A SURVEY ON FEDERATED IDENTITY MANAGEMENT SYSTEMS LIMITATION AND SOLUTIONS

Maha Aldosary and Norah Alqahtani

Department of Computer Sciences,
Imam Mohammad Ibn Saud Islamic University, Riyadh, KSA

ABSTRACT

An efficient identity management system has become one of the fundamental requirements for ensuring safe, secure, and transparent use of identifiable information and attributes. Federated Identity Management (FIdM) allows users to distribute their identity information across security domains which increases the portability of their digital identities, and it is considered a promising approach to facilitate secure resource sharing among collaborating participants in heterogeneous IT environments. However, it also raises new architectural challenges and significant security and privacy issues that need to be mitigated. In this paper, we provide a comparison between FIdM architectures, presented the limitations and risks in FIdM system, and discuss the results and proposed solutions.

KEYWORDS

Federated Identity Management, Identity Management, Limitations, Identity Federation.

1. INTRODUCTION

Federated Identity Management (FIdM) is a concept that helps to link user's digital identities and attributes stored on several sites. It also allows cooperation on identity processes, policies, and technologies among various domains to simplifies the user experience. FIdM typically involves Identity Providers (IdPs) and Service Providers (SPs) in a trust structure called Circle of Trust (CoT). Based on a business agreement all the identifiable information of users is federated at a central location such as the Identity Provider IdPs who is responsible to pass authentication tokens to SPs, and SPs after that provide their resource to the user. FIdM is considered a promising approach to facilitate secure resource sharing among collaborating participants in heterogeneous IT environments [1].

Many advantages are demonstrated by FIdM systems such as reduce the cost, provide convenience for the users, and interoperability among Identity Management systems in addition to support single sign-on SSO service and other valuable services. However, it has limitations that present several security and privacy risks due to the valuable information shared across domains in the FIdM using loosely coupled network protocols. The risks and limitations in FIdM require to be introduced and explained to find appropriate solutions to mitigate these risks.

In this paper, we discussed the concept of personal identity in a real-world and digital identity as a prelude to the identity management systems. The notion of Identity Federation was discussed in this work, we also provided a comparison between FIdM architectures such as liberty alliance, security assertion markup language SAML v2.0, WS-Federation, and Shibboleth, etc. In this

paper, we presented the limitations of Federated Identity Management based on how it affects the user. Finally, we discussed the solutions proposed in literature to mitigate the risk of these limitations.

This paper is organized as follows: Section 2 gives background and basic information that needs to be understood before discussing the FIdM system. The concept of identity federation and the comparison between architectures that implement FIdM is given in section 3. Related works are in Section 4. Section 5 presented the limitation and risks in the FIdM. A discussion of the solutions provided in section 6 before the paper is concluded in section 7.

2. BACKGROUND

2.1. Identity

Human identity is the representation of an individual by several properties which indicates that person, reflecting its uniqueness, and distinguish that person from others. These properties could be intrinsic (e.g. DNA, retina scan, fingerprint), descriptive (e.g. name, birthplace, birthdate), demographic (e.g. gender, occupation), geographic (e.g. country, address, postcode), or psychographics (e.g. preferences, interests).[2]

The identity of an individual consists of a large number of personal properties. All subsets of the properties form partial identities of the person.[3]The person may have multiple different partial identities depending on the context. These partial identities could also relate to roles the person plays. Identity involves all the primary characteristics that make each person unique but also all the characteristics that enable belonging to a particular group as well as established position within the group[4].

In today's world, living and working in the networked environment requires digital identity for each individual, it has allowed us to interact, transact, communicate, share reputations, and create trusted relationships with devices, people, and businesses electronically. Digital identity is the representation of identity in a digital system, Roussos et al[4] describe the digital identity as the electronic representation of personal information of an individual or organization (name, phone numbers, address, demographics, etc.).

