On the Structure and Assessment of Trust Models in Attribute Assurance

Andreas Grüner and Christoph Meinel

Abstract Online services fundamentally rely on identity management to secure and personalize their presence. Within identity management, attribute assurance techniques target correctness and validity of attributes. These properties are an essential foundation for service provisioning in digital businesses. A myriad of attribute assurance trust models has been published. However, a superior trust model from the various proposals has not been discriminated. Additionally, a profound assessment is challenging due to a missing general notation and approach. In this paper, we work towards the structural characteristics of a secure trust model. To achieve this, we analyze common elements of attribute assurance trust models and outline differentiating factors compared to other domains. Based on the key components, we propose a formal meta-framework to depict existing trust models. Using the framework, characteristics and security attacks of these trust schemes are elaborated. As an outcome, we can conclude that a secure trust model depends on an attack-resistant trust function that considers high trust values and several attestation issuers.

1 Introduction

Identity management plays a significant role at virtually all online services that provide user-specific offerings in digital businesses. An identity is a set of information that characterizes a physical entity and enables an online service to recognize a user. On the same lines, user-specific offerings or benefits at an online service are bound to its particular identity. Therefore, identity management is at the forefront of the online service's security design. Generally, an Identity Provider (IdP) implements identity management processes such as authentication, credential and attribute management. An attribute defines a characteristic of an entity. The IdP is responsible to

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

provide correct facts that reflect the reality. Additionally, the IdP must revoke it when they are not valid anymore.

In open domain identity management models, e.g. federation topologies, the IdP is a trusted third party towards the user and the Service Provider (SP). The IdP, the SP and the user belong to different trust domains and therefore, must trust each other. In a wide range of different scientific subjects, trust is considered a subjective phenomenon that is meaningful in personal relationships. In our opinion, one of the most applicable denotations is the definition of decision trust from Jøsang et al. [1] based on the work of McKnight and Chervany [2]. It characterizes trust as *"the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible."*

Concerning attribute management, the user and the SP are willing to depend on the IdP for the process of attribute attestations. User and SP rely on transferred attributes that are authentic. The user intends to consume a service, and the SP offers the respective service. Correct and valid attributes are required to provision and potentially invoice the offering accurately. Otherwise, either the service is not usable or the usage might not get invoiced as negative consequence. Both factors restrain the relationship between the user and the SP.

In related research, trust in identity management is holistically referred to as identity trust [1] or trust management in authentication systems [3]. In contrast, the latter one limits the trust context to the public key to identity binding. Nonetheless, Gomi [4] proposes a separation between identity and attestation trust.

We conform to this separation and concentrate our work on trust models in attribute assurance for specifying trust in the correctness of an identity's properties (attestation trust). This research focus is also motivated by the development of a decentralized IdP based on blockchain. This advancement facilitates the separation of the identifier from the actual attributes of an identity. Furthermore, a decentralized IdP fosters the reduction of the traditional IdP to a mere Attribute Provider (AP) [5]. Besides that, a decentralized IdP resolves the IdP as a trusted third party and lets the AP be the last central authority in identity management. Overall, an attribute ecosystem is established to combine properties for a single identity from distinct providers.

Trust models in attribute assurance have been mainly proposed in reference to a specific implementation of a trust management system or authentication scheme. The web of trust and, on the opposite, the chain of trust are the two main directions of trust model development. A web of trust describes the mutual verification of properties by equitable peers. The PGP [6] trust model is one of the popular representatives. On the other side, a chain of trust reflects hierarchical trust models where specific entities confirm properties to other participants. Public-Key Infrastructures (PKI) based on the X.509 [7] standard apply a hierarchical trust model.

These dedicated entities represent trusted third parties. Both models have their distinct advantages and disadvantages. Besides these edge cases, there are many intermediate schemes [8] with differences in the underlying trust modelling. Based on the number of different trust models in attribute assurance and the emerging possibilities of a decentralized IdP, we formulate our research question: *Is there a secure trust model in attribute assurance and how is its structure?*

To address this topic, we analyze the structure of attribute assurance trust models to outline major components and differentiating factors to trust schemes apart from attribute assurance. The structure forms a meta-framework to depict such trust models. Furthermore, we study characteristics and security-related attacks. Moreover, we conclude on characteristics of an attack-resistant attribute assurance trust model based on the previous analysis.

