Dynamic Trust-based Recertifications in Identity and Access Management

Christian Richthammer, Michael Kunz, Johannes Sänger, Matthias Hummer, Günther Pernul
Department of Information Systems
University of Regensburg
Regensburg, Germany
Email: {firstname.lastname}@wiwi.uni-regensburg.de

***Abstract*—Security compliance has become an important topic for medium- and large-sized companies in the recent years. In order to fulfill all requirements legally imposed, high quality identity management – particularly with respect to correct and consistent access control – is essential. In this context, the concept of recertification has proven itself to maintain the quality and correctness of access rights over a long period of time. In this paper, we show how the traditional recertification concept can be notably enhanced through involving the notion of trust. We thereto propose a trust-based recertification model and demonstrate its benefits by means of a realistic use case. Our dynamic concept can help to better spread the recertification overhead compared to the traditional approach with fixed periods. Furthermore, it aids in the identification of risky employees.**

***Keywords*—Computational trust, enterprise identity management, recertification, access control, compliance, identity and access management**

I. Introduction

The increase of compliance policies and regulations imposes new challenges for medium- and large-sized companies. To avoid legal consequences, the importance of compliance within enterprises is growing steadily. Capgemini [1] lists security compliance among the top IT trends of 2014, expressing the significance of the topic in practice. Similar conclusions can be drawn from PwC's report [2] underlining the increase of compliance staffing and budget. The handling of sensitive data, personal data and trading data is subject to several national and international requirements. As a prerequisite for registration at the US stock market, the actually national regulations of the Sarbanes-Oxley-Act from 2002 (SOX, [3]) are affecting companies worldwide. While at first glance not directly connected to IT systems, the initial requirements of SOX on accountability and auditing affect areas of Identity and Access Management (IAM) as well. However, the demands by SOX towards fraud detection, segregation of duties, compliance and audits can only be delivered with correct and consistent access control information. Similarly, knowledge about who can access what within the organization is of utmost importance in order to adhere to privacy protection of employee and customer data. Furthermore, continuous internal and external revisions are obligatory for organizations which want to acquire certifications of frameworks and standards such as ISO/IEC 27001 [4]. Additionally, especially regulated industries such as the finance sector (e.g. through Basel III [5]) and the health sector (e.g. through HIPAA [6]) are expressing their need for more automated and helpful tools and measurements in order to demonstrate proof of their compliance [2].

From a bird's eye view, structured IAM provides a centralized control center for managing (compliance) and reporting (auditing) users concerning the presented requirements. One of the practical methods for ensuring the correctness of access within an organization is the concept of recertification [7]. With these periodic inspections of access rights, an employee's correct set of authorizations can be renewed by a domain expert, thus allowing for the evaluation of audits. The overall goal of this paper is to aid companies in a semi-automated conduction of recertifications. In order to achieve this, we introduce computational trust concepts into the field of IAM. With this interdisciplinary work, we can help to identify employees whose access privileges should be recertified more often than others. This is based on the heterogeneity of employee positions in organizations. For instance, companies naturally tend to oblige employees in security relevant functions to be certified more often than low-privileged colleagues.

The remainder of the paper is organized as follows. We provide a short overview of the related work relevant to this paper in Section II before we present our novel trust-based recertification concept in Section III. In Section IV, we demonstrate its applicability by means of a use case using synthetic data based on real-world examples. Finally, we discuss the benefits and limitations of our proposal and provide a summary of our contributions and an outlook for future work in Section V.

II. Background and Related Work

In this section, we briefly introduce the most important characteristics of computational trust and how we use them in our proposal. This helps to impart a common understanding regarding the main contribution of the paper. Furthermore, we demarcate our work from related approaches that try to introduce trust concepts into IAM.

A. Computational Trust

Trust has been discussed in various research domains for decades, such as sociology, psychology, and economics. In this paper, we focus on the meaning of trust in the computer science community. In particular, we employ the ideas related to the formalization of trust as a computational concept. Since Marsh's [8] early work on this topic, a vast number of computation models and algorithms has been proposed in literature. For an extensive overview of the field, the interested reader is referred to existing surveys (e.g. [9], [10], [11]).

