2019-09

# FCMDT: A novel fuzzy cognitive maps dynamic trust model for cloud federated identity management

Bendiab, K



10.1016/j.cose.2019.06.011
Computers and Security
Elsevier

# FCMDT: A Novel Fuzzy Cognitive Maps Dynamic Trust Model for Cloud Federated Identity Management

Keltoum Bendiab, Stavros Shiaeles, Samia Boucherkha, and Bogdan Ghita

***Abstract*—Efficient identity management system has become one of the fundamental requirements for ensuring safe, secure and transparent use of cloud services. In such a borderless environment, entities belonging to different network domains need to cooperate dynamically with each other by exchanging and sharing a significant amount of personal information in a scalable, effective and seamless manner. The traditional approach to address this challenge has been identity federation, aiming to simplify the user experience by aggregating distributed rights and permissions. However, the current federated identity management solutions are missing mechanisms to achieve agile and dynamic trust management, which remains one of the biggest obstacles to their wide adoption in cloud computing. In this paper, we aim to address this issue by introducing a novel dynamic trust model for Federated Identity Management. The proposed model relies on fuzzy cognitive maps for modelling and evaluating trust relationships between the involved entities in federated identity management systems. This trust mechanism facilitates the creation of trust relationships between prior unknown entities in a secure and dynamic way and makes Federated Identity Management systems more scalable and flexible to deploy and maintain in cloud computing environments. In addition, we propose a set of trust features for Federated Identity Management, which serves as a basis for modelling and quantifying the trust level of unknown entities. The effectiveness of the proposed trust model is proven through performance analysis and experimental results.**

***Index Terms*—Cloud computing, fuzzy cognitive maps, federated identity management, FIM, IdP, trust management.**

## I. Introduction

SECURE and efficient identity management in and across clouds is one of the main challenges currently faced by cloud computing [1], [2], [3]. In such a borderless environment, a wide range of stakeholders, including cloud consumers, businesses, partners and loud providers, need to cooperate dynamically with each other by exchanging and sharing a massive amount of resources and users' sensitive data in a scalable, effective and seamless manner [2],[3]. In this context, Federated Identity Management (FIM) is considered the most useful solution to achieve reliable and effective collaboration among various domains that simplifies the user experience by allowing efficient authentication mechanisms and use of identity information from data distributed across multiple domains [4], [5]. It typically involves Identity Providers (IdPs) and Service Providers (SPs) in a trust structure called Circle of Trust (CoT), based on business agreements [5]-[7]. The IdP is responsible for the complete user management and does the authentication process in order to validate the user identity [6], as well as sharing identity information with various trusted SPs in the CoT. Meanwhile, the SP provides access to services and protected resources to users who are authenticated by a trusted IdP [6]. FIM provides many benefits for cloud environments [5], [6], such as increased simplicity by using cross-domain SSO (Single Sign-On) features, reduced number of credentials, seamless access to resources, and reduced administrative costs of user accounts [5]-[7].

The research community proposed several FIM systems. Security Assertion Markup Language (SAML) [8] and WS-Federation [9] are the predominant use case in these systems because of the scale of their deployment in several sectors (enterprise, educational networks, e-government, etc.). They are already implemented in many products, and serve as a foundation for the majority of identity federation protocols including Liberty Alliance [10] and Shibboleth [11]. In addition, well-known protocols OpenID [12], OpenID connect [13], FIDO (Fast ID Online) [14] and SCIM (Simple Cloud Identity Management)[15] are also lightweight FIM systems originally designed for relatively simple applications. All these frameworks typically follow a similar architecture based on pre-configured, static and closed CoT, in which interactions are only possible with pre-configured entities [7],[16]. The pre-established CoTs are typically rigid and have poor scalability, which leads to closed and isolated communities [6], [16]. Moreover, trust relationships are manually set and managed by administrators using trust anchor lists with a public key infrastructure [16], [17]. While convenient for setting up long-term relationships on server-to-server communication, such a trust model is unsuitable for dynamic environments such as cloud computing [18], where trust between parties within a federation process should be created dynamically on-demand instead of being statically defined. In the case of OpenID, OpenID connect, and SCIM, there is no specified model to manage trust between CSPs and OpenID providers, as CSPs must decide by themselves which OpenID providers are trustworthy [8].

Poor management of trust in these systems carries significant security and privacy risks [7]. Identity theft within an IdP

K. Bendiab is with the Department of Electronics , University of freres Mentouri, Constantine, Algeria, e-mail: (bendiab.kelthoum@umc.edu.dz).

S. Shiaeles and B. Ghita are with the Centre for Security, Communications and Network Research (CSCAN). University of Plymouth, Plymouth, UK, e-mail: (stavros.shiaeles@plymouth.ac.uk),(bogdan.ghita@plymouth.ac.uk) .

S. Boucherkha is with the Faculty of New Technologies of Information and Communication, Abdelhamid Mehri University Constantine, Algeria, e-mail: (samchicki@yahoo.fr).

Manuscript received xxxxx, 2018; revised xxxxx xx, xx.

or an SP, misuse of identity information by SPs and IdPs, and trustworthiness of the user are the most active problems and concerns in FIM [6]. The evidence from many studies shows that the sharing and processing of user sensitive information by SPs and IdPs typically involves the collection of user data without user consent [7], [16], [18]. Collected data can be subsequently compromised or improperly disclosed by malicious CSPs and IdPs, which may lead to further information leakage. These issues are further complicated in cloud environments due to their highly dynamic, multi-tenancy, insecure, and open nature.

Motivated by the shortcomings of existing FIM frameworks and aiming at contributing to solve the cloud computing identity management issues, especially the lack of agile and dynamic trust management, we propose in this paper a new trust model that allows dynamic and secure management of trust relationships between unknown entities in cloud environments. The main contributions of this paper are as follows:

- A comprehensive set of trust features needed to build trust between CSPs and IdPs in the context of FIM is proposed. The proposed set is used as a basis to model and quantify the trust level of unknown entities.
- A dynamic trust management model for FIM is proposed. The proposed model relies on Fuzzy Cognitive Maps (FCM) for modelling and evaluating the trustworthiness of unknown entities (e.g CSPs or IdPs) based on the proposed set of trust features. The effectiveness of FCMs to model the uncertainty of trust in complex and dynamical systems was widely proven by prior studies [19]-[22].

Applying the proposed trust model, a CSP can predict the trust level of the target IdP in real time and decide whether to establish or not a trust relationship with it and vice versa, which allows trust relationships to be established on-demand and makes the FIM approach more suitable for cloud environments. The trust model presented here extends and improves our prior work in [24].

The rest of the paper is organized as follows: Section II provides a critical review of the current state of the art in dynamic FIM. Then, Section III presents the basic concepts of FCMs and we define the set of trust features for FIM in section IV. We introduce the proposed system in section V. Then, the implementation and the experimental results are presented and analysed in Section VI. In Section VII, we conduct a comparison between our proposal and representative trust management models specifically built for cloud computing environments. Finally, Section VIII summarises the paper and outlines our future work.

## II. RELATED WORK

Dynamic trust management in FIM systems represents a topical research area and several dynamic FIM systems have already been introduced by prior studies conducted by individuals or research and international groups [25]-[31]. In [32], the ETSI *(European Telecommunications Standards Institute)* proposed a set of recommendations to achieve ad-hoc federation establishment based on dynamic SLA (Service Level Agreement) negotiations. The study shows that using bilateral static agreements is not feasible for a global scale federated internet. In this regard, the ABFAB *(Application Bridging for Federated Access Beyond Web)* working group from the IETF *(Internet Engineering Task Force)* proposed the ABFAB Architecture [33] that addresses the problem of dynamic trust establishment in non-web-based services. The proposed architecture outlines the need for a TRP *(Trust Router Protocol)* for the creation of dynamic relationships between providers. The main functions of the TRP are the distribution of information about existing trust relationships within the ABFAB federation and allow a new provider to be dynamically added to the federation. The *"Distributed Dynamic SAML"* [34] is another project proposed by the Internet2 group. The aim of this work is to achieve the distribution and dynamism that can solve challenges regarding deployment, scalability and interoperability of existing SAML federations. The notion of *"dynamic"* implies various means to support discovery and auto-configuration instead of static pre-arrangement between the interacting parties. The proposed work reduces the manual steps in trust management and makes federation establishment faster, but the trust management still depends on static pre-established relationships.

As SAML is one of the most widely used technologies to enable identity federations among different domains. There have been several works that provide proposals to tackle the problem of dynamism of this protocol such as works in [17], [27], [28], [29]. In [17], the authors proposed a generic extension for the SAML standard, which facilitates the creation of dynamic trust relationships between unknown parties and minimizes the dependence on previous configurations. Each entity will maintain a dynamic list called Dynamic Trust List (DTL), instead of the static TAL (Trust Anchor List), which will contain the list of joined entities in the same federation with their reputation data and will be updated dynamically as the federation evolves. That makes entities more autonomous in making trust decisions. However, this approach has significant implementation issues, as SAML is typically designed for limited-scale identity federation and it does not fully address interoperability, privacy, or deployment. In the same context, the authors in [25] proposed a dynamic trust policy language that extends the Attribute-based Trust Negotiation Language (ATNL) to support dynamic trust management for Single Sign-On (SSO) architectures and allows an untrusted CSP to automatically join an existing CoT through negotiation. This approach provides a flexible dynamic trust management but fails to capture a number of identity management issues, including questions regarding policy deployment and users privacy, such as using a vocabulary suitable only for a subset of users and organizations. In [30], the authors introduce the notion of Trust Service Provider (TSP) in the context of FIM. The TSP is a centralized trust management component which can automatically establish trust relationships between federation parties in runtime. It reduces the overhead of an organisation joining a federation, by requiring it to register each of its FIM parties on the TSP with a unique entityID and related metadata, and then communicate securely with all other parties within the federation. This approach makes trust management more flexible and empowers the user privacy. Un-

fortunately, the centralized architecture decreases significantly the scalability of FIM system since the list of trusted entities increases.

Several Dynamic FIM systems based on cloud identity broker-model have emerged, such as [26] and [31]. In [26], the authors introduce a trusted third party as a trust broker for the management of the trust relationship among services in-cloud or across clouds. With this trusted intermediary, the transitive federation may be dynamically established and be available to a broader range of cloud services. In [31], the authors propose an identity broker model that introduces federating identity brokers between SP and IdP. This new model enhances the user privacy through cryptographic mechanisms, in particular re-encryption proxies. These models reduce significantly the cost of trust established with external cloud services, although they have many security and privacy issues given that the identity data are stored and processed in the cloud. In addition, the model in [26] requires both the user and the CSP to rely on the same central identity broker for both identification and authentication.

This review reveals that none of the analysed systems is able to heuristically cover all the trust aspects in FIM, including security, privacy, scalability, interoperability, implementation and deployment, as they all have inherent trust implementation or scalability weaknesses. Furthermore, these systems do not include a dynamic trust model to provide them with the flexibility required for deployment and maintenance in cloud environments. Hence, we propose in this paper a novel dynamic trust model that addresses these trust challenges by using a Fuzzy Cognitive Map (FCM) to integrate FIM systems and cloud computing. The details of the proposed system are provided in the following sections.