The remainder of this paper is organized as follows. In Section 2, related work in this area is described. Subsequently, in Section 3 we analyze trust modelling in attribute assurance and provide a structure of respective trust models and desired properties. Finally, we conclude the paper in Section 4.

2 Related Work

In 1999, Jøsang [9] proposed an algebra for assessing trust in certification chains. The work's objective is to decide on trust between peers for communication in open networks without having previous interactions. Furthermore, in 2009, Yang et al. [10] published a trust algebra as the foundation for a general trust model. The trust algebra comprises trust evaluation and propagation algorithms for communication partners. Huang and Nicol [11] created a formal semantics based calculus of trust. The calculus provides means to logically model trust relationships and derive trust decisions.

Further research work is done to compare general trust models. Carbone et al. [14] focuses on trust modelling and comparison in dynamic and peer to peer networks. Kinateder et al. [15] concentrate on the comparative study of trust update algorithms of trust models. Fragkakis and Alexandris [16] differentiate trust models for mobile agents. Additionally, Moyano et al. [17] proposed a general conceptual framework for trust models.

Moreover, the PKI domain is an in detail analyzed research field. The main focus of the contributions is on trust in the public key to identity binding. Bakkali and Kaituni [18] [19] as well as Haibo [20] propose a logical model to reason about trust in PKI. Huang and Nicol [21] published a general calculus of trust and applied it to identity management. The work enables conclusions about trustworthiness and risks of certification paths. Furthermore, research concentrates on structures and trust distribution within different types of PKI. For instance, narrative comparisons of different models for PKIs are conducted [22]. Besides that, Maurer [23], Marchesini and Smith [24] and Henderson et al. [25] published various trust models for PKI. Additionally, Ulrich et al. [26] examined an instance of the OpenPGP web of trust. The data is evaluated with regard to network structure and security-relevant criteria. Alexopoulos et al. [3] studied the benefits of using blockchain for trust management in authentication. The authors created a formal model for blockchain-based authentication and studied attacks against the model.

3 Trust Modelling in Attribute Assurance

In this section, we study the structure of trust models in attribute assurance. Thereby, we start with common elements and outline differentiating factors to trust models in outside attribute assurance. Subsequently, we elaborate on attestation and trust networks as well as the trust composition. Finally, security attacks for these trust models are considered and desired properties are presented.

3.1 Common Elements of Trust Models

A trust model environment is comprised of a set of common elements. Primarily, different **entities** are part of the model. These entities rely on each other and reflect the trustors and the trustees. For instance, an entity can be a person, an organization or a company. Furthermore, the **relationships** between the participants are important. From certain entities, trust originates to other entities based on neighbourhood, previous interactions or other important criteria for the trust modelling in the respective domain. Entities that provide trust for other entities are related. These relationships build the foundation for the **trust** evaluation **function**. The trust evaluation function specifies the composition of the trust value in an entity. As a last point, the trust value is used to determine if the interaction with this entity is continued or terminated.

3.2 Distinction to Trust Models in other Domains

As trust is omnipresent in various domains, manifold trust models have been proposed [1]. Trust models can be based on reputation. Reputation considers previous experiences between the peers. These schemas are applied in agent systems, for instance in peer to peer file-sharing models or in evaluation patterns for market places to judge buyers and sellers. Besides common components, we see direct feedback and trust ageing as specific differences to trust models outside the attribute assurance domain.

No direct feedback: Reputation-based trust models retrieve trust from previous experience [27]. Therefore, the prior experiences need to be classified into the categories positive or negative. Positive feedback increases trust while negative feedback decreases trust. This decision must happen on time to influence the trustworthiness of an entity. In the file sharing scenario, the received file can be directly tested for validity. In attribute assurance, a direct decision on the correctness of an attribute, after the SP has received it, might not be possible. Logic checks can superficially verify the attribute, but not conclusively validate it. If the first name or the user's last name is wrong, it might be solely uncovered if an ordered shipment is returned by the logistics company to the seller.

