2018-04-02

A New Dynamic Trust Model for "On Cloud" Federated Identity Management

Bendiab, K

http://hdl.handle.net/10026.1/12690

10.1109/ntms.2018.8328673
2018 9TH IFIP INTERNATIONAL CONFERENCE ON NEW TECHNOLOGIES, MOBILITY AND SECURITY (NTMS)
IEEE

A New Dynamic Trust Model for "On Cloud" Federated Identity Management

Keltoum Bendiab
LIRE laboratory
Frères Mentouri University
Constantine, Algeria
bendiab.kelthoum@umc.edu.dz

Stavros Shiaeles
Centre for Security, Communications and Network Research (CSCAN)
University of Plymouth, Plymouth, UK
stavros.shiaeles@plymouth.ac.uk

Samia Boucherkha
LIRE laboratory
Abdelhamid Mehri University
Constantine, Algeria
samchicki@yahoo.fr

***Abstract*— With the proliferation of Cloud-based services, Federated Identity Management (FIM) has gained considerable attention in recent years. It is considered as a promising approach to facilitate secure resource sharing between collaborating partners in the Cloud. However, current FIM frameworks such as OpenID, SAML, Liberty Alliance, Shibboleth and WS-Federation do not define a suitable trust model to allow dynamic and agile federation establishment. Hence, they cannot be deployed in dynamic and open environments like Cloud Computing. In this paper, we address this issue by presenting a new dynamic trust model that fulfils Cloud requirements. The proposed model introduces the theory of Fuzzy Cognitive Maps (FCM) into modelling and evaluating unknown entities trustworthiness in FIM systems.**

Keywords—Cloud Computing, Trust, Trust model, Federated Identity Management, Fuzzy Cognitive Maps.

I. Introduction

The exponential growth of Cloud applications is putting the IT security infrastructure under strain, in particular about Identity and Access Management (IAM) [1]. With this model, IT staffs face issues of managing and securing a whole arsenal of user's accounts, identifiers and passwords in a highly dynamic, multi-tenancy, insecure, and open environment. Identity Federation may seem like a promising approach to mitigate these identity management issues. It provides open, standardised and secure methods for a Cloud Service Provider (CSP) to identify users who are authenticated by an Identity Provider (IdP) [2].

This approach has many benefits for Cloud environments [3], such as increased simplicity by using cross-domain SSO (Single Sign-On) features, Seamless access to resources and reduced administrative costs of user accounts. However, current FIM frameworks like OpenID, SAML (Security Assertion Markup Language), Liberty Alliance, Shibboleth and WS-Federation are limited by the complexity of the underlying trust models that need to be set before inter-domain cooperation [4]. All these frameworks are based on pre-configured and static Circle of Trust (CoT), in which entities must establish trust relationships before the interactions take place [5]. This pre-configured CoT is usually hard to scale and not technically extendable which results in forming of closed communities [6]. In the case of OpenID, Relying Parties (RPs or CSP) must decide for themselves which OpenID Providers are trustworthy [7] because there is no trust model specified by this protocol to manage trust between these entities [8]. Furthermore, all these systems are suffering from many challenges such as lack of security and privacy [9], and limitations regarding interoperability and deployment [8]. As a result, existing FIM frameworks cannot be deployed in Cloud Computing which is a highly dynamic and open environment. In this model, trust between parties involved in a federation process should be managed dynamically without the need for pre-configured CoT. In this paper, we aim to address in particular this issue by proposing a new dynamic trust model that helps the successful integration of FIM systems and Cloud Computing. The proposed model introduces the Fuzzy Cognitive Maps (FCM) tool into modelling and evaluating the trust relationship between unknown entities in FIM systems.

The rest of the paper is structured as follows: Section II reviews and analyzes some related works and their limitations. Section III presents basic concepts about FCMs. After that, the proposed model is presented in Section IV. Then an application example of this model is presented in Section V. Finally, section VI reviews the content of the paper and presents the conclusions.

II. Related Works

Nowadays, dynamic FIM has become an interesting research area and several dynamic FIM systems have already evolved [4]. However, this section will be focused on representative systems for Cloud Computing environment as this is the scope of this research work.