Despite that there is a strong association between real life and digital identity, digital identity breaks from the restriction of everyday life, allowing users to exceed the boundaries of the real world [5]. Clarify that digital environments granted the users the chance to get rid of the human qualities of age, race, gender, and disability.

2.2. Identity Management

Identity management (IdM) is defined as a set of procedures, policies, and technologies that help authoritative sources as well as individual entities to manage and use identity information, it also provides access and privileges to end-users through authentication schemes[6]. Identity management procedures include management of the identity lifecycle, management of identity information, and management of entity authentication as an initial step for authorisation.

Identity Management responsible for handling the lifecycle of identity, its creation, maintenance, and eliminating a digital identity, by providing the credentials and means for identification during the preparatory process, through to authenticating and authorising access to resources, and to revoking access credentials and identities. Identity management is a crucial part of many security

services since it assures user legitimacy. Therefore, identity management is an integral part of any access management system[7].

There are numerous technologies, services, and terms related to identity management such as Directory services, Service Providers, Identity Providers, Digital Cards, Digital Identities, Web Services, Access control, Password Managers, Single Sign-on, Security Token Services, Security Tokens, WS-Trust, WS-Security, OpenID, OAuth, SAML 2.0 and RBAC.

Identity management is particularly used to authenticate a user on a system and make certain whether that user is allowed or unauthorized to access a particular system. IdM also covers issues such as how users obtain an identity, the protection of that identity and the technologies supporting that protection. Digital identity management technology is an essential function in enhancing and customizing the network's user experience, protecting privacy, underpinning accountability in transactions and interactions, and respecting regulatory controls [8].

3. IDENTITY FEDERATION

Federated identity management (FIdM) is when multiple enterprises allow individuals to use the same identification information or login credentials to obtain access to the services or networks of all the enterprises in the group. The partners in an FIdM system are accountable for authenticating their users and for ensuring their access to the networks.

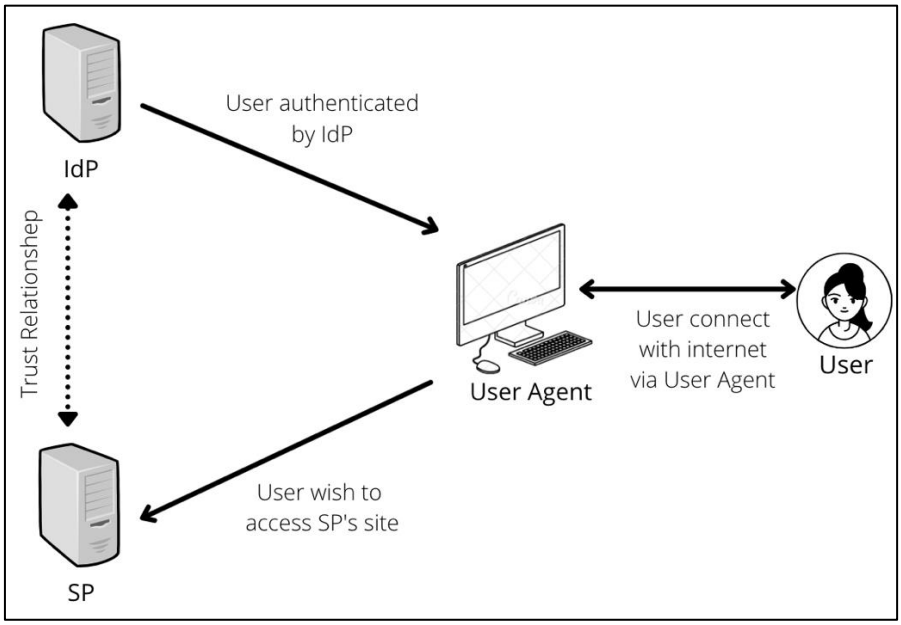

Figure 1. Component of FIdM system

The federated identity model includes four logical components:[9]

- A user is a person who acquires a specific digital identity to interact with an online network application.
- The user agent is a software application or browser that runs on any device such as PC, mobile phone, and medical device. The online interactions of a user always take place via an agent, which can allow identity information flow or mediate it.