## III. FUZZY COGNITIVE MAPS (FCM)

Fuzzy Cognitive Maps (FCMs) are a convenient, simple, and powerful qualitative technique used to model and compute trust in complex and dynamical systems [19], [22]. They were introduced by Kosko [19] enhancing the cognitive map [20] concept with the extension of the fuzzified causal relationships. FCMs bring several advantages over other modelling techniques, including great flexibility in representation [21], comprehensible structure and operations, capability to handle dynamic effects, ability to deal with fuzzy information, and transparency of the underlying model [35].

An FCM is typically a signed fuzzy weighted digraph. It consists of a set $(C_1, C_2, \ldots, C_n)$ of $n$ interconnected nodes representing variable concepts of the modelled system such as inputs, outputs, states, events, and signed weighted arcs which describe the causal relationships between these nodes and interconnect them [20]. These nodes (concepts) interact with each other to illustrate the dynamics of the model. Given two concepts $C_i$ and $C_j$, the edge weight $w_{ij}$ that interconnects them is a given value on the interval $[-1, 1]$ to indicate three possible types of relationship [21]: positive causality $(w_{ij} > 0)$, negative causality $(w_{ij} < 0)$ or independence $(w_{ij} = 0)$ between the two nodes; the value of $w_{ij}$ indicates how strongly concept $C_i$ influences concept $C_j$ [22]. The map is represented in a weight connection matrix $W_{n\times n}$ [26]. Within the matrix, row $i$ represents the causality between concept $C_i$ and all other concepts in the map [22]. The state vector $A_{1\times n}$ represents the current values of the n concepts (nodes) in a particular iteration. The value of each concept is computed from the influence of other concepts to the specified concept, by applying the calculation rule in Equation (1) [22].

$$A_i^{(t+1)} = f\left(A_i^{(t)} + \sum_{j=1 j\neq i}^{n} A_j^{(t)} \times W_{ji}\right) \tag{1}$$

where $A_i^{(t+1)}$ is the value of concept $C_i$ at time step $t+1$, $A_i^{(t)}$ is the value of concept $C_i$ at time step $t$, whereas, $f$ is the threshold or activation function for converting the output of each computation to the range $[0, 1]$ or $[-1, 1]$. The activation function can output either discrete or binary concept values or continuous concept values. One such widely used function in the literature is the hyperbolic tangent function [36], which is defined as fellow:

$$f(x) = Tanh(\lambda \times x) = \frac{e^{\lambda x} - e^{-\lambda x}}{e^{\lambda x} + e^{-\lambda x}} \tag{2}$$

Where $\lambda > 0$ is a constant parameter used to adjust a proper form or slope of the function named degree of fuzzification. Researchers should define a specific value to this parameter fitting the context under investigation [36]. For large $\lambda$ values (e.g., $\lambda > 10$), it approximates a discrete function, while, for smaller $\lambda$ values (e.g., $\lambda < 1$) it approximates a linear function. Fig. 1 shows an example of a simple FCM which consists of 5 nodes and 10 arcs. The rows in its weight connection matrix are the source nodes and the columns are the destination nodes [36].

| | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ |
|---|---|---|---|---|---|
| $C_1$ | 0 | $+w_{12}$ | 0 | 0 | $-w_{15}$ |
| $C_2$ | $+w_{21}$ | 0 | $-w_{23}$ | $-w_{24}$ | 0 |
| $C_3$ | 0 | 0 | 0 | 0 | $+w_{35}$ |
| $C_4$ | $+w_{41}$ | 0 | $-w_{43}$ | 0 | 0 |
| $C_5$ | 0 | 0 | $-w_{53}$ | $+w_{54}$ | 0 |

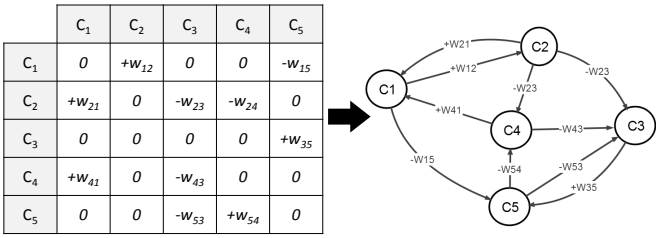


Fig. 1. A simple FCM and its weight connection matrix.

FCMs have shown promising results by successfully modelling real-world problems and indicating a strong ability to capture the dynamic aspects of the system's behaviour [19], [20], [21], [22]. In addition to the dynamic characteristics of FCMs [19] and their learning capabilities [22], the fuzzy nature of these qualitative tools makes them essential for modelling the uncertainty of trust in complex environments [19], [22]. Compared to the related works, this technique has the potential to improve the way that trust is established between unknown entities by increasing the flexibility and agility of the trust model. This has prompted us to propose a new dynamic and lightweight FCM-based trust computation approach, which attempts to exploit the advantages offered by

TABLE I
FEATURES OF TRUSTWORTHINESS FOR FIM

| Feature | Description | CSP | IdP |
|---|---|---|---|
| $C_1$: Security | It refers to CSP or (IdP) The ability of the CSP or (IdP) to fulfil security requirements, such as authentication, authorization, integrity, and availability. | × | × |
| $C_2$:Privacy | The ability of the CSP or (IdP) to fulfil privacy requirement, such as limited disclosure of user attributes, user consent and control. A privacy policy has a positive relationship with trust. | × | × |
| $C_3$:Dependability | The ability of the CSP or (IdP) to fulfil reliability, maintainability, usability, availability, and safety requirements. | × | × |
| $C_4$:Reputation | The uniformity of the CSP (or IdP) behaviour, derived from the trustee's past experience or opinions reported by third parties. | × | × |
| $C_5$: Anonymity | The ability of the IdP to preserve the user privacy by using anonymous or pseudonymous identifiers, allowing the user to choose and provide consent regarding the attributes that he/she wants to release to the CSP. | | × |
| $C_6$:Limited Disclosure | The ability of the CSP to request only the minimum number of user attributes required to access any of its services and to use them only for the stated purpose(s). | × | |
| $C_7$:Communications | The ability to digitally sign and exchange between the IdP and the CSP claims holding user attributes over secure channels by using secure communication protocols, such as HTTPS, SSL. | × | × |
| $C_8$: Confidentiality | The ability to provide IdP with satisfactory mechanisms to register, store and issuing user attributes safely and securely (strong encryption algorithm can proves the confidentiality of user attributes). | | × |
| $C_9$: Integrity | The ability of the IdP to ensure the integrity and the quality of the identity credentials by using an audit and verification mechanism. | | × |
| $C_{10}$: Availability | The ability to ensure 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, such as high uptime percentage. | × | × |
| $C_{11}$: Authentication | The ability of the IdP to use a strong authentication mechanism that releases users attributes as per the requirement. | | × |
| $C_{12}$: Authorization | The ability of the CSP to adhere to the non-disclosure of attributes, not abuse the released attributes, and maintain the agreed policies and procedures regarding access control. | × | |
| $C_{13}$: Interoperability | The degree of technical, operational, and legal interoperability between the CSP and the IDP. | × | × |
| $C_{14}$: Trustworthiness | The level of trust of the CSP or the IdP. | × | × |

these tools, in the dynamic and complex environment of cloud computing.

## IV. TRUST FEATURES FOR FIM

Trust is one of the most complicated concepts in open and dynamic environments because it is inherently subjective, context-dependent, non-symmetric, uncertain, and partially transitive [37]. It is influenced by many measurable and non-measurable properties including security, privacy, reliability, availability, and ability [37], [38]. In the context of FIM, the concept of trust and trust management is a widely studied topic and has been defined in numerous ways. For the purpose of this paper, we use the definition from [12].

*"Trust is the expression between parties that one party (trustor) to a relationship agrees to believe statements (also called claims) made by another party (trustee)"*.

This means that trust is founded on particular beliefs that the trustor has about the trustee. These beliefs are derived from strong evidence, such as history, experience, knowledge about the entity's nature, recommendations and certificates from trusted entities. This definition gives a directional relationship between the *"Trustor"* and the *"Trustee"*. However, in FIM, the trust relationship between the IdP and the CSP is bidirectional [18], both the IdP and the CSP have to trust each other. In particular, IdPs (as *trustors*) have to trust the SPs (as *trustees*) to securely handle and process a received user's identity data in a way that conforms to data protection laws [39], whereas the SPs (as *trustors*) have to trust the IdPs (as *trustees*) to correctly authenticate users that want to access their services and protected resources [39]. This means that the features influencing the trust level of each entity must be identified.

In FIM, there are many features that build trust between CSPs and IdPs [18], [39], [42]. However, there is no unified standard for selecting them, as there are only a few research projects that focus on the analysis and identification of trust features for FIM. Authors in [7], [18], [40]-[42] proposed a comprehensive set of trust features that are needed for the various FIM scenarios and topologies. In all these studies, the set of the required trust features is typically divided into security, privacy, and functional requirements. Proposed features in [41] were used in [42] to evaluate trust between entities in a federation and to assess the quality of service provided by IdPs or CSPs. In [43], the authors proposed a novel taxonomy of trust risks in cloud FIM, which were divided into three main categories: security and privacy, knowledge, and interoperability. The main purpose of this new classification is the dynamic creation of trust relationships between untrusted entities in a secure way. In [44], the Trans-European Research and Education Networking Association (TERENA) proposed

a set of features or requirements that must be covered in the real-world federation agreements in order to ensure sufficient trust and security among the different participating IdPs and CSP in real-world federations. This study shows that security and privacy were the most important considerations that must be taken into account before creating real-world federations.

To conclude this review, it is apparent that there is no standard or common set of contributor trust features to establish a dynamic federation between providers; instead, each of the studied works proposes a set of different features which cover some of the trust aspects in FIM. For example the interoperability is only considered in [7], [43], while it is an indispensable feature for establishing real world-federations [44]. Similarly, the availability is not considered in [38]-[40]. Moreover, in all those studies, the security and privacy are taken into account to some extent. For example, the security of the identity information in the transport level is ignored in [38] and [39]. Similarly, the limited disclosure, which is an important privacy related-feature [7], [44], is not considered in some studies. Consequently, in this paper, we aim to cover all the trust features needed to obtain a more accurate trust model. For that, we proposed a set of features that can influence the trust level of IdPs and CSPs. The features were chosen based on the TERENA recommendations for real-world federation agreements [44]. The proposed set improves our prior set of features in [24]. In addition, it is intended to be generic compared to previous work and useful for any FIM protocol. In this paper, we use the notion of "trustworthiness" as a measure to quantify the trust level of the CSP or the IdP.

Table I summarizes the proposed set of features. Sign $\times$ means that the trustworthiness of the CSP (IdP) is influenced by this feature. For example, the trustworthiness of the IdP is influenced by feature $C_{11}$ (Authentication) since this security-related feature ensures that the IdP has implemented the required methods to correctly authenticate users that want to access the CSP services and protected resources [44]. Meanwhile, the trustworthiness of the CSP is influenced by the feature $C_{12}$ (Authorization) which ensures that the CSP will securely handle a user's identity data [44]. Some features influence the trustworthiness of both the CSP and the IdP such as $C_7$ (Communication) [44] because in the context of FIM, it is strongly recommended to use secure communication protocols by the interacting parties (CSPs and IdPs).