One of the most important properties of trust is its dynamic nature, meaning that trust can increase and decrease through new experiences and referrals. Moreover, trust is said to decay with time. These characteristics lead to the generally accepted proposition that new trust assessments are more important than old ones. We take this into account by basing our evaluation of the users' trustworthiness on the beta reputation system by Jøsang and Ismail [12], which relies on the beta probability density function. As outlined in Section III, beta models are a popular way to consider the decay of trust assessments.

B. Trust in Identity and Access Management

The integration of trust concepts into IAM has received increasing attention during the last years. At first, most interest has been dedicated to trust in federated IAM. Liu and Gao [13], for instance, extend the Security Assertion Markup Language (SAML) by a trust value that is calculated based on a subject's behavior. Employing this value in IAM procedures, malicious behavior can directly be reflected in inter-domain access permissions. In this way, subjects are encouraged to act properly. Moreover, Gao et al. [14] not only address the trust value of a subject but also involve the trustworthiness of a service provider in single sign-on mechanisms. They propose a dynamic trust policy language to support trust negotiation. Further approaches have been introduced in [15] and [16].

More recently, researchers have also started to consider the integration of trust into centralized IAM. As we focus on access control management in enterprise IAM, these approaches are particularly relevant to our proposal. Zhao et al. [17], for example, assign trust values as a minimum requirement for each role in an RBAC model. In their system, users are constantly rated by other actors and resources. Consequently, malicious behavior is directly reflected in a bad trust value and roles can immediately be revoked. Yang et al. [18] go one step further and provide trust values for the behavior in different situations. They argue that the trust value associated with a subject should be calculated for multiple contexts because the perception of trust is context-dependent. Further interesting approaches can be found in [19] and [20].

While the integration of trust in access control models is definitely a step into the right direction, all current approaches focus on the extension of one specific access control model and thus suffer from low flexibility. In this work, we propose a concept that is independent of the access control model in use. We thereby focus on the recertification process, which has also not been addressed in this context so far.

III. Trust-based Recertification Concept

Our concept for trust-based recertifications is based on the generic recertification process depicted in Figure 1. The process is a simplified version of the IAM lifecycle [21] and is reduced to the parts directly connected to recertifications.

At first, there has to be an initial provisioning stage in which an employee is assigned with permissions. In our trust-based recertification concept, we consider two main components: a time-related one and a usage-related one. In the initial provisioning, the time component is set to the maximum value (e.g. 1) whereas the usage component is assigned a neutral value (e.g. 0.5). The second stage represents the actual

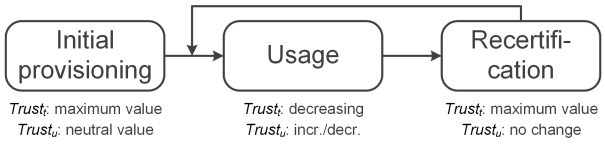

Fig. 1. Generic recertification process

activities of the employee between the initial provisioning and the recertification (or between two recertifications). Since there may be certain attribute and entitlement updates (e.g. acquiring permissions that are not officially approved), it is necessary to have domain experts assess conspicuous access control outliers. Depending on the outcome of the assessments, the usage-based trust value of the employee may increase or decrease. Irrespectively of this, his time-based trust value steadily decreases. Once the total trust value reaches a certain threshold, the recertification stage becomes necessary. Similarly to the initial provisioning, the recertification sets the time-related component back to the maximum value.

In the following, the different elements important during the usage stage are explained in detail. These are the time-related component (i.e. the temporal decay of trust), the usage-related component (i.e. the outlier assessments), and the recertification threshold.