In this context, a generic extension for the SMAL standard was proposed in [10]. The proposed extension facilitates the creation of federation relationships in a dynamic way between unknown entities and minimizes the dependency on previous configuration, making entities more autonomous and capable of taking trust decisions. However, this approach has many implementation issues because SAML is basically designed for limited-scale identity federation. Furthermore, it does not resolve problems of interoperability, privacy, and deployment. Authors in [5] have proposed a dynamic trust policy language that allows untrusted CSP to join automatically an existing CoT by negotiation. The policy language extends the Attribute-based Trust Negotiation Language (ATNL) to support dynamic trust management for Single Sign-On (SSO). This approach provides a flexible and dynamic trust management system. However, this policy language suffers from many privacy and deployment problems. In [11], authors have proposed a centralized trust management component named TSP (Trust Service Provider), which can automatically establish trust relationship between federation parties in runtime. So, when an organization wants to join a federation, it only needs to register each of its FIM parties on the TSP and then communicate securely with all other parties within the federation. The centralized architecture of this model decreases significantly their scalability since the list of trusted entities could become very large as the number of parties increases. In addition, this model has many security challenges. Recently, several Dynamic FIM works based on Cloud Identity Broker-model have emerged [6], [12] and [13]. This model introduces a trusted third party as a trust broker to manage trust relationships among services in-Cloud. With this trustable intermediary, the transitive federation could be established dynamically and to a broader range of Cloud services, reducing significantly the cost of trust established with external Cloud services. However, the broker brings serious security and privacy risks because identity data are stored and processed in the public Cloud.

This study reveals that none of the studied systems has addressed all the trust management aspects related to security, privacy, scalability, interoperability, implementation and deployment. Each of these mechanisms addresses one aspect of trust but not others. Each system is designed specifically for a particular application used for specific purposes. As a result, there is a strong need for an efficient trust model to solve the issue of dynamic identity federation in Cloud Computing. The main goal of this work is to address this trust issue by presenting a new dynamic trust model. The later used the theory of Fuzzy Cognitive Maps (FCM) in the modelling and evaluating the trust relationship between unknown entities in FIM systems.

III. Fuzzy Cognitive Maps (FCM)

FCM is typically signed fuzzy weighted digraph. It consists of nodes which represent variable concepts of the modelled system, and signed weighted arcs or edges which describe the causal relationships between these concepts and interconnect them [14]. Concepts represent key factors and attributes of the modelled system, such as inputs, outputs, states, events and goals [15]. Each signed weighted arc W_{ij} represents the degree to which the concept C_i influences the concept C_j. It is described by a non-linear transformation function $f(C_i, C_j)$ which takes values in the [-1, 1] interval [14]. The value of W_{ij} can express positive ($W_{ij}>0$) or negative ($W_{ij}<0$) or no relationship ($W_{ij}=0$) between the concepts C_i and C_j. The sign of W_{ij} indicates whether the relationship between the two concepts is direct or inverse [15].

The FCM is represented in a (n x n) weight connection matrix called W [14], where n is the number of concepts (nodes). The row i represents the causality between concept C_i and all other concepts in the map [15]. The state vector called A(1xn) represents current values of the n concepts (nodes) in a particular iteration. The value of each concept is obtained by computing the influence of other concepts to the specific concept using the calculation rule of equation (1) [15].

$$A_i(t) = f\left(\sum_{i=1, i\neq j}^{n} A_j(t-1).w_{ji}\right) \qquad (1)$$

Where $A_i(t)$ is the value of concept C_i at time t, $A_j(t-1)$ is the value of concept C_j at time t-1, and f is a threshold function to convert the output of each computation into the range [0, 1].

IV. Proposed Model

First, we need to explain the core idea of the proposed trust model. As can be seen in figure 1, each user gets his identity from a trusted IdP. If the CSP does not trust this IdP (1), the CSP and IdP can use the proposed trust model to compute the trustworthiness of each other in real time (2). Based upon the final trust value, the CSP decides to establish a connection with the target IdP and vice versa. When "*Trustworthiness-evaluation*" algorithm is successful, a trusted connection is automatically established between the CSP and IdP (3).

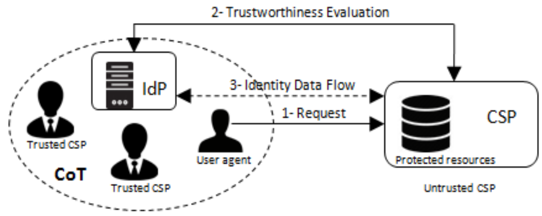

Fig. 1. The general architecture of the proposed model

The proposed trust model is described in graphical illustration using the FCM inference to handle uncertainty and fuzziness in trust. Concepts are entity's trustworthiness and its influencing features in the context of FIM, and weighted arcs represent the impact of the trust influencing factors to the trustee's trustworthiness.

