Identifying and Prioritizing Evaluation Criteria for User-Centric Digital Identity Management Systems

Sepideh Banihashemi / Master Candidate
Department of Computer Science
Ryerson University
350 Victoria Street Toronto, Ontario, Canada
Shahid Beheshti University
Tehran, 1983963113, Iran

Alireza Talebpour/Assistant professor
Cyberspace Research
Institute
Shahid Beheshti University
Tehran, 1983963113,
Iran

Elaheh Homayounvala/Assistant Professor
Cyberspace Research Institute
Shahid Beheshti
University
Tehran, 1983963113, Iran

Abdolreza Abhari / Professor
Department of Computer Science
Ryerson University
350 Victoria Street
Toronto, Ontario, Canada

***Abstract*—Identity Management systems are used for securing digital identity of users in reliable, automated and compatible way. Service providers employ identity management systems which are cost effective and scalable but cause poor usability for users. Identity management systems are user-centric applications which should be designed by considering users' perspective. User centricity is a remarkable concept in identity management systems as it provides more powerful user control and privacy. This approach has been evolved from amending past paradigms. Thus, evaluation of digital identity management systems based on users' point of view, is really important. The main objective of this paper is to identify the appropriateness of the criteria used in evaluation of user-centric digital identity management systems. These criteria are gathered from the literature and then categorized into four groups for the first time in this work to examine the importance of each parameter. In this approach, several interviews were performed as a qualitative research method and two questionnaires have been filled out by forty six users who were involved with identity management systems. Since the answers are perception based data the most important criteria in each category are assessed by using fuzzy method. This research found that the most important criteria are related to security category. The results of this research can provide valuable information for managers and decision makers of hosting companies as well as system designers to adapt and develop appropriate user-centric digital identity management systems.**

***Keywords*—management of information technology; digital identity management systems; evaluation criteria; fuzzy analytical hierarchy process (FAHP); user-centricity**

I. INTRODUCTION

In today's Information Systems, users have various compounds of login-name and password for every online service or even distinct credentials for different roles inside the services which are available for them. This can result in privacy risk for end-users and jeopardize service providers by security threats. Applying identity management systems is therefore the solution. These systems issue a digital identity for each user and users can control the full life cycle of their identities, from creation to termination [30]. In federated identity management model, identities from various service provider, particularly identity domains, are identified across all domains [3]. The major goals of these systems are to increase user convenience and privacy, and to decentralize user management tasks inside or across the trust circle [1]. It is complicated for user to choose his/her identity provider along with username and password in federated identity management systems which can be considered as a drawback. In addition, the user should remember which federations he/she belongs to or can utilize [33]. In Single Sign-On (SSO) solution, the user authenticates him or herself only once and it is very similar to the federated identity scenario as the same identifier of the user is automatically used by each service provider when the user logged into. Capturing the information of authentication and identification by system and giving the user access to services is the functionality of single sign-on systems [29].

In order to overcome the complicated, unintuitive difficulties which affect the actual users' needs, the latest approach in identity management systems that is user-centric identity management systems has been emerged [32]. These systems support user control and privacy and designed from the users' perspective [7]. A beneficial control of the use and management of Personal Identification Information (PII) is considered in these systems [35]. There are two different user-centric identity management concepts: relationship-focused in which a relationship between the user and identity provider must be established, and credential-focused identity management that is offering user a long-term credentials from the identity provider and keeping them locally [6].An instance of a user-centric identity management system is PRIME which is a European government-funded project [8]. Enhancing user control which is accepted by user-centric identity management paradigms is one the objectives of PRIME project along with considering identity credential misuse and physical stealing of devices [26]. Former studies have presented features and frameworks, and considered numerous metrics for user-centricity paradigm, but most of them have not examined the prioritizing of a comprehensive classification concerning the most important criteria. Since, user-centric digital identity management approach has been emerged in order to conquer the drawbacks of previous identity management models, and concentrates particularly on users' perspective rather than other entities, prioritizing the evaluation criteria which can be aggregated in a universal system is very worthwhile and will assist the design and implementation of these systems beneficially. This paper identifies and prioritizes evaluation criteria for user-centric digital identity management systems. These evaluation criteria have been surveyed in the literature and then evaluated through several interviews with experts in Iran and Canada. In this research, Fuzzy Analytical Hierarchy Process (AHP) has been applied for prioritizing identified criteria, by providing a web-based questionnaire based on the most important criterion in each group.

The rest of this paper is structured as follow. Section two provides literature review. The paper's approach is evaluated in section three. In particular, fuzzy AHP and pairwise comparisons which have been performed in each category are discussed in section four. Finally, we conclude and give an outlook for future work in section five.

II. Literature Review

In order to identify appropriate criteria for evaluating identity management systems, we have conducted a vast search in related literature. In this section, user-centric digital identity management systems are examined based on their characteristics and requirements. Vossaert et al. [40] proposed a user-centric federated identity management approach based on trusted secure modules which meets several requirements, including: 1) Verification to prove that the only information from identity providers for which they gave their consent, is inquired. 2) Performing access restriction to the information by users. 3) Managing the disclosure of personal information. 4) Trustworthiness of service providers in order to request their information. 5) A flexible revocation procedure can be predicted. 6) Scalability property in order to add new identity and service providers. 7) User consent on release of data.

According to Ahn et al. [1] privacy is a major issue as a result of the immense exchange of sensitive information. Pseudonymity is the key principle for protecting user identities and personal information. Furthermore, user-centric models used in the organizations are required to pursue four key principles: 1) Notice: gaining notice about information practice. 2) Choice: Users have the capability of the usage of information type and its purpose. 3) Access: Users should have access to their personal information and be able to modify it whenever is essential. 4) Security: Organizational system must confirm securing users' personal information.

As stated by Ahn et al. [2] an identity metasystem is designed to provide minimal disclosure for a limited usage and consistent experience across contexts in order to improve security and privacy enhanced interoperable architecture, based on the laws of identity.