A. Temporal Decay of Trust

As pointed out in Section II, one of the most important properties of trust is its decay with time. We take this into consideration with a time-related component. The component has to be defined in such a way that the total trust value reaches the ultimate threshold when the recertification is mandatory at the latest. This point in time is predefined by compliance requirements such as Basel III and SOX. For the sake of simplicity, we use the following linear decay function for the time-related component. It reaches 0 by no later than after one year, which we use as the predefined recertification deadline. Note that the linear decay function can easily be replaced by a progressive function, for instance. Similarly, the recertification deadline may be adapted to an organization's specific needs.

$$Trust_t(t) = 1 - (\omega_x x + \omega_y y)\frac{t}{360} \tag{1}$$

$Trust_t$ is the time component of the total trust value, t is the number of days since the last recertification, and $(\omega_x x + \omega_y y)$ is the decay factor. The default value for $(\omega_x x + \omega_y y)$ is 1, so that $Trust_t$ reaches 0 at the predefined recertification deadline of one year. ω_x and ω_y are used as weighting factors, whereby $\omega_x + \omega_y = 1$.

x considers properties of the observed employee such as his position in the organization and the characteristics of his contract. Table I provides an exemplary overview of these properties along with possible scales for their values x_k. x is defined as the average of these values. We use a scale from 1 to 2 with steps of 0.25, which results in five possible values per property. Preliminary considerations have shown the appropriateness of this scale. Nevertheless, more detailed observations might be considered for future work.

TABLE I. EXEMPLARY EMPLOYEE PROPERTIES

Employee property	Possible scale
Position	From manager ($x_1 = 1$) to clerk ($x_1 = 2$)
Entry date	From more than 30 years ago ($x_2 = 1$) to newly arrived employee ($x_2 = 2$)
Contract type	From permanent contract ($x_3 = 1$) to external contract ($x_3 = 2$)
Job history	From loyal employee ($x_4 = 1$) to competitor history ($x_4 = 2$)

y is affected by the criticality levels of the permissions of the employee. In order to assign a value to y, we use a classification scheme which is exemplary outlined in Table II. Similarly to the aforementioned employee properties, we use a scale from 1 to 2 with steps of 0.25. An employee is classified according to the sum of the criticality levels of his permissions. These depend on the internal directives of the organization and have to be determined in interviews with the responsible staff members. For example, the criticality level of high-risk permissions may be 15, the one for medium-risk permissions may be 5, and the one for low-risk permissions may be 1.

TABLE II. EXEMPLARY CRITICALITY CLASSIFICATION SCHEME

Employee criticality	Sum of permission criticalities
Very low ($y = 1$)	< 50
Low ($y = 1.25$)	$50 - 100$
Medium ($y = 1.5$)	$100 - 150$
High ($y = 1.75$)	$150 - 200$
Very high ($y = 2$)	> 200

B. Outlier Assessments

We further take account of the dynamic nature of trust by integrating a usage-related component into our trust calculations. This usage trust is based on positive and negative assessments of conspicuous outlier permissions. Positive means that the employee is officially approved to own the particular outlier permission. Negative means that he may have obtained it in an informal way. A typical example for this is an employee asking a colleague to quickly assign permissions to him without obtaining official approval beforehand. The outlier detection can be performed automatically with the help of access control data cleansing methods. For more details on these techniques, see [22]. The assessments are provided by domain experts and are aggregated with the help of a beta probability density function (PDF) according to the beta reputation system introduced by Jøsang and Ismail [12]. The reason for basing our usage-related component on the beta PDF is its suitability for describing the probability distribution of binary events. We calculate the component as:

$$Trust_u = \frac{\alpha}{\alpha + \beta} \tag{2}$$

In the original beta model, α is defined as $\alpha = r + 1$ and β is defined as $\beta = s + 1$. r is the number of positive assessments whereas s is the number of negative assessments. In this form, all assessments carry the same weight. This especially means that old assessments are just as important as more recent ones. However, Jøsang and Ismail [12] additionally propose a forgetting scheme that discounts old feedback by multiplying it with a forgetting factor $0 < \lambda < 1$. It is also possible to use different forgetting factors λ and σ for positive and negative assessments, respectively. Applying the forgetting scheme leads to $r = \sum_{k=0}^{n} r_k \lambda^k$ and $s = \sum_{k=0}^{n} s_k \sigma^k$.