A. Trust features in FIM

Trust is the most complex relationship among entities in distributed computing environments because it is extremely subjective, context-dependent, non-symmetric, uncertain, and partially transitive [16]. It is founded on particular beliefs or features of trustworthiness that an entity (trustor) has about another entity (trustee) [16]. According to [17], [18] and [19] the commonly relevant beliefs which have a direct influence on the entity's trustworthiness are summarized in table 1:

TABLE I. Beliefs of trustworthiness

Trust feature	*Description*
C1: Ability	It refers to the perceived competence level of an entity to perform some intended behaviour [39]. It allows the trustor to dynamically form an opinion about another entity [19]
C2: Intention or willingness to trust	It is the extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security, even though negative consequences are possible [16].
C3: Privacy	It is the ability of an entity to determine whether, when, and to whom information about itself is to be released or disclosed [19]. "A privacy policy has a positive relationship with trust".

C4: Security	It refers to the trustor's perception on the trustee's ability in fulfilling security requirements [18], such as authentication, authorization, integrity and availability.
C5: Dependability	It refers to the trustor's perception on the trustee's ability in fulfilling reliability, maintainability, usability, availability and safety requirements [18].

In the FIM context, there is no unified standard to select trust factors. There are only few research projects dealing with analyzing and identifying trust factors in FIM such as [20], [21], [22] and [23]. Based on these works, we have proposed the following trust factors (Table 2).

TABLE II. TRUST FACTORS IN FIM

Trust feature	*Description*
C6: Reputation	Reputation can be derived from IdP or CSP past experience or opinions reported by third parties. It can be used to guide behaviours of potential partners in future situations.
C7: User privacy	The IdP must preserve the user privacy by using anonymous or pseudonymous identifiers and allowing the user to choose and provide consent regarding the attributes that it wants to release to the CSP [20].
C8: Limited Disclosure	The SP will ask only for the minimum number of user attributes that are required to access any of its services and will use them only for the stated purpose(s).
C9: Communications	The claims holding user attributes must be digitally signed and exchanged between the IdP and the CSP over secure channels by using secure communication protocols such as SSL.
C10: Confidentiality	The IdP has satisfactory mechanisms for registering, storing and issuing user attributes safely and securely.
C11: Integrity	Ensuring the integrity and the quality of the identity credentials by using an audit and verification mechanism.
C12: Availability	Ensuring that a system is operational and that it is accessible to those who need to use it; adequate measures should be in place to prevent and detect the malfunctions of the system
C13: Authentication	The IdP registers users securely, authenticates them and releases attributes as per requirements.
C14: Authorization	The SP adheres to the non-disclosure of attributes, not abuses the released attributes, and maintains agreed access control policies.
C15: Prior transactions	Through prior interactions history, CSP (IdP) may evaluate trust level given to IdP (CSP). Lack of prior transactions may contribute to fragile trust among unknown parties.
C16: Interoperability	Interoperability refers to the degree of technical, operational and legal interoperability between the CSP and IdP.

The trust relationship between the IdP and CSP in Dynamic FIM is bidirectional; each entity must decide to trust or not the other entity. The IdP needs to confirm if it is secure to collaborate with an unknown CSP. Similarly, the CSP will have to decide if it is secure to accept authentication statements issued by a specific IdP. So, the trustworthiness of each entity must be identified. Table 3 presents the causal relationships between the previous trust features for both CSP and IdP. These causal relationships have been identified based on reported works [18, 23]. Sign (+) means feature 1 is positively influenced by feature 2. If feature 2 has a positive value, feature 1 increases, otherwise it decreases.