- The service provider (SP) site is a Web application that offloads authentication to a third party, which also might send the SP some user attributes. Because the SP depends on external information, it's often called a relying party (RP).
- The identity provider (IdP) is a Web site that users log in to and that occasionally stores attributes of common interest to share with several SPs.

In a Federated identity management system, the user might have one or more local identities issued by service providers (SPs), in addition to a single identity issued by the identity provider (IdP) within a specific domain called a circle of trust (CoT). A standard CoT is composed of a single IdP and multiple SPs. In CoT, the IdPs must be trusted by all the SPs within it. Each SP could be a member of more than one CoT. A user can federate its IdP-issued identity with the local identities issued by SPs within the same CoT. [7]

With FIdM the user's credentials are always stored by the IdP. When a user registers into service, they do not have to provide their credentials to any of the SPs. Instead of authenticating directly with the user, the SP trusts the IdP to verify the user's credentials. The IdP then authorizes the user to the application of SP, and the user is then allowed to access the service. Therefore, the user in FIdM systems never provides their credentials to anyone but the IdP.

FIdM presents numerous benefits to the various stakeholders, it offers users the single sign-on (SSO) capability that allows them to proceed between the various SPs with no need to authenticate or login again, it allows SPs to offload the cost of managing user attributes, passwords and login credentials to trusted IdPs, it provides scalability, allowing SPs to provide services to a greater number of users, it allows IdPs to maintain close relationships with end-users and sell them more services, as well as extract fees from the SPs they support.[10]

Table 1. A Comparison between FIdM and SSO

	FIdM	**SSO**
Single access	To multiple system across various organization	To different services within a single organization
User credential	Given only to Idp	Given to any system the user logging into
Log-in to several services	Allow	Allow
Use of the same credential	Allow	Allow
Authentication process	Only once in the same working session	Only once in the same working session
Identity federation	Supported	Not supported

FIdM has aspects that are similar to single sign-on (SSO), but they are different at their core. FIdM gives you SSO, but SSO does not necessarily give you FIdM. Despite that the SSO and FIdM both allow users to log in to several services using the same login credentials, there are two things that FIdM does that SSO cannot: Firstly, SSO allows users to access multiple systems but only within a single organization, whereas FIdM allows users to log into systems across various organizations. Secondly, FIdM is more secure than SSO. For SSO, the user credentials are still being provided to any system that the user is logging into. While with FIdM, user's credentials are only given to the IdP exclusively.

Certainly, FIdM depends heavily on SSO technologies to authenticate the users across diverse websites and apps, however it has advanced these technologies further. Therefore, while FIdM does provide users SSO, SSO does not offer all of the benefits that FIdM does. Table 1 present a comparison between FIdM and SSO.

FIdM presents economic and convenience advantages to both the users and the organizations that employ it. However, there are some serious security considerations, techniques like strong authentication must be implemented for a secure SSO because the SSO system may introduce a single-point-of-failure. [9] Moreover, FIdM requires a lot of trust and open communication between partners that choose to make use of it. Organizations that are considering creating or joining an identity federation need to assure that they agree upon all factors. [10]

3.1. Federated Identity Management Architectures

3.1.1. Liberty alliance

Liberty Alliance is a project presented first in 2001. according to the official web site of the project [11], it is a consortium of more than 150 member includes governments and companies from around the world. The consortium is committed to creating an infrastructure that provides support for all existing and emerging network access devices and has defined interoperability requirements developing an open standard for federated network identity for products that meet its specifications. The specifications developed by the Liberty Alliance Project enable individuals and organizations to control their identity information securely also it is providing conveniently by supporting SSO service which is the service that enables users to interact with different service providers or Web sites with trust relationships by signing in just once.