This results in the following clarification of Eq. (2):

$$Trust_u = \frac{\sum_{k=0}^{n} r_k \lambda^k + 1}{\sum_{k=0}^{n} r_k \lambda^k + 1 + \sum_{k=0}^{n} s_k \sigma^k + 1} \tag{3}$$

r_0 and s_0 are the most recent assessments whereas r_n and s_n are the oldest ones. In case of a positive assessment, one has $r_k = 1$ and $s_k = 0$. In case of a negative assessment, one has $r_k = 0$ and $s_k = 1$. To illustrate the functioning of the forgetting scheme, Table III shows an example in which three assessments have taken place. The first assessment is negative, the following two assessments are positive. The employed forgetting factors are $\lambda = 0.7$ and $\sigma = 0.9$. This means that positive assessments are forgotten comparably fast whereas negative assessments have a considerable influence for a long time. Observing the values for r and s, it can be seen that the kth assessments are discounted by λ^k and σ^k, respectively. Nielsen et al. [23] call this principle "exponential decay".

TABLE III. FORGETTING SCHEME FOR A NEGATIVE (N) ASSESSMENT FOLLOWED BY TWO POSITIVE (P) ASSESSMENTS ($\lambda = 0.7, \sigma = 0.9$)

Assessments	r	s	α	β	$Trust_u$
N	0	1	1	2	0.33333
PN	$1 + 0$	$0 + 0.9$	2	1.9	0.51282
PPN	$1 + 0.7 + 0$	$0 + 0 + 0.81$	2.7	1.81	0.59867

By putting together the time-related and the usage-related component (cf. Eq. (1) and Eq. (3)) and providing the opportunity to assign different weights ω_t and ω_u to them, we receive the following metric for the total trust value of an employee:

$$Trust = \omega_t Trust_t + \omega_u Trust_u \tag{4}$$

C. Recertification Threshold

In order to be able to arrive at a particular recertification decision, the total trust value (cf. Eq. (4)) developed in the course of this section has to be related to a predefined threshold at which the recertification is required by law. This threshold has to be reached at the latest when the time-related component becomes 0. Thus, it has to be equal to the maximum value of the weighted usage-related component. Since the maximum value is reached if there are only positive and no negative assessments (i.e. $r_k = 1, s_k = 0$ for all $k = 0, ..., n$), the threshold is defined as follows. Note that the geometric series $\sum_{k=0}^{n} \lambda^k$ is equal to $\frac{1-\lambda^k}{1-\lambda}$ and converges to $\frac{1}{1-\lambda}$ for $\lim_{n\to\infty}$.

$$\theta = \lim_{n\to\infty} \omega_u \frac{\sum_{k=0}^{n} \lambda^k + 1}{\sum_{k=0}^{n} \lambda^k + 1 + 0 + 1} = \omega_u \frac{\frac{1}{1-\lambda} + 1}{\frac{1}{1-\lambda} + 2} \tag{5}$$

If the total trust value of an employee is above the threshold, he is able to activate his permissions without any restrictions. If it is below the threshold, the employee's permissions have to be recertified by a domain expert.

IV. Use Case

In the following, we demonstrate the practical applicability of our trust-based recertification concept in a fictional use case. Our company data has been designed according to practical information from a real-world example with industry-standard assumptions. The company – hereinafter called "Weyland Industries" – is a medium-sized enterprise in the robotics manufacturing industry. Its master data comprises 4,114 employees, which can be assigned a selection of 1,171 access privileges. This amounts to 86,104 user-access assignments in total. The assignments result from breaking down the access control model in place into a direct access model. Dissolving the initially hierarchical and aggregated access control helps in having a detailed view on each employee's access privileges. The employees are distributed within 343 departments in a typical hierarchical structure. The employee data is enriched with additional information from various applications allowing for a structured analysis including employee context. Furthermore, Weyland Industries is providing a list of 233 risky access privileges. 111 of them are marked as high-risk, the rest imposes medium risk to the respective activation.