## V. TRUST COMPUTATION MODEL

In this section, we present our trust computation model for FIM. the proposed model allows to dynamically measure the trustworthiness of unknown entities using the FCM tool. Before explaining how the trust model is applied, we begin first with an overview of the system architecture.

### A. System architecture

The proposed solution involves three entities: cloud users (CU), the IdP and the CSP. The CU send service requests to the CSP. Before providing the corresponding services for the CU, the CSP requires proper identification and authentication. The IdP is responsible for authenticating the registered CU and validates its identity. The IdP is ultimately trusted by the CU.

Trust establishment is managed directly between the CSP and IdP themselves, without the need for central authorities or intermediaries. Fig. 2 illustrates the core idea of our system, which involves three major stages. The first stage occurs when the CU sends a request to access the protected resources of a CSP but the CSP does not trust the IdP that handles its identity. Then, in stage 2, the CSP and IdP can use the proposed trust model to compute the trustworthiness of each other in real time. In this step, the trust management service computes a trust value related to the collaborating entity. Based on this trust value, it decides whether to initiate or not a transaction with the other entity. If the trustworthiness evaluation is successful, a trust relationship is automatically established between the CSP and the IdP in step 3. After that, the CSP and the IdP can exchange identity information in order to validate the CU identity.

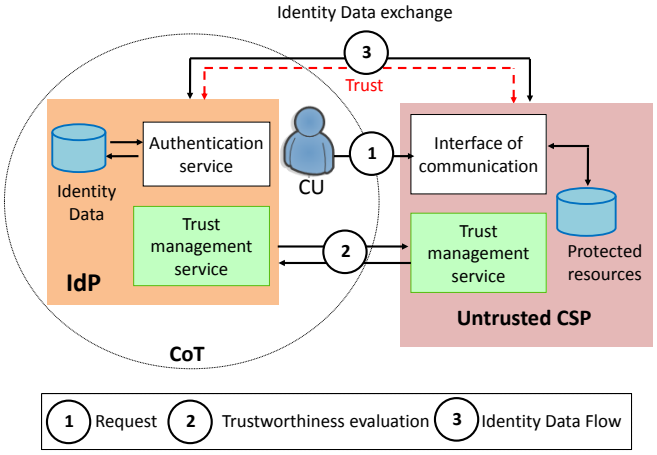


Fig. 2. The general architecture of the proposed system.

The trust management service is the core part of the system that evaluates the trust level of unknown entities by using the FCM. It takes initial values of trust features as input and then outputs the final trust value. Depending on this value, the CSP can decide whether to establish or not a trust relationship with the target IdP. The IdP performs the same steps to determine if it should interact with the CSP or not. The gathering of the trust features values is performed in the second stage, where the trust management service uses the information available in the entity metadata, the protocol in use, and the internal policies to quantitatively measure the initial values of the trust features. More details about the approach used to compute the initial features values are given in section V-C.

The following sections explain how the trust model is applied.

### B. FCM model Construction

In our approach, the trustworthiness of each entity (CSP or IdP) is modelled as a directed graph $G(C, E)$ using FCM, where $C = \{C_1, C_2, \ldots, C_n\}$ is a finite set of nodes that

represent the features influencing the CSP (or IdP) trustworthiness (Table I), and $E$ is a finite set of $k$ edges that represent the causal relationships between features, where $E = \{e_{ij}/i, j \in C, E \sqsubseteq C \times C\}$.

Each edge $e_{ij}$ that interconnects the $C_i$ and $C_j$ features has a relative weight $w_{ij} \in [-1, +1]$, which represents the degree by which node $i$ influences node $j$. As mentioned in section III, the weight $w_{ij}$ indicates three types of interrelationships between nodes, which are positive, negative, or zero. The positive interrelationship means that any change in the source node will positively change the situation of the destination node. The negative relationship is reverse and zero denotes that the two nodes do not have any interrelationship [22]. Since the possible value of $w_{ij}$ is not known precisely due to its subjectivity, the fuzzy set theory [45] is used to describe its vague nature using linguistic variables from the fuzzy set $T$. The fuzzy set T is comprised of nine linguistic variables, as presented in Table II together with the corresponding triangular membership functions, as shown in Fig. 3.

TABLE II
STATES OF THE FUZZY SET T

| Linguistic variables (States) | Membership function (Triangular) | Triangular membership region |
|---|---|---|
| Negatively very strong (NVS) | $\mu_{NVS}$ | (-1, -1, -0.75) |
| Negatively strong (NS) | $\mu_{NS}$ | (-1, -0.75, -0.5) |
| Negatively medium (NM) | $\mu_{NM}$ | (-0.75, -0.5, -0.25) |
| Negatively weak (NW) | $\mu_{NW}$ | (-0.25, 0, -0.25) |
| Zero (Z) | $\mu_{Z}$ | (-0.25, 0, 0.25) |
| Positively weak (PW) | $\mu_{PW}$ | (0, 0.25, 0.5) |
| Positively medium (PM) | $\mu_{PM}$ | (0.25, 05, 0.75) |
| Positively strong (PS) | $\mu_{PS}$ | (0.5, 0.75, 1) |
| Positively very strong (PVS) | $\mu_{PVS}$ | (0.75, 1, 1) |

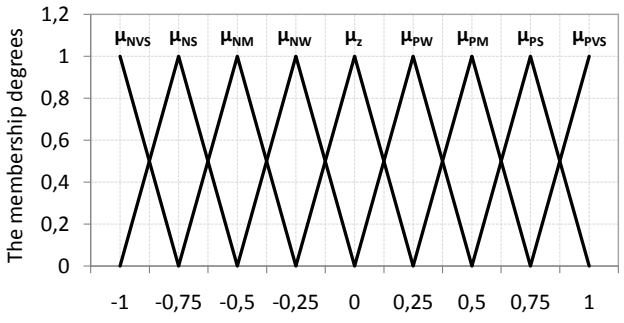


Fig. 3. Membership functions of the linguistic variable influence.

At this step of the FCM construction, the fuzzy value of the weight $w_{ij}$ is computed based on input from experts [22]. In this method, each expert estimates the strengths of the causal relationships between features based on their knowledge by using linguistic variables from the fuzzy set T ( Table II). Then, all the proposed linguistic values for the same weight $w_{ij}$, suggested by experts, are aggregated using the SUM fuzzy inference method and an overall linguistic weight is produced. At the end of this step, the Center of Gravity (CoG) defuzzification method [22] is used to calculate the crisp value of $w_{ij}$ which belongs to the interval $[-1, +1]$. A detailed description of this method is given in [22], [23]. This formally replicates the expert knowledge into the system, allowing it to take similar decisions based on the input factors.

As an example, if three experts 1, 2 and 3 propose the respectively linguistic values PS, PVS and PS for the weight $w_{ij}$, these linguistic variables (PS, PVS and PS) are summed and an overall linguistic weight is produced. Then, through the CoG method, the overall linguistic weight is transformed into the crisp value 0.79, as shown in Fig. 4.

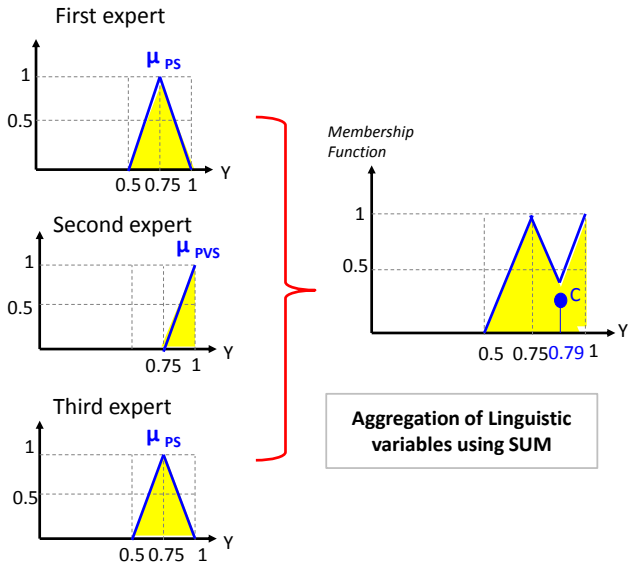


Fig. 4. Aggregation of the three linguistic variables (PS, PVS and PS) using the SUM technique. Point C is the numerical weight after defuzzification using the CoG method.

Based on the CoG result, the weights matrix for the CSP map (IdP map) can be built after determining all the weights using this approach. For each $w_{ij} \in W_{n \times n}$, if $i = j$, then $w_{ij} = 0$, because it is assumed that no concept can cause itself.

By using this method, each CSP or IdP can propose their own causal weights that meet their requirements because the various components of trust evolution do not have the same impact and importance. Depending on the scenario requirements, for a specific CSP in a specific context, the security of the IdP is more important than its availability. That means a CSP or an IdP can use a team of experts to apply the proposed technique and determine their weight connection matrix, as their internal policies change or differ from other use cases.

### C. Assurance levels for the trust features

Before computing the trust level of the unknown entity (CSP or IdP), the constructed FCM map (section V-B) must be initialized, which requires defining the initial value of each of the map's nodes. These values are based on measurements

TABLE III
ASSURANCE LEVELS FOR THE TRUST FEATURES

| Features | Metrics | Levels | Quantitative values | Source |
|---|---|---|---|---|
| $C_5$: Anonymity | No anonymity | Low | 1 | Defined high-levels of assurance based on the Kantara privacy framework for identity federation [49] and recommendations in [7] for identity management. |
| | Anonymous credentials | Medium | 2 | |
| | Anonymous credentials and anonymous authorization | High | 3 | |
| $C_6$: Limited disclosure | No user-control and consent | Low | 1 | |
| | Partial user-control and consent | Medium | 2 | |
| | Full user-control and consent | High | 3 | |
| $C_7$: Communications | Non secured channels (HTTP) | Low | 1 | Based on TERENA recommendations [44]. |
| | Partially secured channels (HTTPS) | Medium | 2 | |
| | Secured channels SSL/TLS protocol | High | 3 | |
| $C_8$: Confidentiality | Legacy-use encryption algorithm and key length | Very low | 1 | Based on NIST 800-131A specifications [49]. The encryption algorithm is used to provide confidentiality for identity information, while, the digital signature proves the integrity of the identity information. |
| | Restricted encryption algorithm and key length | Low | 2 | |
| | Deprecated encryption algorithm and key length | Medium | 3 | |
| | Acceptable encryption algorithm and key length | High | 4 | |
| | Approved encryption algorithm and key length | Very high | 5 | |
| $C_9$:Integrity | Legacy-use digital signature and key length | Very low | 1 | |
| | Restricted digital signature and key length | Low | 2 | |
| | Deprecated digital signature and key length | Medium | 3 | |
| | Acceptable digital signature and key length | High | 4 | |
| | Approved digital signature and key length | Very high | 5 | |
| $C_{10}$:Availability | $80\% \leq Availability < 95\%$ | Low | 1 | Defined high-level of assurance (Self-defined based on the study in [52]) |
| | $95\% \leq Availability < 99\%$ | Medium | 2 | |
| | $Availability \geq 99\%$ | High | 3 | |
| $C_{11}$:Authentication | Simple Password and PIN | Low | 1 | Based on NIST 800-63 Levels of Assurance (LOA) metrics [47] |
| | Single-factor authentication | Medium | 2 | |
| | Multi-factor authentication | High | 3 | |
| | Multi-factor authentication and Hard tokens | Very high | 4 | |
| $C_{12}$:Authorization | Simple password | Low | 1 | Defined high-levels of assurance based on the authorization type [51]. |
| | Identity-based authorization | Medium | 2 | |
| | Role-based authorization or Attribute-based authorization | High | 3 | |
| $C_{13}$:Interoperability | Only technical interoperability | Low | 1 | Defined high-levels of assurance based on TERENA recommendations [44]. |
| | Operational and technical interoperability | Medium | 2 | |
| | Legal and operational and technical interoperability | High | 3 | |

from the real system and gathered in the initial state vector $A_{initial}(0)$, where $A_{initial}(0) = \{C_1, C_2, \ldots, C_n\}, n \geq 1$.

