurance in identity management cover a wide range of different combinations of the properties. An overview of all studied schemes and their respective properties is shown in Table **??**.

The reviewed trust models encompass trust scales of type binary, discrete and continuous. Hereby, continuous trust scales clearly outweigh the other types and enable a more fine-grained trust decision. Considering the category trust applicability, the trust schemes cover in terms of rating and acceptance the combinations predefined/ predefined, predefined/ individual and individual/ individual. A mix of an individual rating with globally predefined acceptance level is not available. However, a

trust model that implements this combination would not seem expedient because an entity specific rating might not logically fit to a global predefined acceptance grade. The majority of trust models apply the individual/ individual scheme whereas the predefined/ predefined concept is solely implemented by the PKI trust model. For the characteristic attribute aggregation, all values can be seen within the different trust models. The studied trust models use predominantly attribute aggregation for completing a required set of attributes or increasing trust in a specific property. The PKI trust model does not use these techniques at all. With regard to trust composition, the majority of the schemes apply a structured understanding of trust compared to a simple trust definition. In analyzing the category centralization of trust we see that more trust models use a centralized pattern, which relies on trusted third parties for attribute assurance.

Evaluating the trust models across the property categories, we can deduce that trust models that have an individual trust rating usually also implement a continuous trust scale. Additionally, these trust schemes apply a trust enhancing attribute aggregation methodology. Based on these features, a typical configuration for a web of trust is depicted. Whereas a chain of trust uses a binary trust scale and no attribute aggregation technique by having a very centralized nature of the trust model.

5 Research Directions

Based on the trust model review and the conducted comparison, we can see two further research directions on evolving related trust models. On the one hand, the development of a trust model that combines predefined/ predefined trust applicability with a continuous trust scale and a certain attribute aggregation methodology seems to close a gap in the current landscape. The centralized model could also benefit from the further decentralized characteristics. On the other hand, further research in predefined/ individual trust models would seem to be promising as a fine grained trust rating is globally available for all actors.

6 Conclusion

In identity management, trust models are used for attribute assurance. A relying party is enabled to decide if the attributes of a user's identity are trustworthy. We consider trust scale, trust applicability, attribute aggregation, trust composition and centralization of trust as significant characteristics of these trust models. After defining the properties, we have presented published trust models. Furthermore, we have reviewed these schemes according to their characteristics and compared the results between the models. Finally, we have drawn conclusions towards future research directions.

References

1. A. Grüner, A. Mühle, T. Gayvoronskaya, and C. Meinel, "A comparative analysis of trust requirements in decentralized identity management," in *In Proceedings of the International Conference on Advanced Information Networking and Applications*. Springer, 2019.
2. P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Nist special publication 800-63. digital identity guidelines," 2017.
3. T. Grandison and M. Sloman, "A survey of trust in internet applications," *Commun. Surveys Tuts.*, 2000.
4. J. Sabater and C. Sierra, "Review on computational trust and reputation models," *Artificial Intelligence Review*, 2005.
5. S. Ruohomaa and L. Kutvonen, "Trust management survey," in *Trust Management*. Springer, 2005.
6. A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, 2007.
7. Z. Yan, P. Zhang, and A. Vasilakos, "A survey on trust management for internet of things," *Journal of Network and Computer Applications*, 2014.
8. J.-H. Cho, K. Chan, and S. Adali, "A survey on trust modeling," *ACM Comput. Surv.*, 2015.
9. R. Perlman, "An overview of pki trust models," *Netwrk. Mag. of Global Internetwkg.*, 1999.
10. A. Jøsang, "Pki trust models," *Theory and Practice of Cryptography Solutions for Secure Information Systems*, 2013.
11. Internet Engineering Task Force. (2008) Rfc 5280. internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. [Online]. Available: https://tools.ietf.org/html/rfc5280 [Accessed: 2019-08-25]
12. P. R. Zimmermann, *The Official PGP User's Guide*. Cambridge, MA, USA: MIT Press, 1995.
13. A. Abdul-Rahman, "The pgp trust model," *Journal of Electronic Commerce,*, 1997.
14. J. Jonczy, M. Wüthrich, and R. Haenni, "A probabilistic trust model for gnupg," in *In 23C3, 23rd Chaos Communication Congress*, 2006.
15. I. Thomas and C. Meinel, "Enhancing claim-based identity management by adding a credibility level to the notion of claims," *2009 IEEE International Conference on Services Computing*, 2009.
16. ——, "An attribute assurance framework to define and match trust in identity attributes," in *Proceedings of the 2011 IEEE International Conference on Web Services*. IEEE, 2011.
17. A. Mohan and D. M. Blough, "Attributetrust a framework for evaluating trust in aggregated attributes via a reputation system," in *Proceedings of 6th Annual Conference on Privacy, Security and Trust, PST 2008*, 2008.
18. J. Huang and D. Nicol, "A calculus of trust and its application to pki and identity management," in *Proceedings of the 8th Symposium on Identity and Trust on the Internet*. ACM, 2009.
19. A. Grüner, A. Mühle, T. Gayvoronskaya, and C. Meinel, "A quantifiable trust model for blockchain-based identity management," in *Proceedings of the 2018 International Conference on Blockchain*, 07 2018, pp. 1475–1482.
20. A. Grüner, A. Mühle, and C. Meinel, "Using quantified attribute aggregation for increasing trust in attribute assurance," in *Proceedings of the IEEE Symposium Series on Computational Intelligence (to be published)*. IEEE, 2019.