Poursalidis et al. [31] introduced a multi-pseudonym Identity Management Infrastructure in which users can manage and make an excessive amount of pseudonyms. Their scheme has several advantages. First, users can maintain their anonymity. Next, preventing the existence of a single point that keeps numerous digital identities to preserve the privacy of the user.

According to Ben Ayed et al. [5] the notion of user-centricity has emerged by offering convenience and control to the users over their personal data and fulfilling to their requirements. The attribute management systems are developed to guarantee that any system section can't collect an individual's confidential attributes. From privacy-preserving perspective, keeping track of which digital identity attributes have been revealed and operate by whom, are also considerable issues. In order to prohibit other parties' unpleasant context-spanning linkage and profiling, pseudonyms can be applied.

Claycomb et al. [12] discussed that, the user control over the kind of information being kept, the actual content of the information and the authorizing individuals to view the information are the major motivations in the concept of user-centric identity management systems. Another motivation is privacy and confidentiality, accomplished by offering users the option about what is shared, and with whom it is shared. Furthermore, various service providers such as financial institutions or online merchants must use a centralized repository of user information. Scalability and data authenticity should be taken into account as well.

Jøsang et al. [21] proposed a user-centric identity management approach in a single tamper resistant device in order to improve usability, simplify the user experience, provide mobility by supporting the user in using any hardware platform while obtaining online services and enhance user control. These systems introduce process automation and system support of the identity management at the user side.

According to El Maliki et al. [17] there are some basic rules which have been considered in the new user-centric identity paradigm, specifically: 1) Enhancing the user privacy by providing them full control over their identity information 2) Usability and user experience quality as a result of consistent identity interface and using the same identity for each identity transaction 3) Decreasing identity attacks, including phishing 4) Reducing reachability/disturbances caused by spams 5) Policy specification on both sides, identity providers and service providers 6) Profiting from huge scalability 7) Providing secure conditions at the time of data exchange 8) Separating the digital data from applications.

As stated by Suriadi et al. [35] communication security, minimal data sharing and disclosure, negotiation, user registration, anonymous authentication, data storage, accountability and user control are the requirements for user-centric identity management systems. It also requires that users have an effective control of the use and management of their personal identifiable information, leading to a better privacy.

Some properties have been laid out in Bhargav-

Spantzeletal et al. upon which user-centric federated identity management is based on. The key properties of a user-centric federated identity management system are user control and consent, and numerous system properties help to achieve user control. The properties that are not based on the realization of other properties are basic properties whereas composite properties are composed of basic properties. There are four basic system properties: 1) User chosen identity provider 2) Policy specification and enforcement 3) Auditing 4) Assurance support. Another basic property is transaction property. Transaction properties concern all the transactions which deal with identity-related information that is: 1) Context bound transactions 2) Unlinkability 3) User consent. The final properties in this category are identity information properties which are: 1) Confidentiality 2) Integrity 3) Availability 4) Stealing protection 5) Revocation 6) Portability 7) Sharing prevention 8) Selective release and 9) Conditional release. Several composite properties are defined which build on one or more of the basic properties: 1) Attribute security 2) Service protection 3) Non-repudiation 4) Data minimization 5) Attribute privacy 6) Accountability 7) Privacy policy, obligations, and restrictions 8) Notification 9) Anonymity 10) User in the middle. It is also stated that multi-device management and usability are the unique properties which are essentials for these systems. Usability addresses the relationship between the user-centric tools and their users. Some key aspects are 1) To have consistent user experience, 2) An intuitive and easy UI which may also help required functionality from the user like policy specification, and finally 3) Process automation that is, automating user-side processes of identity management as far as possible through policy and preferences-driven methods [6]. On the other hand, some research projects look at Digital Identity Management as the core of the Internet economy and from public policy concept [14]. Or another research project studies identity through one's whole life. [19].

To sum up, previous research projects have surveyed key principles and properties required in user-centric digital identity management systems. Our work demonstrates taxonomy of criteria in terms of security, user control, system capabilities and cost-effectiveness. These groups of criteria and criteria within each group are first evaluated and then prioritized based on fuzzy Analytical Hierarchy Process.

III. Evaluation Approach

As the first step to evaluate identity management criteria, a thorough list of identified criteria was provided to the specialists in this domain in order to obtain their verification. Then a common decision making tool has been used to prioritize these criteria.

A. *Decision Making Models*

In recent decades, researchers have paid attention to multi criteria decision making model (MCDM) for complex decision making. In such models, instead of using one optimal evaluation criterion, several evaluation criteria may be used. [22]

These decision making models are categorized into two groups: Multi objective decision making models (MODM) and Multi attribute decision making models (MADM). Multi objective models are used to design the alternatives whereas multi attribute models include the choice of the best option [30]. One of the methods for MADM is Analytical Hierarchy Process (AHP) which is based on pairwise comparison [37].

B. *Analytical Hierarchy Process*

Analytical Hierarchy Process was developed by Thomas L. Saaty in 1970 which is a tool of decision making that can deal with structured and semi-structured decisions [23]. In AHP, both qualitative and quantitative features of human thoughts are included in decision making process. The analytical hierarchy process deals with the inconsistency because people are more likely to be inconsistent when they are making judgments. Therefore, the pairwise comparison matrix is used which is perfectly consistent [34].

The first step in AHP is creating a multi-level hierarchical structure of objectives, criteria, sub criteria, and alternatives [36]. Then, the priorities for each level of criteria are required which come from pairwise comparison [34]. These comparisons obtain the relative importance of each factor that is defined by their weights [37]. The decision maker has to present his idea about the value of one single pairwise comparison at a time [36]. After obtaining the relative weights, the best alternative can be determined from the aggregation value of them [37]. Relative weights can be evaluated from least square, geometric means, and eigenvalue methods [36]. In order to quantify pairwise comparison which is the most crucial step in decision making process, a scale is used. Since people cannot distinguish between two very close values of importance (e.g., 3.00 and 3.02), Saaty used 9 as the upper limit and 1 as the lower limit in his scale [11] and for the comparison of factors, the available values are the members of this set: {1.9, 1.8, …, 1.2, 1, 2, …, 8, 9} [38].