TABLE III. CAUSAL RELATIONSHIPS BETWEEN TRUST FEATURES

Trust Features	CSP	IdP
Ability	▫ (+) Security, (+) Privacy, (+) Prior transactions.	
Intention	▫ (+) Reputation.	
Security	▫ (+) Privacy ▫ (+) Dependability ▫ (+) Limited Disclosure ▫ (+) Authorization ▫ (+) Availability ▫ (+) Communications	▫ (+) Privacy ▫ (+) Dependability ▫ (+) Confidentiality ▫ (+) Authentication ▫ (+) Integrity ▫ (+) Availability ▫ (+) Communication
Privacy	▫ (+) Security ▫ (+) Communications ▫ (+) Limited Disclosure ▫ (+) Authorization	▫ (+) security ▫ (+) user privacy ▫ (+) communications ▫ (+) confidentiality ▫ (+) Integrity ▫ (+) authentication
Dependability	▫ (+) Availability, (+) Interoperability.	
Reputation	▫ (+) security ▫ (+) privacy ▫ (+) limited disclosure ▫ (+) authorization ▫ (+) prior transactions.	▫ (+) security ▫ (+) privacy ▫ (+) prior transactions.
User privacy	Non-influencing factor	▫ (+) Integrity ▫ (+) authentication ▫ (+) confidentiality ▫ (+) communication
Integrity and confidentiality	Non-influencing factor	▫ (+) authentication
Authentication	Non-influencing factor	▫ (+) communications
Prior transactions	▫ (+) communication	
Trustworthiness	▫ (+) Security, (+) Privacy, (+) Ability, (+) Intention, (+) Dependability.	

B. Trust modelling using FCM

As shown in figures 2 and 3, the proposed trust model is described as a direct graph G(C, E). Where C= $\{C_1, C_2, \ldots, C_{17}\}$ is a finite set of nodes, and E=$\{ e_{ij} \mid i, j \in C, E \subseteq C \times C \mid / W_{ij} \in [-1, 1]\}$ is a finite set of edges. The graph contains three layers of nodes. The lowest nodes (C_6, …., C_{16}) are the concepts which have an indirect influence on the entity's trustworthiness, the middle nodes (C_1, …, C_5) are the trust features which have a direct influence on the entity's trustworthiness, and C_{17} is the output node which represents the final trust value. Based on this value, the CSP decides to establish a connection with the target IdP and vice versa.

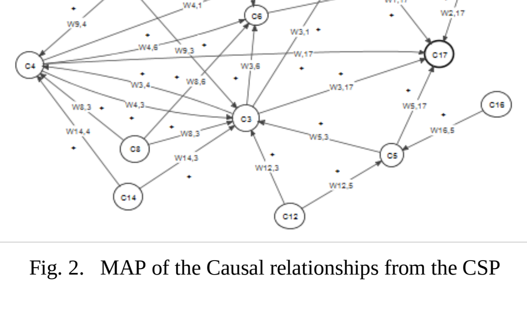

Fig. 2. MAP of the Causal relationships from the CSP

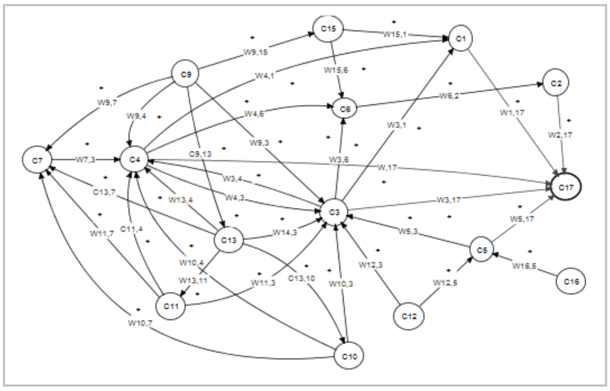

Fig. 3. MAP of the Causal relationships from the IdP.

Based on previous maps (figures 2, 3), an initial version of weight matrix can be built for both CSP and IdP (Tables 4 and 5).