No trust ageing: Trust models that specify trust into entities based on prior interactions usually include elements of trust ageing [1]. Interactions that lie further back in the past contribute less to the overall trust score. Recent experience or contact influence the trust level in a significant higher manner. Trust ageing is not formally incorporated into a trust model within attribute assurance, but it can be practically addressed. A property attestation has a limited validity period or can be revoked on demand. For instance, a certificate issued by an authority has an expiration time. Additionally, a revocation mechanism may exist.

3.3 *From an Attestation Network to a Trust Network*

We separate the structure of trust models in attribute assurance into a graph-based network to depict the relations. An additional set of functional elements refer to the composition of trust. Related trust modelling activities use a graph-based approach [26] or a formal logic [12]. However, a directed graph naturally reflects the relations between the entities. Furthermore, a calculus or logic can determine the actual trust value. We focus on an abstract model and omit peculiarities of an implementation. In particular, we assume the existence of cryptographic measures to secure communication and verify the attestations' origin.

IdPs or APs attest properties for a user and transfer them to the SP. In PKI systems a Certificate Authority (CA) issues certificates for entities to assert a public key to identity binding whereas properties of a user characterize the identity. In the PGP setting, the confirmation that an email address belongs to a public key is also referred to as a certification. Thereby, the email address is the attested attribute. In the Self-Sovereign identity (SSI) ecosystem, attested attributes are referenced by the term verifiable claim or credential. Nonetheless, such an attribute attestation is a confirmation of an entity, e.g. a CA or a user, about a characteristic of another entity.

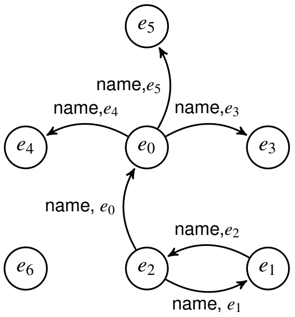

Fig. 1 Sample attestation network

Definition 1 (Attestation network). An attestation network AN is a directed graph $AN = (E, A)$ that expresses attribute attestations as relations A between the nodes E whereas:

- Nodes E represent all the entities, e.g. IdPs, APs, SPs, CAs or users
- Attestations A constitute asserted attributes by one entity to another. An attestation $a \in A$ is an attribute relation tuple $\langle attribute\ class, attribute\ value \rangle$.

Fig. 1 shows a sample graph of an attestation network. The entities attest each other their names whereas node e_0 issues the most assertions. In a PKI environment, the node e_0 can be seen as a CA. In contrast, the entities e_3, e_4 and e_5 constitute regular users. The attestations between entities e_1 and e_2 reflect paradigmatically a web of trust where nodes attest each other their properties. Entity e_6 neither attest nor receives properties. We call a node an AP if it issues at least one property assertion. A user receives at least a single attribute attestation.

An attestation does not directly reflect a trust relation. However, it builds the foundation to assess trust relationships. Concerning the asserted attribute, the issuer may trust the receiver that verification procedures are not deliberately circumvented. Furthermore, the receiver can trust the issuer that delivered private information is adequately protected. Nonetheless, from an outside perspective, the major trust relation exists in case the attestations are presented to a SP for service consumption. The SP or generally any Relying Party (RP) validates the attribute attestations. The RP trusts the issuer of the provided attestations that they are authentic. The attributes of a user must reflect reality. This trust relation between the entities can be depicted in a directed graph as a trust network. The illustrated trust relation in a trust network is context-specific to an attribute class. An AP might be eligible to attest an email address, but it cannot sufficiently verify the name of another entity. Therefore, the trust is dependent on the context of the asserted characteristic.

Definition 2 (Trust network). A trust network TN is a directed graph $TN = (E,R)$ that expresses trust relations R between the nodes E whereas:

- Nodes E reflect all relying parties, e.g. IdPs, APs, SPs, CAs and users
- Trust relations R illustrate a dependency between an entity that acts as trustor and the trustee for attribute assurance. A trust relation $r \in R$ is a tuple $\langle attribute\ class, trust\ rating \rangle$.