The company is facing two challenges resulting in a need of improvement of the current processes. Up to now, the company has recertified the employees once per year, which leads to a significant overhead during the recertification period and presents obstacles to the daily manufacturing business. This reasons in the fact that business responsibles are drawn away from their daily work in order to come up with access control decisions by means of job functions and activities of their respective employees. Adding up to this issue, the marketing department has noted an increased customer need for certifications of qualifications and security standards. In order to proof a professional information security management to its customers, the strategic department of the company has decided to acquire the ISO/IEC 27001 certification. Section 11 of the Annex to ISO/IEC 27001 demands for structured deployment of managing access to resources. Furthermore, the certification requires a risk-based system in order to identify high-risk employees [4]. The two main goals are as follows:

- Business responsibles should be lifted from the heavy-weight recertification blocks.
- Employees' privilege assignments with risky access should be identified for complying with the ISO/IEC 27001 certification.

To achieve the two goals, Weyland Industries is planing on integrating our proposed approach into their existing Identity Intelligence System (IIS) which is monitoring and analyzing the functionality of the Identity and Access Management System (IAMS). In order to evaluate the functionality of our trust-based recertifications, the enterprise is testing its applicability in the marketing department. We consider the two employees Bolek and Botero to illustrate our concept. Table IV contains all details regarding their employee properties as well as their permission criticalities that are necessary to compute the decay factor of the trust-related component. The decay variables x and y are determined according to the specifications introduced in Section III-A. They are weighted equally.

During their time of employment, the two employees have been subject to several outlier assessments according to Section III-B. The outlier assessments inherently resolve the goal of the company project aiming at an identification of risky employees. Bolek has received three positive assessment followed by two negative ones and again by five positive ones. Botero has received one negative assessment in the first month of his employment. Since then, he has received nine positive ones. For the sake of simplicity, we assume that both employees do not receive any assessments during the year of consideration. Thus, the values for α, β and $Trust_u$ remain constant within this period. They are also included in Table IV. To calculate them, we use $\lambda = 0.7$ and $\sigma = 0.9$ (see Section III-B). In this first use case, we weight the time-related component with $\omega_t = 0.7$ and the usage-related component with $\omega_u = 0.3$. This yields the graphs depicted in Figure 2. The recertification threshold is $\theta = 0.3 \cdot \frac{\frac{1}{1-0.7}+1}{\frac{1}{1-0.7}+2} = 0.24375$.