TABLE IV. INITIAL WEIGHT MATRIX OF CAUSAL RELATIONSHIPS FROM THE CSP

	C1	C2	C3	C4	C5	C6	C8	C9	C12	C14	C15	C16	C17
C1	0	0	0	0	0	0	0	0	0	0	0	0	$W_{1,17}$
C2	0	0	0	0	0	0	0	0	0	0	0	0	$W_{2,17}$
C3	$W_{3,1}$	0	0	$W_{3,4}$	0	$W_{3,6}$	0	0	0	0	0	0	$W_{3,17}$
C4	$W_{4,1}$	0	$W_{4,3}$	0	0	$W_{4,6}$	0	0	0	0	0	0	$W_{4,17}$
C5	0	0	$W_{5,3}$	0	0	0	0	0	0	0	0	0	$W_{5,17}$
C6	0	$W_{6,2}$	0	0	0	0	0	0	0	0	0	0	0
C8	0	0	$W_{8,3}$	$W_{8,4}$	0	$W_{8,6}$	0	0	0	0	0	0	0
C9	0	0	$W_{9,3}$	$W_{9,4}$	0	0	0	0	0	0	$W_{9,15}$	0	0
C12	0	0	$W_{12,3}$	0	$W_{12,5}$	0	0	0	0	0	0	0	0
C14	0	0	$W_{14,3}$	$W_{14,4}$	0	$W_{14,6}$	0	0	0	0	0	0	0
C15	$W_{15,1}$	0	0	0	0	$W_{15,6}$	0	0	0	0	0	0	0
C16	0	0	0	0	$W_{16,5}$	0	0	0	0	0	0	0	0
C17	0	0	0	0	0	0	0	0	0	0	0	0	0

TABLE V. INITIAL WEIGHT MATRIX OF CAUSAL RELATIONSHIPS FROM THE CSP

	C1	C2	C3	C4	C5	C6	C7	C9	C10	C11	C12	C13	C15	C16	C17
C1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$W_{1,17}$
C2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$W_{2,17}$
C3	$W_{3,1}$	0	0	$W_{3,4}$	0	$W_{3,6}$	0	0	0	0	0	0	0	0	$W_{3,17}$
C4	$W_{4,1}$	0	$W_{4,3}$	0	0	$W_{4,6}$	0	0	0	0	0	0	0	0	$W_{4,17}$
C5	0	0	$W_{5,3}$	0	0	0	0	0	0	0	0	0	0	0	$W_{5,17}$
C6	0	$W_{6,2}$	0	0	0	0	0	0	0	0	0	0	0	0	0
C7	0	0	0	$W_{7,4}$	0	0	0	0	0	0	0	0	0	0	0
C9	0	0	$W_{9,3}$	$W_{9,4}$	0	0	$W_{9,7}$	0	0	0	0	$W_{9,13}$	$W_{9,15}$	0	0
C10	0	0	$W_{10,3}$	$W_{10,4}$	0	0	$W_{10,7}$	0	0	0	0	0	0	0	0
C11	0	0	$W_{11,3}$	$W_{11,4}$	0	0	$W_{11,7}$	0	0	0	0	0	0	0	0
C12	0	0	$W_{12,3}$	0	$W_{12,5}$	0	0	0	0	0	0	0	0	0	0
C13	0	0	$W_{13,3}$	$W_{13,4}$	0	0	$W_{13,7}$	0	$W_{13,10}$	$W_{13,11}$	0	0	0	0	0
C15	$W_{15,1}$	0	0	0	0	$W_{15,6}$	0	0	0	0	0	0	0	0	0
C16	0	0	0	0	$W_{16,5}$	0	0	0	0	0	0	0	0	0	0
C17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

C. *Trustworthiness evaluation algorithm*

The pseudo-code bellow is used to obtain the final trust value based on the initial values of the state vector $A_{initial}$ (0).

Algorithm: Trustworthiness-evaluation

Input

- *State Vector $A_{initial}$ $(C_1, C_2, \dots C_n)$. (t=0)*
- *Weight matrix $W_{initial}$ $[W_{ij}]$ / i,j={1,…., n}*

Output

- *Trust/Distrust decision and the state vector $A_{final}(t)$.*

Begin

1. *Read State vector $A_{initial}$ (0) and the weight matrix $W_{initial}$*
2. *For iteration step K*
   a. *Update the State vector according to equation (1)*
   b. *If (A(t+1) = A(t)), stop, Else go to step 2*
3. *Return the final Values of the state vector A_{final} (t) and the final value of trust (C_{17}).*
4. *Return Trust/Distrust decision*