The trust rating of a relation within the trust network is a value that belongs to the trust space. The trust space of a model comprises individual trust values that express trustworthiness. These figures are ordered to state comparable differences in trust. For instance, node e_i is more trusted than node e_j by entity e_k. Discrete numeric trust values can be assigned to verbal expressions to drive the understanding of a certain trust level. In Fig. 2 a sample trust network is shown. It is aligned to the previously depicted attestation network. However, it shows only a potential trust situation. The node e_0 receive the most trust for attribute class *name*. Entities e_1 and e_2 only trust each other.

As the attestation network and the trust network are tightly coupled, we investigate both structures' relationship to each other. IdPs, APs, SPs and users can issue claims towards other entities or may receive assertions. Each of the nodes can also act as a RP to accept attestations. Therefore, it expresses a certain level of trust in the attestation issuer. Furthermore, a node may not receive or issue any attestation or trusts respectively is trusted. Thus, both networks encompass the same entities. Having the same nodes on either network, we can investigate a connection between an attribute attestation and a trust relation.

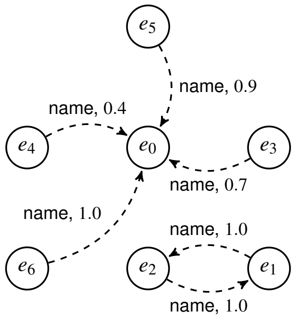

Fig. 2 Sample trust network

In case a certain node issues a large number of attributes it is likely that these properties are also accepted by other entities. Thus, trust exists in the originating entity. The creation of a large number of assertions that can not be used at any RP is unlikely. On the contrary, if an entity does not assert any characteristics it cannot be deduced that this entity is not trusted at all. For instance, the node may issue attestations in future. Examining the transformation from a single attestation into trust relations, there is a myriad of potential relations that comprises the issuer, receiver or any third party node as RP. Besides this complexity, a detailed derivation of the trust rating in a complex trust space is not feasible. Thus, from a superficial view, there seems to be a connection between an attestation and a trust relation. However, an unambiguous transformation of the attestation network to a trust network is not possible. There might be exceptions in a significantly limited trust model where for instance only one CA exists that must be trusted by definition.

3.4 Making a Trust Decision

We see the attestation and trust network as the foundation for deriving trust. These networks enable a RP to conduct a final trust decision concerning the usage of a supplied attribute. Basically, a trust decision considers all elements related to trust and judges the supplied attributes for acceptance.

Definition 3 (Trust decision). A trust decision D is a tuple $\langle T, B, V, S \rangle$ that is self-evaluating to a binary result either indicating *trust* or *no trust*. A trust decision D_e is made from the perspective of an entity e of the trust network. The tuple elements are:

- Trust function T computes a trust score for an attribute
- Trust base B represents trust ratings towards other entities
- Attestations base V comprise the attribute assertions
- Acceptance rules S defines the acceptance or rejection condition for an attribute

The trust function T is the main component of the decision that describes the aggregation of trust in an attribute. It considers the relationships of the underlying attestation and trust network. The trust base B is a partial graph of the trust network that is reduced to the trust relations originating from the entity e that conducts the trust decision. Furthermore, the attestation base V is a partial graph of the attestation network. This subgraph is a reduction to the attestations of the property for that the trust decision should be conducted. The result of the trust function is a trust score. In a simple case, a list of attestation issuers is accepted. A more complex function may mathematically aggregate trust values of different attestations to an overall score. The final result is matched against the acceptance rules. In general, a rule defines a threshold. If the computed trust score is higher than the threshold, the attribute is accepted for further processing. Otherwise, the characteristics are rejected.

3.5 Characteristics

In the previous section, we defined fundamental elements to depict an attribute assurance trust model. Based on these components, we can derive specific evaluation properties of the networks and the decision process.