The interactions in the FCM are caused by the change in the value of one or more concepts. In our approach, the initial values of the concepts are calculated from the information available in the entity metadata, assertions policies, and the protocol in use. The method used to compute the values of these nodes is inspired from the Level of Assurance (LOA) metrics defined by NIST 800-63 [47] to quantitatively measure the strength of identity proofing. This specification forms the basis of many frameworks for authentication assurance such as the Kantara framework [48], the ETSI specification for ad-hoc FIM [32], or the risk assessment framework in [43]. In our approach, each feature is assigned with qualitative levels of trust or confidence (i.e. assurance), including very low assurance, low assurance, medium assurance, high assurance, and very high assurance. These assurance levels are mapped to the quantitative values 1, 2 3, 4, and 5, respectively. Then, the mapping function (3) is used to convert the qualitative value of each feature to the range $[0, 1]$.

$$m(x) = \frac{v(C_i) - v_{min}(AL)}{v_{max}(AL) - v_{min}(AL)} \tag{3}$$

Where $v(C_i)$ is the quantitative value of the node $C_i$, $v_{min}(AL)$ is the minimum assurance level value and $v_{max}(AL)$ is the maximum assurance level value for the feature $C_i$. For example, if node $C_i = C_{11}$ (authentication) has a medium assurance level $(v(C_{11}) = 2)$ (Table III), the corresponding numerical value of this node in the interval [0,1] would be $(2-1)/(4-1) = 0.33$. While, if node $C_9$ (integrity) has a medium assurance level $(v(C_9) = 3)$ (Table III), the corresponding numerical value of this node in the interval [0,1] would be $(3-1)/(5-1) = 0.5$.

Following this approach, Table III overviews the different levels of assurance used to compute the initial values of features from $C_5$ to $C_{13}$. These levels were designed following the guidelines from well-known specifications such as NIST 800-63 [46], NIST SP 800-131A [47] and TERENA [44]. However, new assurance levels have been proposed for features for which there are no existing specifications.

For ease of understanding, Table III provides only a high-level definition of the LOAs, but more details can be found in the referenced documents. For example, for authentication, according to the assurance levels defined by NIST in [46], FIM transactions with a multi-factor authentication mech-

anism should have higher confidence level than a single-factor authentication mechanism or a simple password. For the anonymity feature, anonymous authorization should have the highest level of confidence because it ensures that a CSP never links an authorization request to information that identifies a cloud user [50]. Meanwhile, the confidentiality and the integrity of the identity information can be successfully achieved by using strong encryption algorithm and digital signatures [47]; for example, encryption algorithms with small key size (e.g. SHA-1) are considered to provide lower integrity strength than those with long key size (e.g. SHA-512) [49].

The initial values of the features $C_1, C_2, C_3$ and $C_4$ are set to 0 because, according to the TERENA recommendations [44] and the NIST.IR.8149 report [46], their values depend on the values of other features (Table I); for example, the value of feature $C_1$ (security) can be derived from the values of the integrity, confidentiality, authentication, and authorization features [44], [46]. Thus, the initial value of this feature is set to 0.

### D. Trustworthiness evaluation algorithm

This section presents the trust evaluation algorithm which uses the constructed FCMs in order to evaluate the trust level of CSPs and IdPs. First, the FCM map must be initialized, which means that the initial value of each of the map's nodes must be defined, as described in section V-C, and gathered in the state vector $A_{initial}(0)$ . After initialisation, the following steps are used to compute the last value of trust (node $C_{14}$).

- *Step 1*: Multiply the initial state vector $A_{initial}(0)$ and the weights matrix $W_{n\times n}$ defined by experts using the calculation rule in equations (1) and (2).
- *Step 2*: The resultant vector is used as the initial vector in the next iteration and it is updated using equations (1) and (2). Step 2 is repeated until $A(t) - A(t-1) \leq e = 0.001$. This termination condition helps to stop the iterative process of the trust evaluation algorithm.
- *Step 3*: Make the trust decision based on the last value of the node $C_{14}$ obtained in the final state vector $A_{final}(0)$.

The last value of the trustworthiness depends on the concepts values that belong to the interval [0, 1]. It also depends on the weights values of the causal relationships between features that belong to the interval [-1, 1]. Therefore, in the general case, the last value of trustworthiness is in the interval [-1, 1]. For the interpretation of the results, we propose in this paper an assessment only for the last value of the output node $C_{14}$ according to the following criteria:

$$R(x) = \begin{cases} Untrusted, x < 0.4 \\ Low\ trust, 0.4 \leq x < 0.6 \\ Medium\ Trust, 0.6 \leq x < 0.8 \\ Trusted, x \geq 0.8 \end{cases} \quad (4)$$

The "*Trusted*" criterion means that the evaluated entity to a certain extent respects all the trust features, which makes it more trustworthy. The "*Medium Trust*" criterion means that the CSP can trust the IdP and vice versa, but this can be risky because some trust features are not fully satisfied. While in the cases of "*Low Trust*" and "*Untrusted*", most or all of the trust features are not satisfied which makes the evaluated entity untrustworthy. Because there is no unified security perspective that can be followed by all existing federations, the proposed criteria can be modified according to each CSP and IdP security policies.

## VI. EXPERIMENTS AND ANALYSIS

In this section, we describe and analyse the experiments carried out over the proposed trust model in order to demonstrate its effectiveness and reliability.

1) The effectiveness will determine whether the proposed scheme can consistently provide trust calculation according to the assets and needs of the provider who is making the evaluation.
2) The computational efficiency of the trust system, benchmarked using the time overhead metric will determine whether the proposed trust model can manipulate the rising of input access requests without noticeable loss in quality of service.

The simulation experiments were performed on the cluster of the centre of High-Performance Computing of the FRERES MENTOURI University [1], runing on Intel (R) Xeon (R) CPU, 16 cores 2.20 GHz and 24 GB memory. In the cluster, each entity (CSP and IdP) is deployed in a separate VM, in which the trust management service is implemented. Fig. 5 illustrates the implemented architecture and its components.

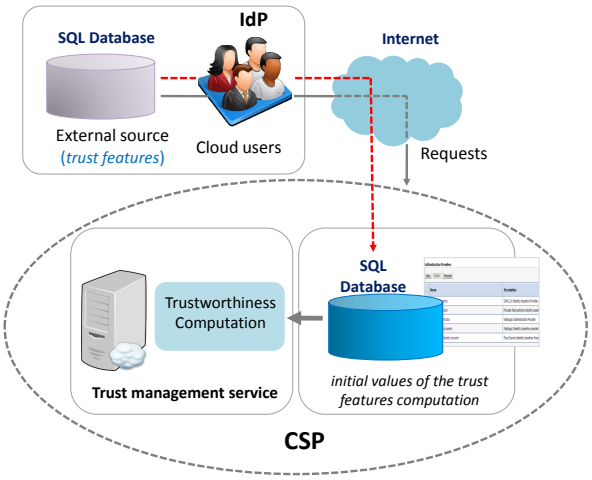


Fig. 5. Implemented architecture for the simulation scenarios.

The following sections describe the test scenarios and discuss the experimental results.

### A. Effectiveness of the proposed system for trust evaluation

The goal of these experiments is to evaluate the effectiveness of our approach for trust computation based on the needs of the provider that is making the evaluation (CSP or IdP). To this end, we have developed a proof-of-concept prototype

[1] https://centre.umc.edu.dz/hpc/

that implements the proposed trust model. Fig. 6 shows the prototype architecture for each entity. In the prototype, the trust management service was implemented using Java, the fuzzy system was developed based on the JFCM (Java Fuzzy Cognitive Maps) library which is an open source library, the weight connection matrix is defined in an XML document, and the trust features values are stored in a MySQL database. As shown in Fig. 6, in each of the test scenarios, we have as input an initial state vector $A_{initial}(0)$ gathering the initial values of the trust features and the proposed weight connection matrix. As output, we have a final state vector $A_{final}(0)$ representing the last state that it may arrive to.

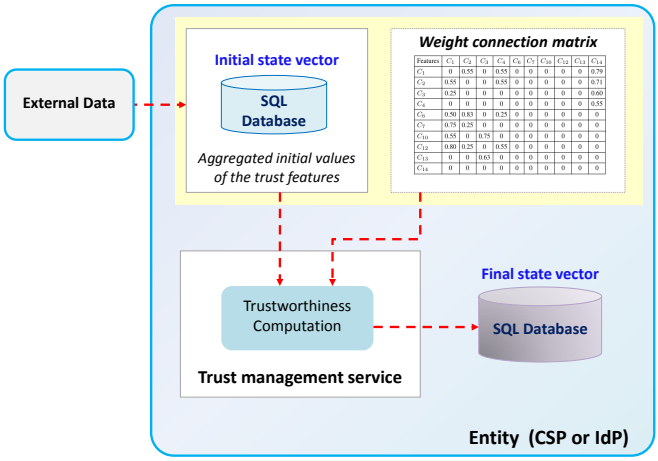


Fig. 6. Simplified schema of the trust evaluation process for each scenario.

In the simulation scenarios, we have used one CSP and one IdP. For each entity, we have proposed a weight connection matrix by using the approach described in section V.B, based on three experts' opinions. The weight connection matrix for the CSP $(W_{csp})$ and the IdP $(W_{IdP})$ are defined in Tables IV and V and the corresponding graphic descriptions are illustrated in Fig. 7 and Fig. 8. In the constructed matrix, the security-related features (confidentiality, integrity, authorization, authentication, availability and communication) were considered as the main influential features on the entities trustworthiness. That means lower values of these features should lead to lower trust levels and vice versa. Therefore, we proposed for each entity two different scenarios, one with low values for security-related features and the other with high values for these features.