C. *Fuzzy Analytical Hierarchy Process*

Although the aim of applying Analytical Hierarchy Process is to obtain the opinions of experts, the typical AHP method does not reflect the human thoughts because the exact numbers are used in pairwise comparisons method. After supplying the graph of hierarchy in FAHP, the decision makers are asked to compare the elements of each level to each other and to express the relative importance of elements by using fuzzy numbers [9].

Van Laahoven *et al.* [38] have introduced the triangular fuzzy numbers based on vector operation to represent the decision maker's opinion for alternatives compared to each criterion.

Chang [9] introduced triangular fuzzy numbers as a new approach in fuzzy AHP. This approach uses triangular fuzzy numbers for pairwise comparisons in FAHP. Noorul Haq *et al.* [28] proposed a model to evaluate and select the supplier based on fuzzy AHP approach. The main advantage of their proposed method was considering qualitative and quantitative criteria in hierarchy structure and problem solving of supplier selection using fuzzy AHP. Lee *et al*. in [25] applied fuzzy AHP method for assessing the importance of effective factors in choosing the supplier. These factors include: cost, performance and number of suppliers. Then based on fuzzy

AHP results, goal planning was used to formulate the constraints. Lee [24] utilized the fuzzy AHP approach in order to analyze and evaluate the relation between the supplier and purchaser.

IV. Analysis and Results

A. Interview

Interviews are among the most familiar strategies for collecting qualitative data. The interview is a method in which, the researcher establishes direct contact with subjects and through this method he/she assesses the perceptions and attitudes. Table I shows the first full list of criteria which have been confirmed and modified by experts. For instance, according to them, confidentiality and user's privacy must be presented as one item, with respect to their definitions. In addition, it was stated that sharing prevention should be a second-order criterion related to security issues in that we only share credentials when we try to obtain services and then we need to invent security mechanisms to avoid identity theft and misuse. As a result of experts' verification and change, second list of criteria, as depicted in Fig 1, was prepared which indeed became an outline for the main questionnaire.

First interview resulted to removing some of the criteria. Security and stealing protection covers features and characteristics of some other criteria. Therefore, these criteria should be removed. In addition, unlinkability criterion should be eliminated since it can't be applied in face-to-face healthcare transactions. Policy specification and enforcement is also not obvious because it should be identified that the policies are related to entities or they are related to privacy policy. Sharing prevention should be considered as a second-level and related to security criteria since sharing the credentials; connection of apps is tempted to share feeds of "data" efficiently so, there is no need to share data by value. Data minimization is an important one but it's very hard to achieve given business model imperatives in most ecosystems. Scalability is one of the most main criterion because without that, no system is likely to succeed any more.

Another interview leads to merging security and stealing protection criteria as they both have the same meaning. In addition, anonymity criterion prevents from revealing identification information of a person and when the conditional release of information exist, this one is fulfilled too. Furthermore, Pseudonymity with anonymity were combined because a person has an identity in the system but he/she has a pseudonym and its anonym.

The outcome of third interview was that Notification should be considered as a second-level criterion related to systems capabilities' criteria. The definition of auditing criterion is that it must support enforcement of responsibility for actions among several loosely coupled identity actors in case of unexpected results. In addition, User Chosen Identity Provider criterion is a hard criterion to achieve but must be considered an important goal to strive for. Many governments are managing to achieve it through contracting with private sector partners.

In the last interview, it is concluded that Confidentiality and Privacy criteria can be considered as one criterion since they have two aspects: Data protection is usually about the service provider's intended security mechanisms, vs. its policies, where it may intend to release sensitive data because it suits the organization's own ends (such as making money). Additionally, Conditional Release seems very second-order criterion related to system and users' security criteria though it's an important one. Verifiability criterion must have remediation abilities in the face of incorrect data.

TABLE I. First List of Evaluation Criteria

Study	Criteria	Study	Criteria
Bhargav-Spantzeletal *et al*. [9], Quasthoff *et al*. [32], Hoffman [20], Mashima *et al*. [26], El Maliki *et al.* [17]	Context Bound Transaction Context—Detection	Ahn *et al*. [1], Suriadi *et al*. [35], Bhargav-Spantzeletal *et al*. [9], Quasthoff *et al*. [32], Mashima *et al*. [26]	Data Minimization Minimal disclosure Minimal data sharing
Ben Ayed *et al*. [4], Bhargav-Spantzeletal *et al*. [9], Quasthoff *et al*. [32], Marx *et al*. [27]	Unlinkability	Suriadi *et al*. [35], Bhargav-Spantzeletal *et al*. [9], Quasthoff *et al*. [32], Marx *et al*. [27]	Accountability
Vossaert *et al*. [40], Claycomb *et al*. [12], Bhargav-Spantzeletal *et al*. [9], Quasthoff *et al*. [32]	Confidentiality Controlling the disclosure of personal information	Ahn *et al*. [2], Bhargav-Spantzeletal et al, [9], Suriadi et al. [35], Quasthoff et al [32], Mashima et al. [26]	Notification Notice user awareness by SMS
Claycomb *et al*. [12], Bhargav-Spantzeletal *et al*. [9], Quasthoff *et al*. [32], Cottrell [13]	Integrity data authenticity Accuracy	Ben Ayed *et al*. [4], Claycomb *et al*. [12], Jøsang *et al*. [21], Suriadi *et al*. [35], Bhargav-Spantzeletal *et al*. [9], Quasthoff *et al*. [32], Mashima *et al*. [26]	User in the middle giving sovereignty to the users over their personal data user control
Vossaert *et al*. [40], Bhargav-Spantzeletal *et al*. [9], Quasthoff *et al*. [32], Mashima *et al*. [26], Marx *et al.* [27]	Verifiability	Ahn *et al*. [1], Jøsang *et al*. [21], El Maliki *et al*. [17]	User experience quality consistent experience simplify the user experience