The main objectives of the Liberty Alliance Project Specifications are to Serve as open standards for SSO, management of federated identity, and web services. Also, it aims to promote permission-based sharing of personal identity attributes and Enable consumers to protect their network identity information. Additionally, aims to create an open network identity infrastructure that supports all current and emerging user agents.

The specifications in the Liberty Alliance are enclouding the following components: Liberty Identity Federation Framework, Liberty Identity Web Services Framework, Liberty Identity Service Interface Specifications, Schema Files and Service Definition Documents, and Support Documents. They are developed to enable federated network identity management. Using web redirection and open-source technologies such as SOAP and XML, they enable distributed, cross-domain interactions[11][12]

For more information about Liberty Alliance: [13][14][15][16]

3.1.2. Shibboleth

Shibboleth is a project created first by US-based Internet2 in 2003. It developed an open-source, standards-based system that provides access management for individuals to a resource depending on their role instead of their identities which means that Role-based attributes are used in the Shibboleth system. Shibboleth allows the affiliated institution of the user to authenticate the user to permit access to on-campus applications and the resources licensed by the library from service providers [17]. to protect the user's privacy, Shibboleth sends anonymous identification to the service provider.

Additionally, Shibboleth provides authorization service that helps sites to make decisions for individual's access and privileges in online resources by transport the role attributes securely between the Identity Provider site (affiliated institution) and Resource Provider site to determine whether the user has a right to access the resource or not. SSO feature is supported in the Shibboleth system which makes the system more flexible and convenient.

For more information about Liberty Alliance: [13][18][19][20]

3.1.3. WS-Federation

The Web Services Security Framework is an identity management approach proposed by International Business Machines Corporation and Microsoft Corporation with other companies. As in Liberty Alliance, they provide several specifications such as WS-Security, WS-Trust, and WS-Security Policy. These specifications determine how to control the assertions (security tokens) that contain identifiable information about the user and issued by an identity provider. The security tokens help the service provider SP to decide to wither or not the user have a right to access the service resource.

According to [21][22], WS-Federation builds upon the base WSS specifications to define mechanisms that enable resources to be shared securely between different domains. The specifications introduce many services include security token service STS which is the IdP service that issues identity tokens to users based on their authentication. authorization service which decides giving access right to the user.

For more information about WS-Federation:[21][23]

3.1.4. Security Assertion Mark-up Language SAML V2.0.

The first release of the Security Assertion Mark-up Language SAML was in 2002 by the Organization for the Advancement of Structured Information Standards OASIS. SAML is standard based on Extensible Mark-up Language XML helps to manage the authentication and authorization processes between identity providers and service providers. The SAML system includes four main concepts which are assertions, protocols, profiles and bindings. Where assertion is the declaration user information asserted by the identity provider IdP for a service provider SP. The SAML protocol is helping to determine the rules on how to embed the SAML elements inside the request/response packet and on how to process them.

Transporting protocol messages using existing widely deployed communication protocols like HTTP (Hypertext Transfer Protocol) or SOAP (Simple Object Access Protocol) was described by The SAML bindings specification (SAMLBind). besides, The SAML profile specification (SAMLProf) provides many profiles that describe how the SAML elements can be used to implement a use case and achieve interoperability. [24][25][26]

3.1.5. Other Architectures

In addition to the FIdM Architectures that we discuss above, there are other federated architectures that designed originally for relatively simple applications such as OpenID [27] which is open-source user-centric and decentralized Identity management system. OpenID connect [28] which is a simple identity layer on top of the OAuth 2.0 specifications family. It is the third generation of OpenID technology. It helps the SP to authenticate the End-User based on the authentication performed by an Authorisation Server, as well as to obtain user attributes in an interoperable and REST-like manner. Besides, SCIM (System for Cross-domain Identity