Degree of Centralization (DoC): The degree of centralization in a network measures the concentration of relations towards a set of entities. In the attestation network, we focus on the originating entities of assertions. In the trust network, we concentrate on the trust receiving (TR) entities that obtain at least one trust rating. A minor number of attestation issuers respectively trusted nodes in relation to the overall set of entities refer to a chain of trust model. Hence, the attestation issuers or the trusted nodes are seen as a trusted third party. This is reflected by a DoC score that approaches 1. In contrast, a high proportion of attestation issuers or trusted nodes in the trust network reduce centralization and indicate a web of trust model. In this case, the DoC value is close to 0.

$$DoC_{AN} = 1 - \frac{|AP|}{|E|} \; DoC_{TN} = 1 - \frac{|TR|}{|E|}$$

Degree of Interconnection (DoI): The degree of interconnection measures the quantity of separated subgraphs (*SG*) within the attestation or trust network. DoI is related to the strongly connected component measure that is proposed by Ulrich et al. [26]. If solely one graph exists the whole network is interconnected. In case each node is a separate graph, the network is least interconnected possible. A subgraph reflects a trust community where entities rely on each other for the correctness of attestations. A DoI score of 1 describes a highly interconnected network. The metric applies for both the attestation and the trust network.

$$DoI = 1 - \frac{1-|SG|}{|E|}$$

Issued (IA) and Received (RA) Attestations: The number of attestations issued by a specific entity provides a measure of how active an entity is by providing attestations. The number of attestations that are received by a specific entity reflects its shape. Weakly and strongly attested properties build the foundation for its interaction with RPs.

Attestations for Acceptance (AfA): The metric reflects the minimum quantity of distinct attestations required for acceptance of an attribute at a RP under the condition of default acceptance rules. This measurement is used to evaluate the robustness of the trust function. For instance, AfA is 1 for PKI based on X.509 because one certificate is sufficient for acceptance.

Trust for Acceptance (TfA): The figure indicates the minimum required trust score for an attestation issuer to contribute to the calculated trust score of an attribute and towards its acceptance. Comparable to the previous metric, we use this measurement to assess the security of the trust function. A normalization of the trust model's trust ratings into an interval from [0,1] might be necessary to achieve comparability towards other schemes.

3.6 Security and Attacks

In this section, we interpret generic security objectives towards trust models in attribute assurance and describes attacks against them.

3.6.1 Security Objectives

The triad of availability, integrity and confidentiality reflect the main security objectives in information security. In attribute assurance, availability refers to obtainable and verifiable attributes. A regular user must be able to retrieve properties for its identity from any AP. Additionally, the attributes must be provided to the RP and the RP must be able to verify their origin if necessary. Concerning integrity, the user and the SP expects that attributes are authentic when they are issued. They must reflect reality. Furthermore, if the underlying properties get invalid also the attribute of the identity must be revoked promptly. Besides that, attributes should not be manipulated during the transfer between the entities. Confidentiality references the protection of private data. In particular, it should only be disclosed to authorized entities. Attributes of an identity may represent personal identifiable information of a user that require extraordinary protection. Attack vectors against confidentiality usually comprise transmission and storage protection of attribute data.

3.6.2 Attacks

In this paragraph, we elaborate on attacks on the attribute assurance trust model level. Therefore, we focus on attacks against availability and integrity because their underlying factors are captured in the abstract scheme. We omit the objective confidentiality due to its concentration on the implementation aspects of a trust management pattern.

Censorship: The censorship attack [3] targets the exclusion of a node from the service of an AP. Thus, the AP does not issue attribute attestations towards this entity. The entity is censored. The censorship attack can be motivated by the AP itself or it might be externally enforced on the AP. As a result, the attacked node is not able anymore to participate in interactions with RPs because required attributes are missing. Having several APs is a counter-strategy because the attack effort rises significantly to censor a node at all APs.

Denial of Service: In this context, the denial of service attack targets the AP and tries to prevent completely its attribute attestation service. The AP cannot issue or revoke attestations for any user. The attack affects the AP and its activities, but also restrict regular users to obtain assertions. In contrast to the censorship attack, a large number of nodes are affected. Furthermore, the attack is externally enforced on the AP because the AP has no interest to stop its complete service. As counter-strategy, the trust model must support plenty of APs to avoid a strong dependency on a single AP.

Attribute Forgery: The attribute forgery attack targets to deceive the AP into attesting a wrong property. This behaviour originates from a user that intends to obtain service from a RP under false pretences. The user achieves to circumvent verification procedures of the AP to get the false attribute value attested. This attack may have an impact on the RP and other entities concerning service consumption. As counter-strategy, the RP should not rely only on a single AP. Executing the attack against several APs increases the effort.