El Maliki *et al*. [17], Bhargav-Spantzeletal *et al*. [9], Suriadi *et al*. [35], Quasthoff *et al*. [32], Poursalidis *et al*. [31], Mashima *et al*. [26]	Stealing Protection		Vossaert *et al*. [40], Claycomb *et al*. [12], El Maliki *et al*. [17], Marx *et al*. [27]	Scalability
Vossaert *et al.* [40], Bhargav-Spantzeletal *et al*. [6], Quasthoff et al. [32], Poursalidis *et al*. [31], Marx *et al.* [27]	Revocation		Vossaert *et al*. [40], Ahn *et al*. [2], Ahn *et al*. [1], El Maliki *et al.* [17], Poursalidis *et al.* [31]	Security
Vossaert *et al*. [40], Bhargav-Spantzeletal *et al*. [6], Quasthoff *et al.* [32]	Conditional release Access Restriction		Jøsang *et al.* [21], El Maliki *et al.* [17], Bhargav-Spantzeletal *et al.* [9], Mashima *et al.* [26]	Usability
Bhargav-Spantzeletal *et al*. [6], Suriadi *et al*. [35], Quasthoff *et al*. [32], Mashima *et al*. [26]	Sharing Prevention		Vossaert *et al*. [40], Bhargav-Spantzeletal *et al*. [6], Suriadi *et al*. [35], Quasthoff *et al*. [32], Mashima *et al.* [26]	User Consent (Negotiation: users should be allowed to negotiate on the PII that they want to reveal and at what level they are willing to disclose it)
Jøsang *et al.* [21], Quasthoff *et al*. [32], Bhargav-Spantzeletal *et al*. [6], Marx *et al.* [27]	Portability Mobility		Bhargav-Spantzeletal *et al*. [6], Mashima *et al.* [26], Vecchio *et al*. [39[40]	Delegation
Bhargav-Spantzeletal *et al*. [6], Rieger [33], Quasthoff *et al*. [32], Poursalidis *et al.* [31], Mashima *et al*. [26], Choi *et al*. [10]	User chosen Identity Provider		Jøsang *et al*. [21], Bhargav-Spantzeletal *et al.* [6], Ben Ayed [5], Marx *et al.* [27]	Fault Tolerant (tamper resistant)
Vossaert *et al.* [40], Bhargav-Spantzeletal *et al.* [6], El Maliki *et al*. [17], Quasthoff *et al*. [32], Mashima *et al*. [26]	Policy Specification and enforcement Privacy policy, obligation and restriction		Ahn *et al*. [2], Mashima *et al.* [26], Claycomb *at al.* [12]	Availability (Accessibility) (User access)
Vossaert *et al*. [40], Bhargav-Spantzeletal *et al*. [6], Mashima *et al*. [26]	Auditing the log of the transactions activities		Bhargav-Spantzeletal *et al*, [6], Vossaert *et al.* [40], Quasthoff *et al*. [32], Poursalidis *et al*. [31]	Service Protection
Vossaert *et al*. [40], Ben Ayed *et al*. [4], Bhargav-Spantzeletal *et al.* [9], Quasthoff *et al*. [32]	Attribute Security		Vossaert *et al*. [40], Ahn *et al*. [2], Ahn *et al*. [1], Poursalidis *et al*. [31], Ben Ayed *et al*. [4], Claycomb *et al*. [12], El Maliki *et al*. [17], Suriadi *et al*. [35], Poursalidis *et al.* [31]	Privacy
Vossaert *et al*. [40], Bhargav-Spantzeletal *et al.* [6], Poursalidis *et al*. [31], Marx *et al.* [27]	Dependable Trustworthiness Legitimacy of the end-entities Authorized entity Justifiable parties		Vossaert *et al*. [40], Ahn *et al*. [2], Poursalidis *et al*. [31], Suriadi et al. [35], Bhargav-Spantzeletal *et al*. [6], Quasthoff *et al*. [32], Poursalidis *et al.* [31]	Pseudonymity and anonymity

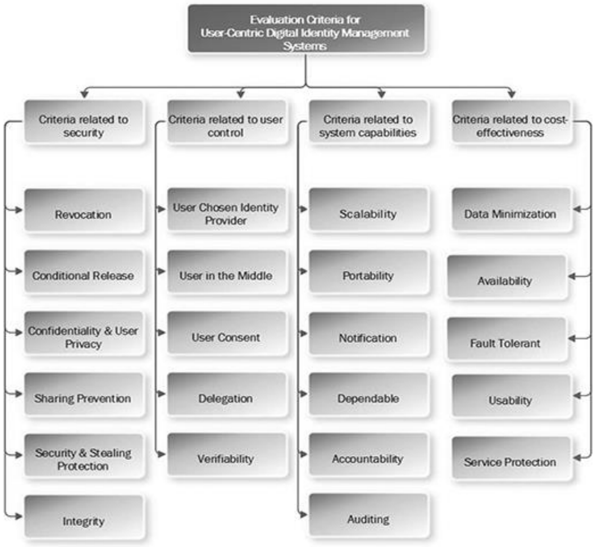
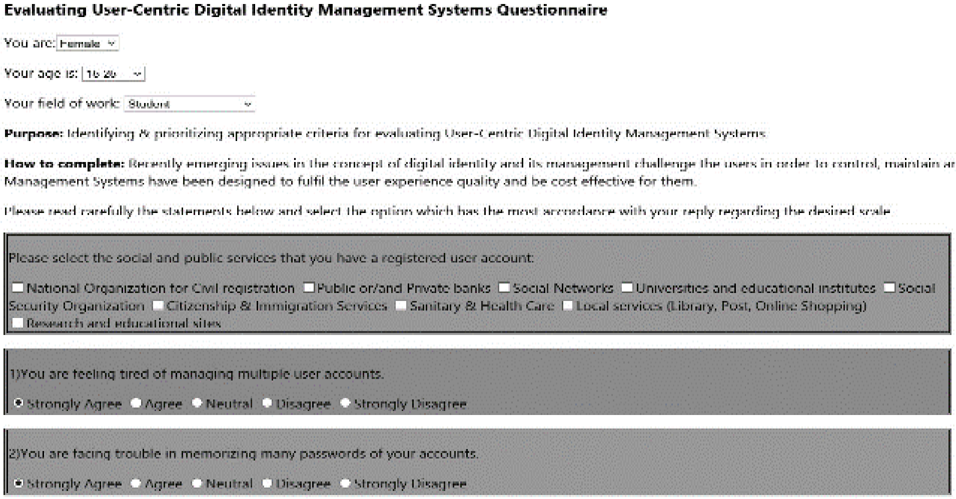