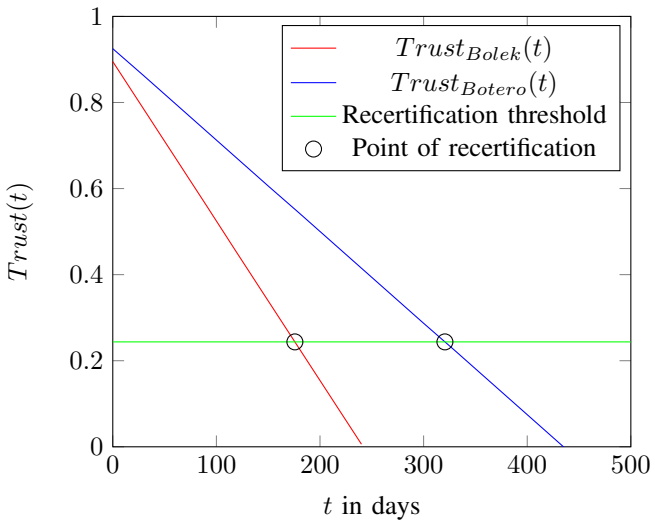

Fig. 2. Progression of the trust values of the two employees

TABLE IV. Recertification Data of the Two Employees

	Bolek	**Botero**
Position	IT clerk ($x_1 = 2$)	Strat. assistant ($x_1 = 1.25$)
Entry date	2 years ago ($x_2 = 1.75$)	8 years ago ($x_2 = 1.5$)
Contract type	3-year ($x_3 = 1.5$)	Permanent ($x_3 = 1$)
Job history	2 competitors ($x_4 = 2$)	Loyal employee ($x_4 = 1$)
$\boldsymbol{x}$	$\mathbf{1.8125}$	$\mathbf{1.1875}$
High-risk perm.	$13 \cdot 15 = 195$	$0 \cdot 15 = 0$
Medium-risk perm.	$16 \cdot 5 = 80$	$2 \cdot 5 = 10$
Low-risk perm.	$14 \cdot 1 = 14$	$31 \cdot 1 = 31$
$\boldsymbol{y}$	$\mathbf{2}$ (289)	$\mathbf{1}$ (41)
$\boldsymbol{Trust_t}$	$\mathbf{1 - 1.90625 \cdot \frac{t}{360}}$	$\mathbf{1 - 1.09375 \cdot \frac{t}{360}}$
Assessments	PPPPPNNPPP	NPPPPPPPPP
$\boldsymbol{\alpha}$	3.95346	4.19882
$\boldsymbol{\beta}$	2.12193	1.38742
$\boldsymbol{Trust_u}$	$\mathbf{0.65073}$	$\mathbf{0.75164}$
$\boldsymbol{Trust_{Bolek}(t)}$	$\mathbf{0.7 \cdot (1 - 1.90625 \cdot \frac{t}{360}) + 0.3 \cdot 0.65073}$	
$\boldsymbol{Trust_{Botero}(t)}$	$\mathbf{0.7 \cdot (1 - 1.09375 \cdot \frac{t}{360}) + 0.3 \cdot 0.75164}$	

Several observations can be made in connection with Figure 2. Firstly, Bolek's time trust decreases much faster

than Botero's. This is due to his comparably low position in the organization as well as his riskier permissions. Secondly, Bolek's usage trust is lower than Botero's because his two negative assessments have a stronger influence than Botero's. Note that both total trust values do not start at 1 because of the decreased usage trust of both employees. Thirdly, the definition of the recertification threshold is absolutely necessary. Otherwise, Botero's permissions would have to be recertified not until after the compliance deadline of one year. The overall goal of diversification of recertification periods is supported in this example by Bolek's early recertification after 178 days. Additionally, this aids in the identification of risky employees. While Botero's recertification point (321 days) is close to the one year period, Bolek can be seen as a risk factor within the company because of the rapid decay of his trust value. The rest of the company's employees needs to be analyzed in the same manner in order to fully complete the recertification goals stated above.

V. Conclusion

Recertification represents a means of maintaining compliant access control within an organization for the price of a high administrative effort. We argue that periodic recertifications are not the best choice and rather recommend to individually conduct them when appropriate. To determine these points in time, we employed a trust value based on employee context, temporal decay and expert information on excessive permission. Nevertheless, integration of company-specific requirements and data can easily be integrated into our approach. By introducing a use case, we demonstrated the applicability of our concept.

Despite the aforementioned benefits, there are some limitations to our proposal. One major issue is that we do not have any data on the suitability of different forgetting factors for our beta PDF-based usage component because there are no publications describing sophisticated evaluations of this [24]. Performing the necessary optimizations on our own is out of the scope of this workshop paper. Regardless of the forgetting factors, there may be better models than the beta PDF-based one for describing our usage component (e.g. hidden Markov models). However, the increased complexity of these models may make parameter prediction even more challenging [25]. Similarly to the parameterization of the usage component, optimizing the weighting factors included in our model is an aspect for future work as well. Moreover, there should also be experiments on replacing the linear decay function in our time component with more sophisticated metrics.

For future work, we intend to further investigate the presented approach. In a next step, we plan to carry out a real-world evaluation with an industrial partner and to integrate the presented solution into an IAMS. In addition, we plan to examine how this concept can be combined with other trust-based concepts within IAM.

Acknowledgment

The research leading to these results was supported by "Bavarian State Ministry of Education, Science and the Arts" as part of the FORSEC research association (http://www.bayforsec.de/).

References

[1] Capgemini, "Studie IT-Trends 2014," Capgemini, Tech. Rep., 2013.

[2] PricewaterhouseCoopers, "State of Compliance 2014 Survey," PricewaterhouseCoopers LLP, Tech. Rep., 2014.

[3] SOX, "Sarbanes-Oxley Act of 2002, PL 107-204, 116 Stat 745," 2002.

[4] ISO, "ISO/IEC 27001 – Information technology - Security techniques - Information security management systems - Requirements," 2005.