Rogue Attribute Provider: An adversary can set up one or more rogue APs to wrongly attest attributes. With this attack, a dedicated subgraph in the attestation and trust network can be built. A RP that falsely trusts rogue APs or applies a generic trust function that considers all APs might be prone to this attack. As a defence mechanism, highly trusted APs should only be considered.

Stale Information: The stale information attack [3] uses outdated information to obtain a service illegitimately. Within this attack, the perpetrator tries to circumvent the revocation mechanism of the AP. Thus, an attribute does not expire or will not get updated in case of changes. As consequence, a RP might still serve a user although the conditions do not hold anymore. Relying on several APs at the same time is a counter-strategy. Thus, the attacker must circumvent revocation mechanism at plenty APs.

Trust Base Manipulation: The trust base manipulation attack targets the trust information of the RP to influence a trust decision about attributes. The adversary increases the trust rating towards an AP or adds new APs with higher trust ratings. Evaluating a characteristic of a user, a property is accepted although it might be wrong. Thus, the RP would be deceived into providing service. Defence strategies can be found on the implementation level, e.g. client hardening.

3.7 Properties of a Secure Trust Model

The major components of an attribute assurance trust model are the attestation and the trust network as well as the trust decision process. The attestation network is solely a result of interaction between entities. Additionally, the trust network relies on subjective trust ratings between the nodes. These two components are an integral part of a trust scheme. However, they can hardly be influenced by modelling activities towards the security of the trust pattern. Studying the factors of the trust decision process, trust and attestation base are reductions of the respective network. Therefore, they are also not significant to determine a secure trust model. Trust function and acceptance rules remain. As the acceptance rules implement a threshold-based approval or rejection, they can be omitted in favour of the trust function. We can normalize the output of the trust function to incorporate differences in the meaning of a rule. Therefore, the trust function is the most significant component of an attribute assurance trust model. To obtain a secure trust model, the trust function must be attack-resistant against the outlined attacks against integrity and availability. Thus, the following properties are of high importance:

1. **High assurance for attribute authenticity:** Important for the RP and the user are correct and valid attributes to consume services. Therefore, attacks against integrity must be mitigated and highest trust on APs must be enforced.
2. **Low dependency on an AP:** The dependency towards one AP or a small number of APs facilitates attacks against integrity and availability. It is easier to execute the attacks against one AP in contrast to several APs to achieve a malicious goal.

4 Conclusion

We analyzed the structure of trust schemes in attribute assurance by formally specifying the attestation and trust network as the foundation. Subsequently, we studied the trust decision process that comprises the trust function, trust base, attestation base and acceptance rules. Based on this framework, we defined important characteristics and elaborated on security attacks against these trust models. As a conclusion, we determined that a secure trust model depends on the security of the trust function. The trust function must incorporate a high assurance that the attributes are authentic and a low dependency towards one attribute provider.

References

1. A. Jøsang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision,” *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.
2. D. H. McKnight and N. L. Chervany, “The meanings of trust,” University of Minnesota, Tech. Rep. MISRC 9604, 1996.
3. N. Alexopoulos, J. Daubert, M. Mühlhäuser, and S. M. Habib, “Beyond the hype: On using blockchains in trust management for authentication,” in *2017 IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications (Trustcom)*, 2017, pp. 546–553.
4. H. Gomi, “Authentication trust metric and assessment for federated identity management systems,” *IEICE Transactions on Information and Systems*, vol. 95-D, no. 1, pp. 29–37, 2012.
5. A. Grüner, A. Mühle, T. Gayvoronskaya, and C. Meinel, “A comparative analysis of trust requirements in decentralized identity management,” in *2019 Int. Conf. on Advanced Information Networking and Applications (AINA)*, 2019, pp. 200–213.