*1) Value of the parameter $\lambda$:* As mentioned in section III, the hyperbolic tangent function (equation (2)) includes a lambda parameter for defining function slope which is the degree of fuzzification. Its value must be established by the FCM designer and can be chosen based on experiments or experience [35], [36]. In this context, Authors in [36] suggested that appropriate value of $\lambda$ can be arrived during experimentation phase because the choice of $\lambda$ affects the performance of the FCM model. In our approach, the value of this parameter is chosen based on experiments, where diverse values of $\lambda$ were examined through the validation analysis to use the proper one. Throughout the experimental analysis, we

TABLE IV
INITIAL WEIGHTS MATRIX OF CAUSAL RELATIONSHIPS FROM THE CSP

| Features | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_6$ | $C_7$ | $C_{10}$ | $C_{12}$ | $C_{13}$ | $C_{14}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $C_1$ | 0 | 0.55 | 0 | 0.55 | 0 | 0 | 0 | 0 | 0 | 0.79 |
| $C_2$ | 0.55 | 0 | 0 | 0.55 | 0 | 0 | 0 | 0 | 0 | 0.71 |
| $C_3$ | 0.25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.60 |
| $C_4$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.55 |
| $C_6$ | 0.50 | 0.83 | 0 | 0.25 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_7$ | 0.75 | 0.25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{10}$ | 0.55 | 0 | 0.75 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{12}$ | 0.80 | 0.25 | 0 | 0.55 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{13}$ | 0 | 0 | 0.63 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{14}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

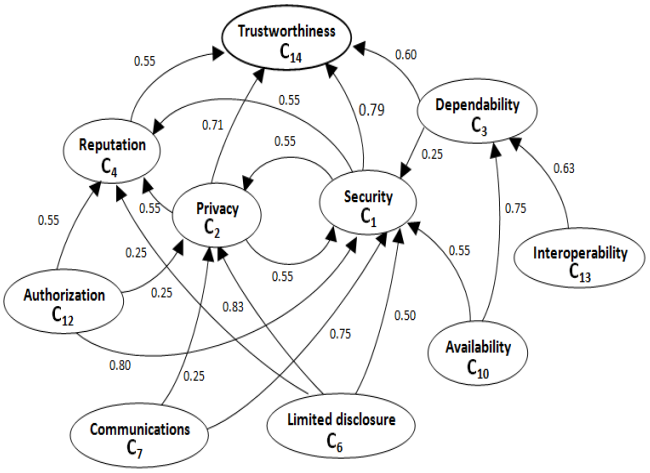


Fig. 7. MAP of the Causal relationships from the CSP.

TABLE V
INITIAL WEIGHTS MATRIX OF CAUSAL RELATIONSHIPS FROM THE IDP

| Features | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ | $C_7$ | $C_8$ | $C_9$ | $C_{10}$ | $C_{11}$ | $C_{13}$ | $C_{14}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_1$ | 0 | 0.55 | 0 | 0.55 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.79 |
| $C_2$ | 0.55 | 0 | 0 | 0.55 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.71 |
| $C_3$ | 0.25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.60 |
| $C_4$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.55 |
| $C_5$ | 0 | 0.55 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_7$ | 0.60 | 0.25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.25 | 0 | 0 |
| $C_8$ | 0.65 | 0.50 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_9$ | 0.65 | 0.60 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{10}$ | 0.55 | 0 | 0.55 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{11}$ | 0.65 | 0.65 | 0 | 0 | 0 | 0 | 0.55 | 0.55 | 0 | 0 | 0 | 0 |
| $C_{13}$ | 0 | 0 | 0.63 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{14}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

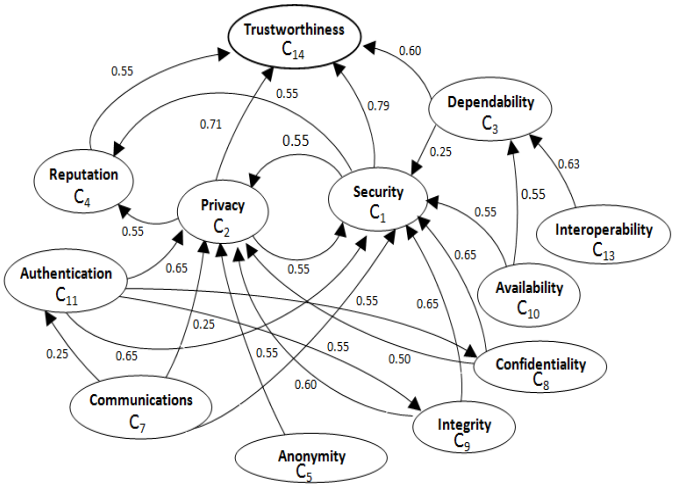


Fig. 8. MAP of the Causal relationships from the IdP.

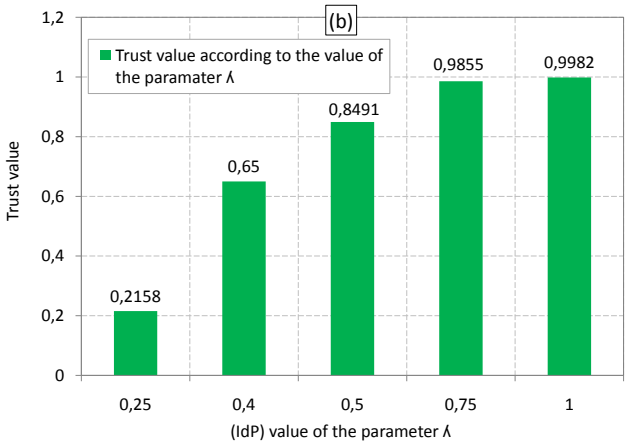


Fig. 10. The last trust values according to the different values of the parameter $\lambda$ for the IdP

applied many scenarios for the varying $\lambda$ values, by calculating the last trust value using the algorithm described in section V-D for each $\lambda$ value, for both the CSP and the IdP. The test scenarios are discussed below.

In the first group of experiments (a) we used the initial state vector $A_{initial}(CSP) = \{0, 0, 0, 0, 0.5, 1, 1, 1, 0.5, 0\}$ and the weight connection matrix from Table IV . In the second group of experiments (b), we used the initial state vector $A_{initial}(IdP) = \{0, 0, 0, 0, 0.5, 1, 0.75, 0.75, 1, 0.66, 0.5, 0\}$ with the weight connection matrix from Table V. The results for the group of experiments (a) and (b) are illustrated by the graphs in Fig. 9 and 10.

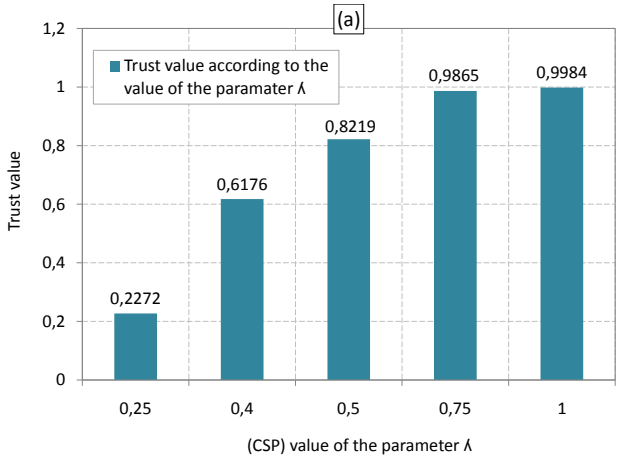


Fig. 9. The last trust values according to the different values of the parameter $\lambda$ for the CSP

From the obtained results, for both the CSP and the IdP, it was observed that the trust evaluations made by the system were most accurate and acceptable with the value of $\lambda$ being 0.5. While higher values of $\lambda$ lead to higher values of trust and lower values of $\lambda$ lead to lower values of trust. Based on the examined scenarios, we chose lambda=0.5 for our study.

*2) Scenarios for the IdP map:* In the first scenario, we have an IdP with a low security mechanism (low authentication mechanism ($C_{11} = 0$), low integrity ($C_9 = 0.25$), low confidentiality ($C_8 = 0.25$), non secure communication channel ($C_7 = 0$), low availability ($C_{10} = 0$)), and medium anonymity and interoperability ($C_5 = C_{13} = 0.5$). Intermediate features from $C_1$ to $C_4$ and the output $C_{14}$ are set to 0 to indicate no effect. In the second scenario, we have an IdP with a high security mechanism (high authentication mechanism ($C_{11} = 0.66$), high integrity ($C_9 = 0.75$), high confidentiality ($C_8 = 0.75$), high secure communication channel ($C_7 = 1$) , high availability ($C_{10} = 1$)), and medium anonymity and interoperability ($C_5 = C_{13} = 0.5$). Intermediate features from $C_1$ to $C_4$ and the output $C_{14}$ are set to 0. Thus, the initial state vectors for the two scenarios are presented in Table VI.

TABLE VI
INITIAL STATE VECTOR FOR EACH SCENARIO FOR THE IDP

| | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ | $C_7$ | $C_8$ | $C_9$ | $C_{10}$ | $C_{11}$ | $C_{13}$ | $C_{14}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Scenario 1 | 0 | 0 | 0 | 0 | 0.5 | 0 | 0.25 | 0.25 | 0 | 0 | 0.5 | 0 |
| Scenario 2 | 0 | 0 | 0 | 0 | 0.5 | 1 | 0.75 | 0.75 | 1 | 0.66 | 0.5 | 0 |

From Table VII(scenario 1), we can observe that after the FCM inference through the trustworthiness evaluation algorithm described in the previous section, the resulting IdP map starts to interact and simulates the trustworthiness evaluation procedure. New values of features were calculated for 4 iterations. From the results, we concluded that at the 4th iteration step, the FCM reaches the stop state and all the casual values were propagated through intermediate features. The last trust value is $C_{14} =$ **0.3632** which means that the trustworthiness level of this IdP is low (*Untrusted*) according to the criterion in Equation(4).

In the second scenario (Table VIII), the final state vector is reached at 3 simulation steps with a final trust value $C_{14} =$ **0.8491** which means that the trustworthiness level of this IdP is high (*Trusted*) according to the criterion in (4).