[5] Basel Committee on Banking Supervision, "Basel III - A Global Regulatory Framework for More Resilient Banks and Banking Systems," 2011.

[6] A. Act, "Health insurance portability and accountability act of 1996," *Public Law*, vol. 104, p. 191, 1996.

[7] T. F. Wave, "Role Management And Access Recertification," Forrester Research, Tech. Rep., 2011.

[8] S. Marsh, "Formalising Trust as a Computational Concept," Ph.D. dissertation, University of Sterling, 1994.

[9] J. Sabater and C. Sierra, "Review on Computational Trust and Reputation Models," *Artificial Intelligence Review*, vol. 24, no. 1, pp. 33–60, 2005.

[10] 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.

[11] J. Sänger, C. Richthammer, and G. Pernul, "Reusable Components for Online Reputation Systems," *Journal of Trust Management*, vol. 2, no. 5, 2015.

[12] A. Jøsang and R. Ismail, "The Beta Reputation System," in *Proc. of the 15th Bled Conf. on Electronic Commerce*, 2002, pp. 41–55.

[13] L. Liu and J. Gao, "Research on Trusted Federated Identity Management and Its Application," in *Proc. of the 1st Int. Workshop on Education Technology and Computer Science (ETCS)*, 2009, pp. 438–442.

[14] H. Gao, J. Yan, and Y. Mu, "Dynamic Trust Model for Federated Identity Management," in *Proc. of the 4th Int. Conf. on Network and System Security (NSS)*, 2010, pp. 55–61.

[15] M. V. Bhonsle, N. Poolsappasit, and S. K. Madria, "ETIS – Efficient Trust and Identity Management System for Federated Service Providers," in *Proc. of the 27th Int. Conf. on Advanced Information Networking and Applications (AINA)*, 2013, pp. 219–226.

[16] M. S. Ferdous and R. Poet, "Analysing Attribute Aggregation Models in Federated Identity Management," in *Proc. of the 6th Int. Conf. on Security of Information and Networks (SIN)*, 2013, pp. 181–188.

[17] L. Zhao, S. Liu, J. Li, and H. Xu, "A Dynamic Access Control Model Based on Trust," in *Proc. of the 2nd Conf. on Environmental Science and Information Application Technology (ESIAT)*, 2010, pp. 548–551.

[18] R. Yang, C. Lin, Y. Jiang, and X. Chu, "Trust Based Access Control in Infrastructure-Centric Environment," in *Proc. of the IEEE Int. Conf. on Communications (ICC)*, 2011, pp. 1–5.

[19] T. Zhao and S. Dong, "A Trust Aware Grid Access Control Architecture Based on ABAC," in *Proc. of the 5th IEEE Int. Conf. on Networking, Architecture, and Storage (NAS)*, 2010, pp. 109–115.

[20] N. Farooqi and S. North, "Evaluation of Practical Trust Based Access Control for XML Databases," in *Proc. of the 7th Int. Conf. for Internet Technology and Secured Transactions (ICITST)*, 2012, pp. 336–340.

[21] P. J. Windley, *Digital Identity*. Sebastopol, CA, USA: O'Reilly Media, 2005.

[22] L. Fuchs and G. Pernul, "HyDRo – Hybrid Development of Roles," in *Proc. of the 4th Int. Conf. on Information Systems Security (ICISS)*, 2008, pp. 287–302.

[23] M. Nielsen, K. Krukow, and V. Sassone, "A Bayesian Model for Event-based Trust," *Electronic Notes in Theoretical Computer Science*, vol. 172, pp. 499–521, 2007.

[24] E. ElSalamouny, K. T. Krukow, and V. Sassone, "An Analysis of the Exponential Decay Principle in Probabilistic Trust Models," *Theoretical Computer Science*, vol. 410, no. 41, pp. 4067–4084, 2009.

[25] M. E. G. Moe, B. E. Helvik, and S. J. Knapskog, "Comparison of the Beta and the Hidden Markov Models of Trust in Dynamic Environments," in *Proc. of the 3rd IFIP WG 11.11 Int. Conf. on Trust Management (IFIPTM)*, 2009, pp. 283–297.