Evaluation Criteria for User-Centric Digital Identity Management Systems
Criteria related to security
Criteria related to user control
Criteria related to system capabilities
Criteria related to cost-effectiveness
Revocation
Conditional Release
Confidentiality & User Privacy
Sharing Prevention
Security & Stealing Protection
Integrity
User Chosen Identity Provider
User in the Middle
User Consent
Delegation
Verifiability
Scalability
Portability
Notification
Dependable
Accountability
Auditing
Data Minimization
Availability
Fault Tolerant
Usability
Service Protection

Fig. 1. Second list of criteria-Hierarchical decision tree

B. The Results of Solving Hierarchy Model Using Change Approach

TABLE II. FUZZY SPECTRUM AND THE CORRESPONDING VERBAL EXPRESSIONS

Row	Verbal Expressions	Fuzzy Numbers
1	Equally Important	(1, 1, 1)
2	Weakly Important	(0.75, 1, 1.25)
3	Strongly Important	(1, 1.25, 1.5)
4	Very Strongly Important	(1.25, 1.5, 1.75)
5	Extremely Preferred	(1.5, 1.75, 2)



Evaluating User-Centric Digital Identity Management Systems Questionnaire

You are: Female

Your age is: 16-25

Your field of work: Student

Purpose: Identifying & prioritizing appropriate criteria for evaluating User-Centric Digital Identity Management Systems

How to complete: Recently emerging issues in the concept of digital identity and its management challenge the users in order to control, maintain and trust these systems. User Centric Digital Identity Management Systems have been designed to fulfil the user experience quality and be cost effective for them.

Please read carefully the statements below and select the option which has the most accordance with your reply regarding the desired scale

Please select the social and public services that you have a registered user account:

□ National Organization for Civil registration □ Public or/and Private banks □ Social Networks □ Universities and educational institutes □ Social Security Organization □ Citizenship & Immigration Services □ Sanitary & Health Care □ Local services (Library, Post, Online Shopping) □ Research and educational sites

1)You are feeling tired of managing multiple user accounts.

● Strongly Agree ○ Agree ○ Neutral ○ Disagree ○ Strongly Disagree

2)You are facing trouble in memorizing many passwords of your accounts.

● Strongly Agree ○ Agree ○ Neutral ○ Disagree ○ Strongly Disagree

http://www.user-centric-idm.ir/

Fig. 2. Web based questionnaire

Step1. Hierarchical decision tree of this project is created as it is shown in Fig. 1. Step2. In order to perform pairwise comparison, the verbal expressions are used, namely: Equally Important to Extremely Preferred, as depicted in Table II.

Results of fuzzy AHP approach for prioritizing the evaluation criteria are presented in this section. In other words, criteria in each category and their arithmetic means are illustrated in details. Forty six experts (20 in Canada and 26 in Iran) have filled the web-based questionnaires, as depicted in Fig. 2.

The experts were both male and female students and university professors with the range of age, 15 to over 45. The questionnaire begins with some inquiries including services in which the users have registered accounts as well as managing and dealing with identity management systems.

Figures 3 to 7 show the arithmetic mean of experts' opinions in which the numbers are separated by comma in Iran and in Canada within each table. Additionally, the bar charts illustrate the preference degrees of both countries.

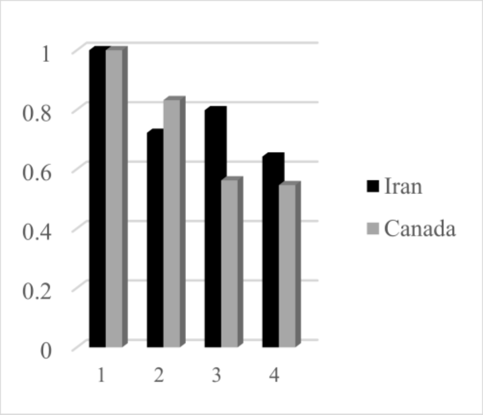
Final weights of sub-criteria are displayed in Table III.

As mentioned before, identified criteria in level 2 as a result of interviews are categorized into four groups:

1) Criteria related to security
2) Criteria related to system capabilities
3) Criteria related to user control
4) Criteria related to cost effectiveness

As it can be seen in Fig.3, the highest rank is dedicated to criteria related to security, in both countries. Second and third criteria are different in Iran and Canada, but forth criteria in both countries are cost effectiveness.