End

V. APPLICATION EXAMPLE: CLOUD APIS

In this section, we present an application example in order to illustrate the feasibility of our trust model. The application example focuses on "insecure Cloud APIs" (Application Programming Interfaces) which is one of the three major security concerns in Cloud Computing [24]. CSPs publish a set of APIs that customers can use to manage and interact with cloud services. Service provisioning, management, orchestration, and monitoring are all performed using these interfaces [25]. The security and availability of general cloud services are depending on the security of these basic APIs [24]. Most Cloud players such as Google, Amazon, Salesforce and Microsoft use OAuth and OpenID protocols to secure their APIs [25]. However, there is no trust model specified by these open protocols to manage trust between CSPs and IdPs (OpenID or OAuth Providers) [7]. CSPs must decide by themselves which IdPs are trustworthy. Many companies believe that OpenID implementation lacks the necessary confidence level in user identity trust [7]. Poor management of trust in these protocols increase significantly many security and privacy issues [26] such as identity theft, unauthorized account access, embarrassment, Phishing, social engineering, replay attacks using old identity assertions, data breach, man-in-the-middle attacks, session hijacking etc. Our trust model is an effective method to enhance security and privacy in Cloud APIs by determining the trustworthiness level of the IdP by using the following method. An average value of the trustworthiness is computed as follow:

$$AVR(x) = \begin{cases} 0, & x < 0.5 \\ \dfrac{x - 0.5}{0.5} \times 100\%, & x \geq 0.5 \end{cases}$$

Where, x is the final value of trust (C_{17}) obtained using the algorithm described in section 4.C. If AVR(x) ≥ 50% the IdP is consider as trusted. Else, it is considered as untrusted. Each API can define their proper thresholds according to their security policy.

As can be seen in Fig. 4, before calling the API, the user (application) must obtain a temporary access token from a trusted IdP (1). Then, the user calls the API by adding the access token to the parameters of the request (2). The token is signed in order to prove the identity of the issuing authority. Before evaluating the token legitimacy and gives its decision to allow or deny access to the protected resources, the API compute the trustworthiness level of the IdP (3). If the trust level is insufficient, the API refuses authentication statements issued by this IdP, otherwise it goes to the evaluation of the token legitimacy with the IdP. The proposed extension can make Cloud APIs more secure and protect them against malicious IdPs.

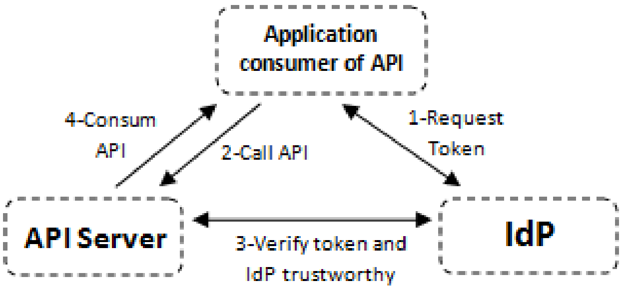

Fig. 4. The Trust Management model for Cloud APIs.

VI. CONCLUSION & PERSPECTIVES

The poor management of trust in existing FIM solutions causes the major integration hurdles of FIM systems and Cloud Computing. The problem of establishing a trust relationship between unknown entities is not covered by these solutions. In this paper a new dynamic trust model based on FCMs has been proposed. The effectiveness of the FCM inference tool has been widely proven through the literature to model uncertainty of trust. It suitably represents the causal relationships that exist among trust and its influencing factors in the context of FIM. This approach allows the dynamic creation of federations based on the resulting trust value which can make Cloud service provisioning and user interaction easier and more flexible. As a result, FIM systems will be more scalable and flexible to successfully deploy in Cloud Computing environments.

As future work, we expect to apply the proposed model in a real Cloud environment in order to carry out tests and experiments. The implementation of this model is actually in progress.

References

[1] S. Saini, and D. Mann, (2014). Identity Management issues in Cloud Computing. International Journal of Computer Trends and Technology, 9(8), pp.414-416.

[2] A. Bhardwaj, and V. Kumar, (2014). Identity management practices in cloud computing environments. *International Journal of Cloud Computing*, 3(2), p.143.

[3] J. Jensen, “Benefits of Federated Identity Management - A Survey from an Integrated Operations Viewpoint,” in Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2011, pp. 1–12.

[4] H. Gomi, “An Authentication Trust Metric for Federated Identity Management Systems,” in Security and Trust Management, Springer Berlin Heidelberg, 2011, pp. 116–131.

[5] H. Gao, J. Yan, and Y. Mu, “Dynamic Trust Model for Federated Identity Management,” in 2010 Fourth International Conference on Network and System Security, 2010.

[6] H. Y. Huang, B. Wang, X. X. Liu, and J. M. Xu, “Identity Federation Broker for Service Cloud,” in 2010 International Conference on Service Sciences, 2010.