From these experiments, we conclude that the security-related features (authentication, confidentiality, integrity, availability and the communication channel) have a high influence

TABLE VII
FEATURES VALUES FOR EACH ITERATION STEP (IDP MAP) FOR THE FIRST SCENARIO

| | Iteration steps | | | | |
|---|---|---|---|---|---|
| Features | 0 | 1 | 2 | 3 | 4 |
| $C_1$ | 0 | 0.1515 | 0.2277 | 0.2287 | 0.1955 |
| $C_2$ | 0 | 0.2783 | 0.2952 | 0.2463 | 0.1891 |
| $C_3$ | 0 | 0.1469 | 0.1364 | 0.0957 | 0.0599 |
| $C_4$ | 0 | 0.1106 | 0.1849 | 0.2066 | 0.194 |
| $C_5$ | 0.5 | 0.2307 | 0.108 | 0.0507 | 0.0238 |
| $C_7$ | 0 | 0 | 0 | 0 | 0 |
| $C_8$ | 0.25 | 0.1169 | 0.0548 | 0.0257 | 0.012 |
| $C_9$ | 0.25 | 0.1169 | 0.0548 | 0.0257 | 0.012 |
| $C_{10}$ | 0 | 0 | 0 | 0 | 0 |
| $C_{11}$ | 0 | 0 | 0 | 0 | 0 |
| $C_{13}$ | 0.5 | 0.2307 | 0.108 | 0.0507 | 0.0238 |
| $C_{14}$ | 0 | 0.2129 | 0.3496 | 0.3863 | **0.3632** |

TABLE VIII
FEATURES VALUES FOR EACH ITERATION STEP (IDP MAP) FOR THE SECOND SCENARIO

| | Iteration steps | | | |
|---|---|---|---|---|
| Features | 0 | 1 | 2 | 3 |
| $C_1$ | 0 | 0.8556 | 0.8889 | 0.8147 |
| $C_2$ | 0 | 0.8048 | 0.8222 | 0.7394 |
| $C_3$ | 0 | 0.428 | 0.4051 | 0.2995 |
| $C_4$ | 0 | 0.4273 | 0.5942 | 0.6196 |
| $C_5$ | 0.5 | 0.2449 | 0.1218 | 0.0608 |
| $C_7$ | 1 | 0.4621 | 0.227 | 0.113 |
| $C_8$ | 0.75 | 0.5053 | 0.3401 | 0.2239 |
| $C_9$ | 0.75 | 0.5053 | 0.3401 | 0.2239 |
| $C_{10}$ | 1 | 0.4621 | 0.227 | 0.113 |
| $C_{11}$ | 0.66 | 0.3694 | 0.2099 | 0.1185 |
| $C_{13}$ | 0.5 | 0.2449 | 0.1218 | 0.0608 |
| $C_{14}$ | 0 | 0.6923 | 0.85 | **0.8491** |

on the trustworthiness level of an IdP, low values of these features decrease significantly the last value of trust and vice versa. Thus, in the two scenarios, the map was converged as desired and the obtained results were decisive for the trust decision in the FIM context.

*3) Scenarios for the CSP map:* In the first scenario, we have a CSP with a low security mechanism (low authorization mechanism ($C_{12} = 0$), non secure communication channel ($C_7 = 0$), low availability ($C_{10} = 0$)), medium limited disclosure ($C_6 = 0.50$) and medium interoperability ($C_{13} = 0.50$). The intermediate features from $C_1$ to $C_4$ and the output $C_{14}$ are set to 0. In the second scenario, the security-related features $C_7$, $C_{10}$, and $C_{12}$ are set to a high value (1). Interoperability and limited disclosure are set to a medium value ($C_6 = C_{13} = 0.50$), and the intermediate features from $C_1$ to $C_4$ and the output $C_{14}$ are set to 0. Table IX presents the initial state vectors for the two scenarios.

Table X shows that in the first scenario, the final state vector

TABLE IX
INITIAL STATE VECTOR FOR EACH SCENARIO FOR THE CSP

| Features | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_6$ | $C_7$ | $C_{10}$ | $C_{12}$ | $C_{13}$ | $C_{14}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Scenario 1 | 0 | 0 | 0 | 0 | 0.5 | 0 | 0 | 0 | 0.5 | 0 |
| Scenario 2 | 0 | 0 | 0 | 0 | 0.5 | 1 | 1 | 1 | 0.5 | 0 |

is reached at 4 simulation steps with a last value of trust $C_{14} = \mathbf{0.3568}$ which means that the trustworthiness level of this CSP is low (Untrusted). Meanwhile, in the second scenario (Table XI), the final state vector is reached at 3 simulation steps with a final trust value $C_{14} = \mathbf{0.8251}$ which means that the trustworthiness level of this CSP is high (Trusted) according to the criterion in (4). From the results, in both scenarios, we get the same conclusions as in the CSP scenarios and the map was converged as desired.

TABLE X
FEATURES VALUES FOR EACH ITERATION STEP (CSP MAP) FOR THE FIRST SCENARIO

| | Iteration steps | | | | |
|---|---|---|---|---|---|
| Features | 0 | 1 | 2 | 3 | 4 |
| $C_1$ | 0 | 0.1194 | 0.1886 | 0.1975 | 0.1731 |
| $C_2$ | 0 | 0.2239 | 0.2416 | 0.2083 | 0.162 |
| $C_3$ | 0 | 0.15 | 0.1422 | 0.1019 | 0.0651 |
| $C_4$ | 0 | 0.1495 | 0.2103 | 0.2189 | 0.1973 |
| $C_6$ | 0.5 | 0.2354 | 0.1125 | 0.0539 | 0.0258 |
| $C_7$ | 0 | 0 | 0 | 0 | 0 |
| $C_{10}$ | 0 | 0 | 0 | 0 | 0 |
| $C_{12}$ | 0 | 0 | 0 | 0 | 0 |
| $C_{13}$ | 0.5 | 0.2354 | 0.1125 | 0.0539 | 0.0258 |
| $C_{14}$ | 0 | 0.2014 | 0.3337 | 0.3765 | **0.3568** |

TABLE XI
FEATURES VALUES FOR EACH ITERATION STEP (CSP MAP) FOR THE SECOND SCENARIO

| | Iteration steps | | | |
|---|---|---|---|---|
| Features | 0 | 1 | 2 | 3 |
| $C_1$ | 0 | 0.8258 | 0.8274 | 0.7203 |
| $C_2$ | 0 | 0.5809 | 0.6134 | 0.5328 |
| $C_3$ | 0 | 0.4872 | 0.4574 | 0.3383 |
| $C_4$ | 0 | 0.6195 | 0.6981 | 0.6476 |
| $C_5$ | 0.5 | 0.2449 | 0.1218 | 0.0608 |
| $C_7$ | 1 | 0.4621 | 0.227 | 0.113 |
| $C_{10}$ | 1 | 0.4621 | 0.227 | 0.113 |
| $C_{12}$ | 1 | 0.4621 | 0.227 | 0.113 |
| $C_{13}$ | 0.5 | 0.2449 | 0.1218 | 0.0608 |
| $C_{14}$ | 0 | 0.6905 | 0.8393 | **0.8251** |

Many other scenarios were applied on the CSP map with different initial state vectors, the obtained results show that the security features were the most influencing features on the trustworthiness level of the CSP which is the objective of the constructed maps for these simulation scenarios.

### B. Computational Efficiency Analysis

The goal of these experiments is to assess the performance of the proposed method by using the time overhead metric to evaluate their computation efficiency. Through these experiments, we will check that the proposed trust model can manipulate the rising of input access requests without noticeable loss in QoS. In the tests scenarios, the number of input requests changes from 1000 to 10,000.

For an effective evaluation of our approach, we used three kinds of time overhead: $T_{agg}$, $T_c$, and $T_{total}$, where $T_{agg}$ is the time overhead of the aggregation and computation of the initial values of the trust features, $T_c$ is the time overhead of the trust computation, and $T_{total}$ is the total time overhead of the trust system. It is composed of the two periods of time $T_{agg}$ and $T_c$.

In the first group of experiments, we separately computed and compared the two times $T_{agg}$ and $T_c$, in order to check the impact of each phase on the overall overhead ($T_{total}$). For $T_{agg}$ time overhead, for the experiment purposes, 10,000 samples of information that represent external entities are collected in an external SQL database. Then, the features were collected from the external SQL database and computed using Equation (3). In this group of experiments, the trust management service configuration is (Intel (R) Xeon (R) CPU, 16 cores 2.20 GHz, 24 GB memory and 7 TB hard disk space) (Fig. 5).

Fig. 11 shows the comparison results for $T_{agg}$ and $T_c$. From these results, we can notice that the time overhead of the initial feature values aggregation $T_{agg}$ phase is always greater than the time overhead of the trustworthiness computation phase ($T_c$). This is due to the fact that external sources were used to collect and compute the initial values of features. We can also notice that the two time overhead $T_{agg}$ and $T_c$ increase with the number of input requests but not significantly.

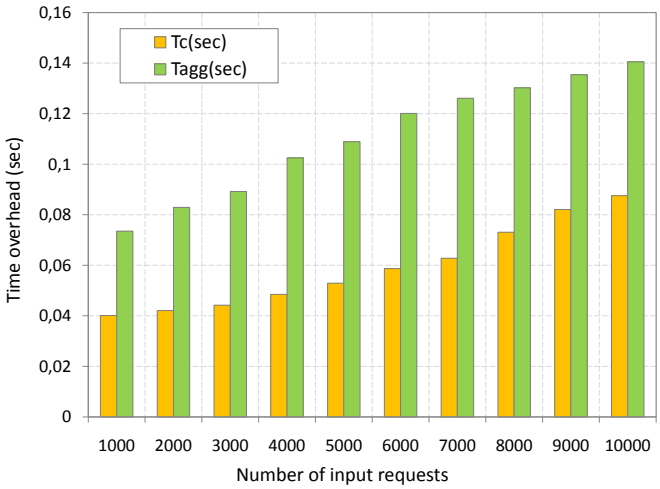


Fig. 11. The $T_{agg}$ and $T_c$ overhead (sec) comparison

In the second group of experiments, we computed the total time overhead $T_{total}$ of the proposed system for different configurations of the trust management service. The total time overhead $T_{total}$ is composed of the two periods of time $T_{agg}$ and $T_c$. For each request, the initial values of the trust features were collected and computed using equation (3)(Section V-C), then gathered in an SQL database. After that, the trust evaluation system takes these values as input and outputs the final trust value using the trustworthiness computation algorithm described in section V-D. The experiments were conducted for three different configurations of the trust management service. The first configuration is **C1**:(Intel (R) Xeon (R) CPU, 4 cores 2.20 GHz, 8 GB memory and 2 TB hard disk space). The second configuration is **C2**:(Intel (R) Xeon (R) CPU, 8 cores 2.20 GHz, 12 GB memory and 7 TB hard disk space). While, the third configuration is **C3**:(Intel (R) Xeon (R) CPU, 16 cores 2.20 GHz, 24 GB memory and 7 TB hard disk space).

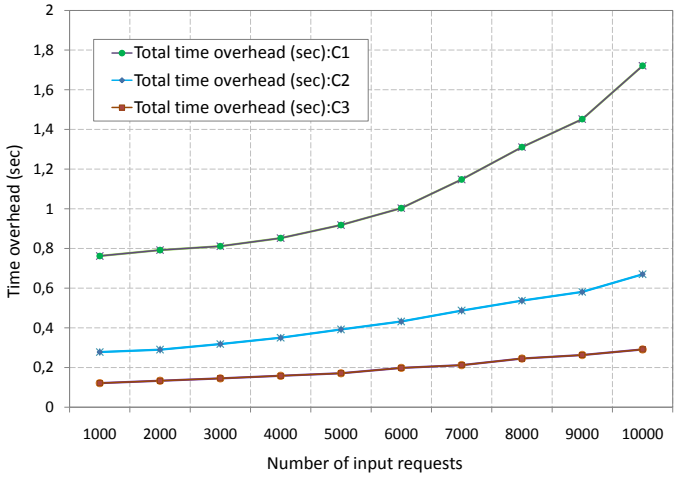


Fig. 12. The total time overhead $T_{total}$ (sec) for the three configurations of the trust management service (C1, C2 and C3)

From Fig. 12, we can see that the time overhead increases with the increase of the number of entities (CSP or IdP) to be evaluated but the increase is not significant and depends on the resources used in the configuration of the trust management service. It is gradually reduced with the resources growing (CPU, memory size) as the value of the total time overhead is less in the second configuration of the trust management service (C2) than in the first one (C1). In the third configuration of the trust management service (C3), the value of total time overhead became far less than in the first one (C1). From the obtained results, we can get the conclusion that the QoS of the proposed scheme is not significantly affected by increasing the number of the input requests as the time overhead decreases significantly with the increase of the resources used by the trust management service (CPU, memory size). Although the proposed FCMDT method has not been tested in a real cloud environment, it can be concluded from our experimental results that it is suitable for cloud computing as the resources is not an issue in such platforms, thus overhead will be negligible.