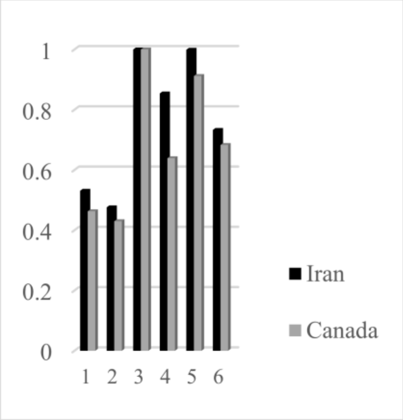
Identifying and Prioritizing The Evaluation Criteria	1	2	3	4
1	-, -	1, 1	1, 1	1, 1
2	0.722, 0.832	-, -	0.916, 1	1, 1
3	0.798, 0.562	1, 0.725	-, -	1, 1
4	0.624, 0.546	0.904, 0.706	0.818, 0.978	-, -



1- Security 2- User control 3- System capabilities 4- Cost-effectiveness

Fig. 3. Arithmetic means and preference degrees of sub-criteria level 2

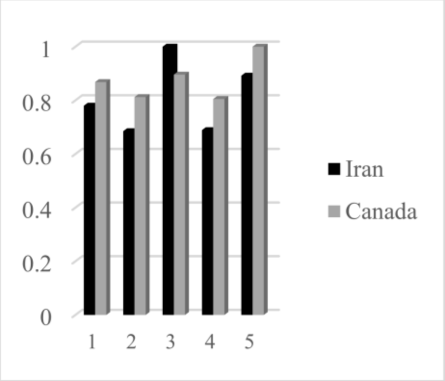
Criteria related to security	1	2	3	4	5	6
1	-, -	1, 1	0.531, 0.463	0.671,0.822	0.541, 0.558	0.803, 0.778
2	0.939, 0.971	-, -	0.476, 0.43	0.614, 0.791	0.487, 0.526	0.745, 0.747
3	1, 1	1, 1	-, -	1, 1	1, 1	1, 1
4	1, 1	1, 1	0.854, 0.639	-, -	0.858, 0.732	1, 0.957
5	1, 1	1, 1	0.999, 0.912	1, 1	-, -	1, 1
6	1, 1	1, 1	0.733, 0.683	0.873, 1	0.739, 0.775	-, -



1- Revocation 2- Conditional Release 3- Confidentiality & user's privacy 4- Sharing Prevention 5-Security & Stealing Protection 6- Integrity

Fig. 4. Arithmetic means and preference degrees of sub criteria level 3 related to *security*

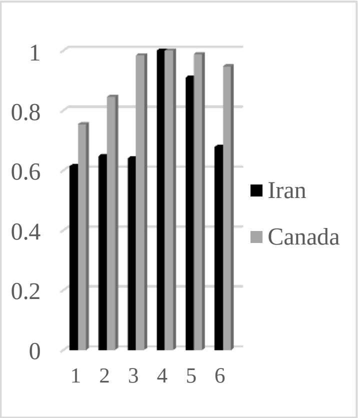
Criteria related to user control	1	2	3	4	5
1	-, -	1, 1	0.78, 0.968	1, 1	0.883, 0.868
2	0.91, 0.934	-, -	0.685, 0.901	1,0.987	0.789,0.812
3	1, 1	1, 1	-, -	1, 1	1, 0.896
4	0.898, 0.947	0.985,1	0.679,0.914	-, -	0.78, 0.805
5	1, 1	1, 1	0.892, 1	1, 1	-, -



1- User chosen identity provider 2- User in the middle 3- User consent 4- Delegation 5- Verifiability

Fig. 5. Arithmetic means and preference degrees of sub criteria level 3 related to *user control*

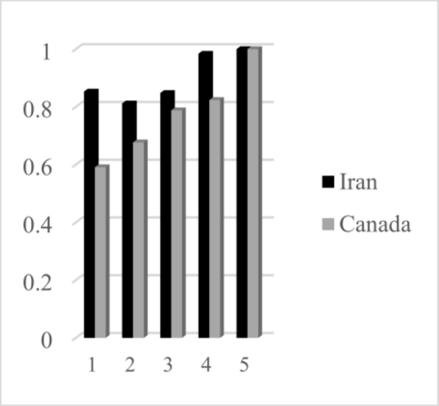
Criteria related to system capabilities	1	2	3	4	5	6
1	-, -	0.969, 0.909	0.976, 0.767	0.614, 0.754	0.701, 0.779	0.932, 0.812
2	1, 1	-, -	1, 0.859	0.648, 0.845	0.734, 0.868	0.964, 0.901
3	1, 1	0.993, 1	-, -	0.64, 0.984	0.726, 1	0.957, 1
4	1, 1	1, 1	1, 1	-, -	1, 1	1, 1
5	1, 1	1, 1	1, 0.993	0.91, 0.988	-, -	1, 1
6	1, 1	1, 1	1, 0.962	0.678, 0.947	0.765, 0.969	-, -



1- Scalability 2- Portability 3- Notification 4- Dependable 5- Accountability 6- Auditing

Fig. 6. Arithmetic means and preference degrees of sub criteria level 3 related to *system capabilities*

Criteria related to cost-effectiveness	1	2	3	4	5
1	-, -	1, 0.905	1, 0.805	0.87, 0.763	0.853, 0.591
2	0.961, 1	-, -	0.97, 0.895	0.828, 0.853	0.812, 0.677
3	0.992, 1	1, 1	-, -	0.864, 0.961	0.848, 0.788
4	1, 1	1, 1	1, 1	-, -	0.984, 0.824
5	1, 1	1, 1	1, 1	1, 1	-, -



1-Data Minimization 2- Availability 3- Fault tolerant 4- Usability 5- Service protection

Fig. 7. Arithmetic means and preference degrees of sub criteria level 3 related to *cost-effectiveness*

TABLE III. FINAL WEIGHT OF SUB CRITERIA

Iran		Canada	
Criterion	**Final absolute weight of criterion**	**Criterion**	**Final absolute weight of criterion**
Revocation	0.037	**Revocation**	0.038
Conditional Release	0.033	**Conditional Release**	0.035
Confidentiality & User's Privacy	0.069	**Confidentiality & User's Privacy**	0.082
Sharing Prevention	0.059	**Sharing Prevention**	0.056
Security & Stealing Protection	0.069	**Security & Stealing Protection**	0.075
Integrity	0.051	**Integrity**	0.058
User Chosen Identity Provider	0.043	**User Chosen Identity Provider**	0.053
User in the Middle	0.039	**User in the Middle**	0.053
User Consent	0.057	**User Consent**	0.056
Delegation	0.039	**Delegation**	0.052
Verifiability	0.051	**Verifiability**	0.065
Scalability	0.036	**Scalability**	0.026
Portability	0.037	**Portability**	0.029
Notification	0.036	**Notification**	0.034
Dependable	0.057	**Dependable**	0.038
Accountability	0.051	**Accountability**	0.034
Auditing	0.037	**Auditing**	0.033