[7] N. Duan and K. Smith, “IDentiaTM - An Identity Bridge Integrating OpenID and SAML for Enhanced Identity Trust and User Access Control,” in Imaging and Signal Processing in Health Care and Technology / 772: Human-Computer Interaction / 773: Communication, Internet and Information Technology, 2012.

[8] E. Maler, and D. Reed, (2008). The Venn of Identity: Options and Issues in Federated Identity Management. IEEE Security & Privacy Magazine, 6(2), pp.16-23.

[9] P. Aparajita, and R. Jatinderkumar, (2012). An Investigation of Challenges to Online Federated Identity Management Systems. International Journal of Engineering Innovation & Research, 1(2), pp.104-108.

[10] P. A. Cabarcos, F. A. Mendoza, A. Marín-López, and D. Díaz-Sánchez, “Enabling SAML for Dynamic Identity Federation Management,” in Wireless and Mobile Networking, Springer Berlin Heidelberg, 2009, pp. 173–184.

[11] J. Jiang, H. Duan, T. Lin, F. Qin, and H. Zhang, “A federated identity management system with centralized trust and unified Single Sign-On,” in 2011 6th International ICST Conference on Communications and Networking in China (CHINACOM), 2011.

[12] B. Zwattendorfer, D. Slamanig, K. Stranacher, and F. Hörandner, “A Federated Cloud Identity Broker-Model for Enhanced Privacy via Proxy Re-Encryption,” in Communications and Multimedia Security, Springer Berlin Heidelberg, 2014, pp. 92–103.

[13] K.Lin, Haiyin Lu, T. Yu, and C. Tai, “A Reputation and Trust Management Broker Framework for Web Applications,” in 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service.

[14] E. Papageorgiou, and J. Salmeron, (2013). A Review of Fuzzy Cognitive Maps Research During the Last Decade. IEEE Transactions on Fuzzy Systems, 21(1), pp.66-79.

[15] C. Castelfranchi, R. Falcone, and G. Pezzulo, “Integrating Trustfulness and Decision Using Fuzzy Cognitive Maps,” in Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2003, pp. 195–210.

[16] D. Harrison Mcknight, N. (2017). The Meanings of Trust Citeseerx.ist.psu.edu. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.155.1213, last viewed August. 2017.

[17] Leading with Trust. 2017. *Dependability | Leading with Trust*. Available at: https://leadingwithtrust.com/category/dependability/. last viewed juin 2017.

[18] X. Zhang and Q. Zhang, “Online trust forming mechanism,” in Proceedings of the 7th international conference on Electronic commerce - ICEC ’05, 2005.

[19] Z. Yan, P. Zhang, and A. Vasilakos, (2014). A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42(1), pp.120-134.

[20] J. Wu, Y. Chen and Y. Chung, (2010). Trust factors influencing virtual community members: A study of transaction communities. Journal of Business Research, 63(9-10), pp.1025-1032.

[21] A. Jøsang , J. Fabre, B. Hay, J. Dalziel, and S. Pope, (2005). Trust Requirements in Identity Management. In In ACSW Frontiers '05: Proceedings of the 2005 Australasian workshop on Grid computing and e-research.. Newcastle, Australia, 2005. Newcastle, New South Wales, Australia: ACM. 99-108.

[22] M. S. Ferdous and R. Poet, “Analysing attribute aggregation models in federated identity management,” in Proceedings of the 6th International Conference on Security of Information and Networks - SIN ’13, 2013.

[23] M. S. Ferdous, G. Norman, A. Jøsang, and R. Poet, “Mathematical Modelling of Trust Issues in Federated Identity Management,” in Trust Management IX, Springer International Publishing, 2015, pp. 13–29.

[24] U. Kylau, I. Thomas, M. Menzel, and C. Meinel, “Trust Requirements in Identity Federation Topologies,” in 2009 International Conference on Advanced Information Networking and Applications, 2009.

[25] Cloud Security Alliance. (2017). Top Threats - Cloud Security Alliance. Available at: https://cloudsecurityalliance.org/group/top-threats/#_overview, last viewed August. 2017.

[26] J. Wang, X. Bai, H. Ma, L. Li, and Z. Ji, “Cloud API Testing,” in 2017 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 2017.

[27] F. R. Kusters, and G. Schmitz, “A Comprehensive Formal Security Analysis of OAuth 2.0,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS’16, 2016.