For the comparative analysis of the obtained results with other works, there are no results from the cited works in this paper which can be compared with our work.

### C. Limitations

The main objective of the experiments is to prove the effectiveness and reliability of the proposed FCMDT method.

Despite the promising results that have been demonstrated by these experiments, it should be noted that the proposed approach has not been tested in a real cloud environment with real-world cases. As an extension of this work could be other research to compare our method in real large-scale environments and produce comparative results with other methods.

## VII. Comparison with other methods

In this section, we compare our trust model with representative trust management models specifically designed for dynamic FIM in cloud computing environments. In the literature, there is no specific assessment criterion that can be used in the comparison. Thus, the comparison is made based on the selected criteria from studies in [7],[53]-[56]. These studies have proposed certain criteria that a cloud trust management system should possess. The selected criteria have been identified in the literature as essential to the development of effective FIM models for cloud environments and are the most frequently applied. A brief description of these criteria is given below:

*1) Trust management technique:* Cloud-based trust management techniques can be classified into four categories: Policy (PocT), Recommendation (RecT), Reputation (RepT), and Prediction (PrdT). [54]-[56]. The PocT uses a set of policies that assume multiple authorization levels with a minimum trust threshold (e.g., if the SLA is satisfied, the CSP (IdP) is considered trustworthy) [55], [56]. RecT takes advantage of entities' knowledge of trusted parties, especially given that the party at least knows the source of the trust recommendation. Recommendations from trusted entities can be explicit or transitive [55]. The RepT, compute aggregated trust metrics based on feedback received from different entities based on their previous interactions [56]. Aggregate feedbacks can have a direct or indirect influence on the trustworthiness of a particular entity. For example, feedback from different cloud service consumers can significantly affect the trustworthiness of a particular CSP, positively or negatively. PrdT is very useful for a cloud environment, especially when there is no prior information about interactions (e.g., history of successful or unsuccessful interactions) [56].

*2) TMS Privacy:* TMS (Trust Management System) privacy is a fundamental concern in cloud computing. It refers to the degree of sensitive information disclosure that users may face during interactions with the trust management system [53]. One way to preserve privacy is to use anonymization techniques that can reduce multiple privacy threats (e.g., tracking of user' behaviour by malicious CSP and IdP), by keeping the owner of the identity information secret from other entities [55]. "High" level is assigned if the trust model assures user privacy through anonymization techniques or cryptographic mechanisms. "Low" level is assigned to this feature if it is not assured by the trust model.

*3) Data Control and Ownership:* This feature means that the disclosure of personal information is under the complete control of the user. Lack of user control can lead to unauthorized disclosure of sensitive data, leading to a breach of privacy and security [53], [55]. Thus, a trust model providing user control assurance is preferable to keep the sensitive data secure [53]. "High" level is assigned if the model assures user consent and control through access control policies or cryptographic mechanisms. "Low" level is assigned to this feature if it is not assured by the trust model.

*4) TMS integrity:* The trust model should be capable of assuring the integrity and accuracy of users' sensitive data in the cloud [53]. "High" level is assigned if the trust model ensures the data integrity through encryption techniques. "Medium" level is assigned if data integrity is ensured through SLAs or certificates. "Low" level is assigned if the trust model does not provide any guarantee about the integrity of data stored in the cloud.

*5) Scalability:* Refers to the ability of the trust mechanism to grow in one or more aspects [53], [55],such as the number of trust evaluation inquiries that can be handled in a given period of time and the number of trust relationships that can be supported. "Low" level is assigned to indicate that the TMS is not scalable or has limited scalability in cloud computing. TMS that follows a centralized architecture is not scalable in cloud environments [53]. Similarly, policy-based TMSs have limited scalability and they are not suitable for cloud environments [7], while the "High" level indicates that the TMS is scalable in cloud environments such as TMS that follows a decentralized or distributed architecture [53], [55].

*6) Federated Identity (FI) Protocols used:* Refers to the capability of the trust model to be deployed with different Identity Protocols [7] such as SAML, or REST (Representational state transfer). This factor helps to identify the portability level of the trust model [55].

***Analysis***

As can be seen from Table XII, the proposed model has several qualitative advantages over previous models. First, each of the discussed models considers some of the selected criteria but not all. Meanwhile, all these criteria are considered in our model. Many studies such as [2], [4], [54], [55] show that considering all these criteria is necessary to obtain a more reliable and flexible trust model for cloud FIM.

First of all, the use of fuzzy logic increases the flexibility of our approach and of [43] as it models the uncertainty of trust. However, the dynamic characteristics of FCMs and their great ability to capture dynamic aspects of system's behaviour make our model more flexible than work in [43]. None of the other analysed models handle the element of uncertainty that may arise in dynamic environments such as cloud computing. The TMS privacy criterion is respected in our approach by the consideration of the anonymity feature in the measure of trustworthiness. Similarly, this criterion is also considered in [30] by the use of a unique entityID for all parties of a federation to ensure anonymity. In [31], [43], this feature is achieved by the use of cryptographic mechanisms in particular re-encryption proxy in [39], while it is not considered in [25], [26], [28], [56], as cryptographic mechanisms and anonymity are completely missing in these systems.

The data control and ownership criterion is not accounted for in [25], [26], [28], [30]. The potential liability of the IdP

TABLE XII
COMPARATIVE ANALYSES OF DYNAMIC TRUST MANAGEMENT SYSTEMS

| Trust mechanisms | Criteria | | | | | |
|---|---|---|---|---|---|---|
| | TM technique | TMS Privacy | Data Control and Ownership | TMS integrity | Scalability | FI Protocols used |
| F. Almenárez et al [28] | SAML PocT | Low | Low | Medium | Low | SAML |
| H. Gao et al [25] | ATNL PocT | Low | Low | Medium | Low | Any FI protocol |
| J. Jiang et al [30] | RecT | High | Low | High | Low | SAML |
| Y. Huang et al [26] | RecT | Low | Low | Low | Low | Any FI protocol |
| B. Zwattendorfer et al [31] | RecT | High | High | High | High | Any FI protocol |
| U. S. Premarathne et al [56] | RepT | Low | Low | Medium | High | Any FI protocol |
| P. Arias et al [43] | RepT (Fuzzy logic) | High | Low | High | High | Any FI protocol |
| FCMDT model | RepT/PrdT (Fuzzy logic) | High | High | High | High | Any FI protocol |

in issuing identity credentials and making identity assertions without user control in [28] decreases significantly the privacy of the trust model. In addition, it does not respect the limited disclosure principle (where the information must be disclosed on the basis of the "need to know" only), which can lead to many security and privacy risks. In [25], the use of the trust negotiation policy language (ATNL) tends to reveal credentials that may incur the loss of user privacy and control of information. In [26] the sensitive data can be transmitted to the cloud identity broker without the user consent. Moreover, the storing and processing of identity data in a public cloud brings many privacy and security risks to users. In [43], [56], there is no control on the disclosure of identity attributes of the users. However, this feature is achieved in [31] by the encrypting the sensitive data before transmitting it to the cloud identity broker and only the user is in control to decrypt it or to generate re-encryption keys. In addition, the user is able to select the amount of data to disclose to the CSP and cloud identity broker. This feature is also followed by our scheme in the measure of entities trustworthiness.

Furthermore,our approach ensures integrity by taking into account encryption and digital signature mechanisms. This feature is also achieved in [30] and [31] through encryption mechanisms that encrypt the user's credentials. However, it is only partially followed by trust models in [25], [28], [56] by using digital certificates. In [25], data integrity is not respected because identity data is stored and processed in a public cloud without using an encryption mechanism which can lead to many security and privacy issues such as intentional or unintentional deletion, modification and theft.

The trust models in [25], [26], [28], [30] are not suitable for cloud environments because of their limited scalability. The trust model in [28] is based on the SAML language which was designed for limited-scale identity federation. In [25], the trust model is not scalable since the number of users and organizations in the ATNL policy could become very large, and increase the total number of attributes. The use of a trusted central controlling authority in [30] decreases significantly their flexibility and scalability. The centralized trust management might have to generate a lot of loads, resulting in an inefficient system. In [26] the dependency of users and CSP on the same central cloud identity broker for identification decreases significantly their scalability and flexibility. The trust models in [31], [56] are more scalable than other models. However, in [31], the static federation of brokers which depend on bilateral agreements between brokers in [31] limits the flexibility of their trust model. From the results of the experiments, our trust model seems to be able to support large-scale cloud environments and it is more flexible than the trust model in [31]. In addition, our solution, as well as the solutions in [25], [26], [31], [43], [56] is extensible to adapt the different kinds of identity federation protocols. However, models in [28] and [30] are only used with the SAML federated identity protocol. Finally, this comparison shows that our trust model comprehensively captures the essential FIM characteristics for effective and successful use in a cloud computing environment.

## VIII. CONCLUSION

The concept of trust is very important for FIM systems as the parties involved in the federation need to rely on each other before exchanging user sensitive information and trust that information. In this paper, we have analysed the main existing frameworks for identity federation and highlighted their limitations for deployment in cloud computing. Our study shows that the underlying trust models are too rigid to allow dynamic federation establishment, especially between previously unknown entities. Our trust model overcomes these limitations by introducing a dynamic management of trust relationships for FIM. The proposed model introduces the FCMs into modelling and evaluating the trustworthiness of unknown entities. The effectiveness of this technique to model the uncertainty of trust was widely proven by prior studies. To evaluate the performance and computational efficiency of our model, we performed intensive tests and experiments; the results proved the effectiveness of our approach in evaluating the trustworthiness of both CSP and IdP. Furthermore, we conducted comparison and analysis between the proposed model and the models analysed in section II. The comparison showed the superiority of our approach in terms of flexibility and efficiency over the other models.

For future work, we intend to conduct in-depth investigation on how to provide more desired properties, such compliance and security. Moreover, we will apply the solution to real cases (with more scenarios)in real cloud environment to gather feedback and requirements.

## ACKNOWLEDGMENT

This work was granted access to the HPC resources of UCI-UFMC (Unité de Calcul Intensif of the University FRERES MENTOURI-Constantine).