Data Minimization	0.038	**Data Minimization**	0.028
Availability	0.035	**Availability**	0.032
Fault Tolerant	0.038	**Fault Tolerant**	0.035
Usability	0.044	**Usability**	0.039
Service Protection	0.044	**Service Protection**	0.048

V. Conclusion and Future Research

According to literature review, transformation of Identity Management Systems can be in the range of development of silo models to federated user-centric identity management models. User-Centric Identity Management Systems should consider scalability and cost-effectiveness issues from users' perspective. Scalability is important because users register with a growing number of services and deal with complexity of managing more personal credentials which has become an impediment [21]. This paper presented an approach for identifying and prioritizing appropriate criteria in order to evaluate user-centric digital identity management systems. It is believed that no single perfect set of criteria is perceived which can be implemented in all user-centric identity management systems. four categoriesare proposed to place the evaluation criteria for accomplishing the notion of user-centricity. It can be observed that based on pairwise comparison matrix and preference degrees of sub-criteria, the highest rank is dedicated to criteria related to security.This could be due to the fact that security issues enhance the trust to these systems which is very important for the user. In addition, most of the survey participants have had users' account in financial institutions and banks.

The second-best criteria in developing country (e.g. Iran), are system capabilities whereas user control in the developed countries (e.g. Canada) have had this spot as the second best criteria. Perhaps for the reason that, digital identity management systems have been more used in developed countries like Canada than developing countries is because system capabilities are more advanced in the developed countries so users are more concern with user control. Lastly, cost-effectiveness criteria have had the least priority both in developed and developing countries. Furthermore, considering sub-criteria of confidentiality and user's privacy, dependability, user consent and service protection in Iran, whereas Confidentiality and user's privacy, dependability, verifiability and service protection in Canada were the ones with highest preference degrees resulted from prioritizing criteria using fuzzy AHP. Based on literature review, it can be concluded that the future outlook of this research will be further taxonomies of appropriate criteria in which the most predominant one could be specified regarding to assessment of user-centric systems. Interoperability with traditional identity management systems would be an asset for this user-centricity concept as it should incorporate the advantages presented by the previous approaches and focus on adaptability [2]. Another important direction for future work is unifying the corresponding criteria implementable in user-centric devices, applications and solutions that facilitates user control and privacy when accessing increasing amount of online services [35]. Currently, web identity management is a technology centered concept, designed to be profitable for service providers but not for users. The browser must be a user-centered identity layer between the service provider and the user, leading to better control for user over his/her identity attributes [13]. Progress in digital identity management systems will become feasible to deploy user-centric paradigm which operate on a massive scale and control the full life cycle of digital identities from creation to termination, maintaining its major advantage that is, involvement in each transaction and improving its main drawback which is not being able to handle delegation [6] along with focusing on users, controlling what information is shared about them, the content of the information and who is allowed to access it [12].

Acknowledgment

We would like to thank the students of faculty of Management and Accounting in Shahid Beheshti University, John Molson School of Business in Concordia University, University of Montreal, University of Quebec in Montreal and University of Toronto as well as Sebastian Medina Lopez Computer Technician at University of Quebec in Montreal, Prof. Dimitrios Hatzinakos at University of Toronto and director of Identity, privacy and Security Institute at UoT, Dr. Jian Yun Nie, full professor at IT department of University of Montreal, Eve Maler, VP Innovation and emerging technology at ForgeRock, and Andre Boysen, chief identity officer at SecureKey Inc. for their support and encouragement as well as sharing their thoughts and experiences with us.

References

[1] G. J. Ahn, and M. Koo. (2007, Nov). User-centric privacy management for federated identity management. Presented at International Conference on Collaborative Computing: Networking, Applications and Work sharing.

[2] G. J. Ahn, M. Ko, and M, Shehab. (2009, June). Privacy enhanced user-centric identity management. Presented at IEEE International Conference on Communications. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] Baldwin, A., Casassa Mont, M., Beres, Y., & Shiu, S. (2010). Assurance for federated identity management. Journal of Computer Security, 18(4), 541-572.

[4] G. Ben Ayed (2014), Architecting user-centric privacy as-a-set-of services, Digital identity related privacy framework, Ph.D. dissertation, Dept. IS, Lausanne. Univ., Lausanne, Switzerland, 2014.

[5] G. Ben Ayed, and S. Ghernaouti-Hélie. (2011, Sept). Digital identity management within network information systems, From Vertical Silos View into Horizontal User-Supremacy Processes Management. Presented at 14th International Conference on Network-Based Information Systems. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[6] A. BhargavSpantzel, J. Camenisch, T. Gross, and D. Sommer. (2007, Oct). User Centricity: A Taxonomy and Open Issues. Journal of Computer Security. 15 (5), pp.493-527.

[7] P. Bramhall, M. Hansen, k. Rannenbeg, and T. Roessler. (2007, July). User-Centric identity management, New trends in standardization and regulation. IEEE Security & Privacy. [Online]. 5 (4), 84-87.

[8] J. Camenisch, A. Shelat, D. Sommer, S. Fischer-Hubner, M. Hansen, H. Krasemann, G. Lacoste, R. Leenes, and J. Tseng, (November 2005), "Privacy and identity management for everyone," DIM '05., New York., NY, pp. 20-25.

[9] D. Y. Chang. (1996, Dec). Applications on the extent analysis method on fuzzy AHP. European Journal of Operation Research. [Online]. 95(3), 649-655.

[10] D. Choi, S. H. Jin, and H. Yoon. (2007, June). Trust management for user centric identity management on the internet. Presented at IEEE International Symposium on Consumer Electronics.

[11] M. T. Chu, and R. Khosia, (2010), Benchmarking of communities of practice model for R&D organizations, Presented at 6th European Conference on Management Leadership and Governance., London, pp. 76-77.