6. P. R. Zimmermann, *The Official PGP User's Guide*. Cambridge, MA, USA: MIT Press, 1995.
7. Internet Engineering Task Force. (2008) Rfc 5280. internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. (accessed on 2020-12-30). [Online]. Available: https://tools.ietf.org/html/rfc5280
8. A. Grüner, A. Mühle, M. Meinig, and C. Meinel, "A taxonomy of trust models for attribute assurance in identity management," in *2020 Workshops of the 34th Int. Conf. on Advanced Information Networking and Applications (WAINA)*, 2020, pp. 65–76.
9. A. Jøsang, "An algebra for assessing trust in certification chains," in *1999 Network and Distributed Systems Symposium (NDSS)*, 1999.
10. W. Yang, C. Huang, B. Wang, T. Wang, and Z. Zhang, "A general trust model based on trust algebra," in *2009 Int. Conf. on Multimedia Information Networking and Security (MINES)*, 2009, pp. 125–129.
11. J. Huang and D. Nicol, "A formal-semantics-based calculus of trust," *IEEE Internet Computing*, vol. 14, pp. 38–46, 2010.
12. S. Ries, S. M. Habib, M. Mühlhäuser, and V. Varadharajan, "Certainlogic: A logic for modeling trust and uncertainty," in *4th Int. Conf. on Trust and Trustworthy Computing (Trust)*, 2011, pp. 254–261.
13. A. Aldini, "A calculus for trust and reputation systems," in *2014 IFIP Int. Conf. on Trust Management (IFIP TM)*, 2014, pp. 173–188.
14. M. Carbone, M. Nielsen, and V. Sassone, "A formal model for trust in dynamic networks," in *First Int. Conf. on Software Engineering and Formal Methods (SEFM)*, 2003, pp. 54–61.
15. M. Kinateder, E. Baschny, and K. Rothermel, "Towards a generic trust model - comparison of various trust update algorithms," in *Third Int. Conf. on Trust Management (iTrust)*, 2005, pp. 177–192.
16. M. Fragkakis and N. Alexandris, "Comparing the trust and security models of mobile agents," in *Third Int. Symposium on Information Assurance and Security (IAS)*, 2007, pp. 363–368.
17. F. Moyano, C. Fernandez-Gago, and J. Lopez, "A conceptual framework for trust models," in *2012 Int. Conf. Trust, Privacy and Security in Digital Business (TrustBus)*, 2012, pp. 93–104.
18. H. El Bakkali and B. I. Kaitouni, "A logic-based reasoning about pki trust model," in *6th IEEE Int. Symposium on Computers and Communications (ISCC)*, 2001, pp. 42–48.
19. ——, "A predicate calculus logic for the pki trust model analysis," in *2001 IEEE Int. Symposium on Network Computing and Applications (NCA)*, 2001, pp. 368–371.
20. Haibo Yu, Chunzhao Jin, and Haiyan Che, "A description logic for pki trust domain modeling," in *3rd Int. Conf. on Information Technology and Applications (ICITA)*, 2005, pp. 524–528.
21. J. Huang and D. Nicol, "A calculus of trust and its application to pki and identity management," in *8th Int. Symposium on Identity and Trust on the Internet (IDtrust)*, 2009, pp. 23–37.
22. Z. E. Uahhabi and H. E. Bakkali, "A comparative study of pki trust models," in *2014 IEEE Int. Conf. on Next Generation Networks and Services (NGNS)*, 2014, pp. 255–261.
23. U. Maurer, "Modelling a public-key infrastructure," in *1996 European Symposium on Research in Computer Security (ESORICS)*, 1996, pp. 325–350.
24. J. Marchesini and S. Smith, "Modeling public key infrastructures in the real world," in *2005 European Public Key Infrastructure Workshop (EuroPKI)*, 2005, pp. 118–134.
25. M. Henderson, R. Coulter, E. Dawson, and E. Okamoto, "Modelling trust structures for public key infrastructures," in *2002 Australasian Conference on Information Security and Privacy (ACISP)*, 2002, pp. 56–70.
26. A. Ulrich, R. Holz, P. Hauck, and G. Carle, "Investigating the openpgp web of trust," in *2011 European Symposium on Research in Computer Security (ESORICS)*, 2011, pp. 489–507.
27. P.-A. Chirita, W. Nejdl, M. Schlosser, and O. Scurtu, "Personalized reputation management in p2p networks," in *2004 Int. Conf. on Trust, Security, and Reputation on the Semantic Web (ISWC)*, 2004, pp. 32–41.