## REFERENCES

## REFERENCES

[1] J. Werner, C. M. Westphall, and C. B. Westphall, "Cloud identity management: A survey on privacy strategies",in Computer Networks, vol. 122, pp. 29-42, 2017

[2] S. Saini, and D, Mann, "Identity Management issues in Cloud Computing", in the International Journal of Computer Trends and Technology, vol. 9, no. 8, pp. 414-416, 2014

[3] Security Intelligence, "Identity Management in Cloud Computing: Top Tips for Secure Identities", Available at: https://goo.gl/iJHRyf, last viewed February. 2018

[4] A. Bhardwaj, and V. Kumar, "Identity management practices in cloud computing environments". in the International Journal of Cloud Computing, vol. 3, no. 2, p. 143-157, 2014

[5] J. Jensen, "Benefits of federated identity management-A survey from an integrated operations viewpoint", in International Conference on Availability, Reliability, and Security, pp. 1-12. 2011

[6] J. Kallela, "Federated Identity Management Solutions", *Seminar on Internetworking*, TKK T-110.5190, 2008

[7] E. Maler, and D. Reed, "The venn of identity: Options and issues in federated identity management", in *IEEE Security & Privacy Magazine*, vol. 6, no 2, pp. 16-23, 2008

[8] S. Cantor, J. Kemp, R. Philpott, and E. Maler, "Assertions and protocols for the oasis security assertion markup language", OASIS Standard (March 2005), pp. 1-86, 2005

[9] M. Goodner, M. Hondo, A. Nadalin, M. McIntosh and D. Schmidt, "Understanding WS-Federation", *Microsoft and IBM*, Available at: https://msdn.microsoft.com/en-us/library/bb498017.aspx. last viewed August 2017.

[10] Liberty Alliance, "Federation Liberty Alliance", Available at: http://www.projectliberty.org/liberty/strategic-initiatives/federation/, last viewed may 2017

[11] T. Scavo and S. Cantor, "Shibboleth architecture", *Protocols and Profiles*, vol. 10, p. 16. 2005

[12] 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

[13] OpenId Foundation, OpenID Project Homepage, Available at: http://openid.net/connect/, last viewed September 2017

[14] L. Ijlel., A. Jøsang, "FIDO Trust Requirements". In: Buchegger S., Dam M. (eds) Secure IT Systems. NordSec 2015. Lecture Notes in Computer Science, vol 9417, 2015

[15] J. Kang, Y. Elmehdwi, D. Lin, "SLIM: Secure and Lightweight Identity Management in VANETs with Minimum Infrastructure Reliance". In: Security and Privacy in Communication Networks. SecureComm, Springer, vol. 238, pp. 823-837, 2018

[16] A. A. Malik, H. Anwar, and M. A. Shibli, "Federated Identity Management (FIM): Challenges and opportunities, " in *Conference on Information Assurance and Cyber Security (CIACS)*, pp. 75-82, 2015

[17] 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*, pp. 173–184, 2009

[18] U. Kylau, I. Thomas, M. Menzel, and C. Meinel, "Trust Requirements in Identity Federation Topologies," *International Conference on Advanced Information Networking and Applications, AINA'09*, pp. 137-145, 2009

[19] Z. Wei, L. Lu, and Z. Yanchun, "Using fuzzy cognitive time maps for modeling and evaluating trust dynamics in the virtual enterprises," *Expert Systems with Applications*, vol. 35, no. 4, pp. 1583–1592, 2008

[20] E. I. Papageorgiou, and J. L. Salmeron, "A Review of Fuzzy Cognitive Maps Research During the Last Decade". In *IEEE Transactions on Fuzzy Systems*, vol. 21, no. 1, pp.66-79, 2013

[21] C. Castelfranchi, R. Falcone, and G. Pezzulo, "Integrating Trustfulness and Decision Using Fuzzy Cognitive Maps", in *International Conference on Trust Management*, pp. 195–210, 2003

[22] P. P. Groumpos, "Fuzzy Cognitive Maps: Basic Theories and Their Application to Complex Systems". *Fuzzy Cognitive Maps*, pp.1-22, 2010

[23] C. D. Stylios and P. P. Groumpos, "Modeling complex systems using fuzzy cognitive maps", *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 34, no. 1, pp. 155–162, 2004

[24] K. Bendiab, S. Shiaeles, and S. Boucherkha, "A New Dynamic Trust Model for "On Cloud" Federated Identity Management", *9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, 2018

[25] H. Gao, J. Yan, and Y. Mu, "Dynamic Trust Model for Federated Identity Management", in *the 4th International Conference on Network and System Security (NSS), IEE*, pp. 55-61, 2010

[26] H. Y. Huang, B. Wang, X. X. Liu, and J. M. Xu, "Identity Federation Broker for Service Cloud," *International Conference on Service Sciences (ICSS), IEE*, pp. 115-120, 2010

[27] P. Harding, L. Johansson and N. Klingenstein, "Dynamic security assertion markup language: Simplifying single sign-on," Security and Privacy, IEEE, vol. 6, no. 2, pp. 83-85, 2008

[28] F. Almenárez, P. Arias, A. Marín, and D. Díaz,. "Towards dynamic trust establishment for identity federation," In Proceedings of the 2009 Euro American Conference on Telematics and Information Systems: New Opportunities to increase Digital Citizenship, ACM, p. 25, 2009.

[29] M. S. Ferdous, and R. Poet, R. "Dynamic Identity Federation using Security Assertion Markup Language (SAML)," In IFIP Working Conference on Policies and Research in Identity Management, pp. 131-146, Springer, 2013.

[30] 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 *6th International ICST Conference on Communications and Networking in China (CHINACOM)*, pp. 785-789, 2011

[31] B. Zwattendorfer, D. Slamanig, K. Stranacher, and F. Hörandner, "A Federated Cloud Identity Broker-Model for Enhanced Privacy via Proxy Re-Encryption," in *IFIP International Conference on Communications and Multimedia Security, Springer Berlin Heidelberg*, pp. 92–103, 2014

[32] ETSI. ETSI GS INS 004 V1.1.1, "Identity and access management for Networks and Services; Dynamic federation negotiation and trust management in IdM systems," Available at: https://www.etsi.org/deliver/etsi_gs/INS/001_099/004/01.01.01_60/gs_ins004v010101p.pdf, last viewed August. 2017.

[33] Internet Engineering Task Force (IETF), "application bridging for federated access beyond Web (ABFAB) architecture", Available at : https://tools.ietf.org/html/rfc7831, last viewed August. 2017.

[34] Internet2, "Distributed Dynamic SAML", Available at: https://spaces.at.internet2.edu/display/dsaml/Distributed+Dynamic+SAML, last viewed August. 2017.

[35] W. V. Vasantha and F. Samarandache. "Fuzzy cognitive MAPS and neuthrosophic cognitive MAPS," Infinite Study, 2003

[36] S. Bueno, and J. L. Salmeron, "Benchmarking main activation functions in fuzzy cognitive maps," In: *Expert Systems with Applications*, vol. 36, no. 3 , pp. 5221-5229, 2009.

[37] D. H. McKnight, and N. L. Chervany, "The Meanings of Trust", Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.155.1213, last viewed August, 2017

[38] X. Zhang and Q. Zhang, "Online trust forming mechanism: approaches and an integrated model," in *Proceedings of the 7th international conference on Electronic commerce*, pp. 201-209, 2005

[39] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, and S. Pope, "Trust Requirements in Identity Management", in *Proceedings of the 2005 Australasian workshop on Grid computing and e-research*, Vol. 44, pp. 99-108, 2005

[40] A. Pandey, and J. R. Saini. "An Investigation of Challenges to Online Federated Identity Management Systems", in *International Journal of Engineering Innovation and Research, IJEIR*, vol. 1, no.2, pp.104-108, 2012

[41] 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*, pp. 181-188, 2013

[42] M. S. Ferdous, G. Norman, A. Jøsang, and R. Poet, “Mathematical Modelling of Trust Issues in Federated Identity Management,” *IFIP International Conference on Trust Management*, pp. 13–29, 2015
[43] P. Arias-Cabarcos, F. Almenárez-Mendoza, A. Marín-López, D. Díaz-Sánchez, and R. Sánchez-Guerrero. “A Metric-Based Approach to Assess Risk for “On Cloud” Federated Identity Management”. In *Journal of Network and Systems Management*, vol. 20, no. 4, pp.513-533, 2012
[44] D. Broeder,R. Wartel, B. Jones, P. Kershaw,D. Kelsey, S. Lüders, A. Lyall, T. Nyrönen, and H. G. Weyer, “Federated Identity Management for Research Collaborations,” No. CERN-OPEN-2012-006, available at: https://cdsweb.cern.ch/record/1442597/files/CERN-OPEN-2012-006.pdf, 2013
[45] C. C. Lo, D. Y. Chen, C. F. Tsai, and K. M. Chao, "Service selection based on fuzzy TOPSIS method," in *Advanced Information Networking and Applications Workshops (WAINA), IEE*, pp.367-372, 2010
[46] NIST Internal Report (NISTIR) 8149, “Developing Trust Frameworks to Support Identity Federations”, available at: http://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf, 2018
[47] B. William, “NIST special publication 800-63: Electronic authentication guideline”. available at: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf, last viewed August. 2017.
[48] B. Glade, "Identity Assurance Framework: Assurance Levels", 2009
[49] B. Elaine, and L. R. Allen, “Sp 800-131a. transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths”, available at: https://csrc.nist.gov/, last viewed August. 2017
[50] Privacy Framework Proposal, Available at: https://kantarainitiative.org/confluence/display/archive/Privacy+Framework+Proposal+-+A+Credential+Lifecycle+Approach, last viewed August. 2017
[51] X. Li, H. Ma, F. Zhou, and X. Gui, “Service operator-aware trust scheme for resource matchmaking across multiple clouds,” in *IEEE transactions on parallel and distributed systems*, vol. 26, no. 5, pp. 1419–1429, 2014
[52] C. Cérin, C. Coti, P. Delort, F. Diaz, M. Gagnaire, M. Mijic, Q. Gaumer, N. Guillaume, J. Le Lous, and S. lubiarz, “Downtime Statistics of Current Cloud Solutions”, in *The International Working Group on cloud computing resiliency*, available at:http://iwgcr.org/, 2014.
[53] M. Chiregi and N. J. Navimipour, “A comprehensive study of the trust evaluation mechanisms in the cloud computing”, in *Journal of Service Science Research*, vol. 9, no. 1, pp. 1–30, 2017
[54] A. A. Malik, H. Anwar, and M. A. Shibli, “Federated Identity Management (FIM): Challenges and opportunities”, in *Conference on Information Assurance and Cyber Security (CIACS), IEE*, pp. 75-82, 2015
[55] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, “Trust management of services in cloud environments, Obstacles and Solutions”, in *ACM Computing Surveys (CSUR)*, vol. 46, no. 1, pp. 1–12, 2013
[56] U. S. Premarathne, I. Khalil, Z. Tari, and A. Zomaya, “Cloud-Based Utility Service Framework for Trust Negotiations Using Federated Identity Management“, in *IEEE Transactions on Cloud Computing*, vol. 5, no. 2, pp. 290–302, 2017