[12] W. Claycomb, D. Shin, and D. Harelland. (2007, Oct). Towards Privacy in Enterprise Directory Services: A User-Centric Approach to Attribute Management. Presented at 41st Annual IEEE International Carnahan Conference on Security Technology.

[13] R. Cottrell, (2011), User-centered identity management, evaluating the role of the browser, Project Report, Faculty of Life Sciences., University College London, London, 2011.

[14] Digital identity management- Enabling innovation and trust in the internet economy, (2011), OECD, Organization for Economic CO-Operation and Development, Paris, 2011.

[15] O. Duran, and J. Aguilo. (2008, Apr). Computer-aided machine-tool selection based on a Fuzzy-AHP approach. Expert Systems with Applications, 34(3),17871794.

[16] T. M. Eap, M. Hatala, and D. Gašević. (2007, July). Enabling user control with personal identity management. Presented at IEEE International Conference on Services Computing.

[17] T. El Maliki, and J. Seigneur. (2007, Oct). A survey of user-centric identity management technologies. Presented at International Conference on Emerging Security Information, Systems and Technologies.

[18] T. El Maliki, and J. Seigneur, (2013), "Online identity and user management services," Computer and Information Security Handbook, 2nd ed. MA, Morgan Kaufmann Publishers, ch. 25, pp. 459–484.

[19] M. Hansen, A. Pfitzmann, and S. Steinbrecher. (2008, May). Identity management throughout one's whole life. Information Security Technical Report. 13(2), pp. 83-94.

[20] M. Hoffmann, (2005), User-centric identity management in open mobile environment, Privacy, Security and Trust within the Context of Pervasive Computing, 1st ed. City of Publisher, Springer US, pp. 99–104.

[21] A. Jøsang, and S. Pope. (2005, May). User centric identity management. Presented at AusCERT.

[22] C. Kahraman, U. Cebeci, and Z. Ulukan. (2003). Multi criteria supplier selection using fuzzy AHP. Journal of Enterprise Information Management. 16(6), 382-394.

[23] M. Kwiesielewicz, E. V. Uden, (2004, Apr). Inconsistent and contradictory judgment in pairwise comparison method in the AHP. Computers and Operations Research. 31 (5), 713-719.

[24] A. H. I. Lee. (2008, Feb). A fuzzy supplier selection model with the consideration of benefits, opportunities, costs and risks. Expert Systems and Applications. 36(2), 2879-2893.

[25] A. H. I. Lee, H. Y. Kang, C. F. Hsu, and H. C. Hung. (2009, May). A green supplier selection model for high-tech industry. Expert Systems with Applications. [Online]. 36(4), 7917-7927.

[26] D. Mashima, D. Bauer, M. Ahamad, and D. M. Blough, (2011), User-centric management architecture using credential-holding identity agents, Digital Identity and Access Management, PA, IGI Global, ch. 5, pp. 78-96.

[27] R. Marx, H. S. Fhom, D. Scheuermann, K. M. Bayarou, and A. Perez, (2010) Increasing security and privacy in user-centric identity management: the IdM card approach," International Conference on P2P., Washington., DC, 2010, pp. 459-464.

[28] A. Noorul Haq, and G. Kannan. (2006, July). Fuzzy analytical hierarchy process for evaluating and selecting a vendor in a supply chain model. The International Journal of Advanced Manufacturing Technology. [Online].29(7-8),826-835.

[29] A. Pashalidis, and C. J. Mitchell, (2003), A Taxonomy of Single Sign-On Systems, Information Security and Privacy, Springer Berlin Heidelberg, pp. 249-264.

[30] W. Pedrycz, P. Ekel, and R. Parreiras, (2011), Decision-Making in System Project, Planning, Operation, and Control: Motivation, Objectives, and Basic Concepts, Fuzzy Multicriteria Decision-Making: Models, Methods and Applications, 1st ed. New Delhi, India: John Wiley & Sons, ch. 1, sec. 1.3, pp. 9-10.

[31] V. Poursalidis, and C. Nikolaou. (2006, September 4-8) A new user-centric identity management infrastructure for federated systems. Trust, Privacy, and Security in Digital Business. 4083.

[32] M. Quasthoff, and C. Mienel, (2007). User-centricity in healthcare infrastructure. LNI. [Online]. 108, pp. 141-152.

[33] S. Rieger. (2009, May). User-centric identity management in heterogeneous federations. Presented at Fourth International Conference on Internet and Web Applications Services.

[34] T. L. Saaty, and L. G. Vargas, (2012), Why is the principal eigenvector necessary?, Models, Methods, Concepts, and Applications of the Analytical Hierarchy Process, 2nd ed. New York, Springer Science & Business Media, ch. 4, sec. 4.1, pp. 63–64.

[35] S. Suriadi, E. Foo, and A. Jøsang. (2009, March). A user-centric federated single sign-on system. Journal of Network and Computer Applications. 32(2), pp. 388-401.

[36] E. Triantaphyllou, and S. H. Mann. (1995, Jan). Using the analytical hierarchy process in decision making in engineering applications: some challenges. Inter'I Journal of Industrial Engineering: Applications and Practice. 2 (1), pages.

[37] G. H. Tzeng, and J. J. Huang, (2012), Analytical Hierarchy Process?, Multiple Attribute Decision Making: Methods and Applications, FL, CRC Press, ch.2, pp. 15-16.

[38] P. J. M. Van Laarhoven, and W. Pedrycz. (1983). A Fuzzy extension of Saaty's priority theory. Fuzzy Sets and Systems. 11(1-3), 199-227.

[39] D. D. Vecchio, J. Basney, and N. Nagaratman. (2005, July). CredEx: user-centric credential management for grid and web services. IEEE International Conference on Web Services.

[40] J. Vossaert, J. Lapon, B. De Decker, and V. Naessens. (2013, April). User-Centric identity management using trusted modules. Mathemathcal and Computer Modeling. 58(7-8), pp. 15921605.