Management) which is a specification designed for cloud-based applications to manage user identities and services [29]. In Table 2, we provide a comparison between Liberty alliance, Shibboleth, Security Assertion Mark-up Language SAML V2.0., WS-Federation, OpenID and OpenID connect. The comparison based on the target area, storage of Identity information, Single Sign-On, Single Log-Out, Identity Mapping, Security Tokens and Access to web applications.[30][31]

Table 2. Comparison Between FIdM Architectures

	Liberty alliance	**SAML V2.0.**	**WS-Federation**	**Shibboleth**	**OpenID connect**	**OpenID**
Identity mapping	By opaque identifiers	Via pseudonym service	Via pseudonym service	By short-term random IDs	Using (STS) chains and JavaScript mapping	Using (STS) chains and JavaScript mapping
Area targeted	Business interactions	Business interactions	Business interactions	Digital academic resource sharing	Developer and programmer	Supporting developer and programmer
Identity information storage	User info could be distributed and federated	User info could be distributed and federated	User info could be distributed and federated	Centrally located and only attributes sent to SP	Attributes and info are distributed IdP	Attributes and info are distributed IdP
Single sign-on	Supported	Supported	Supported	Supported	Supported	Supported
Single log-out	Supported	Supported	Not supported	Not supported	Supported	Supported
Security tokens	Extends SAML assertions for Communicating authentication And authorisation security Tokens between providers	Extends SAML assertions for Communicating authentication And authorisation security Tokens between providers	Builds on ws-security's Profiles and Kerberos	Extend the IdP to support InfoCard profiles using SAML assertions as security tokens	Use json security tokens (json web token) to communicate user attributes	Use json security tokens (json web token) for user attributes
Access to Services	Supports access of both Web Services and web applications	Supports access of both Web Services and web applications	Designed only for Web Services	Only supports access by web browsers to web apps	Support browser-based JavaScript, web app and native mobile apps	Support browser-based JavaScript, web app and native mobile apps

4. RELATED WORKS

The author in [23] has published a research paper which covered the most important technologies and solutions that support federated identity management. the Security Assertion Markup Language (SAML) was one of these technologies, SAML is a generic framework that provides the essential mechanisms for achieving Single Sign On and identity federation in different environments. The Shibboleth, Liberty Alliance framework, and WS-Federation were also presented in this work as further solutions of federated identity management. The author of this paper has presented a comprehensive architecture and provided features of these technologies and solutions. and discusses some of the deployment and usability aspects related to it. Several other identity federation solutions also exist that were left out of the scope of this paper, such as OpenID.

A structured survey on challenges related to Federated Identity Management System have been provided by J. Jensen. Et al [32] they have presented a narrative of the basic challenges and issues that appeared in adopting federation technologies. For solving these technical challenges, a great effort has been carried out in a lot of research which were presented by the authors of this work. Also, to learn more about organisational needs and expectations to Federated Identity Management the authors have defined the baseline for carrying out a case study.

Malik, H at el. [33] have identified a pivotal factor for developing a holistic FIM model or framework which are techniques that support trust management and trust establishment, consistent rights of access across Circles of Trust (CoT), preservation of user privacy, adaptation to unpredicted events a continuous monitoring of collaborating entities. In addition, the authors provide an extensive comparative analysis on existing FIM frameworks and models to identify enhancement areas and challenges in FIdM Systems. The also provide an analysis for the existing models and frameworks against a set of attacks to deduce the level of security they provide.
In [9] E. Maler. Et al. have describe the federated identity model. Furthermore, they have discussed security and privacy issues of Federated Identity Management Systems and its architectural challenges. They in addition profile three important federated identity protocols namely the OpenID specification, The Security Assertion Markup Language (SAML) and the InfoCard specification underlying Microsoft's Windows CardSpace.

The authors in [34] believe that improving efficiency of business collaborations are depend on a crucial factor which is Managing digital identities across trust domains. build up a federation for Federated Identity Management will help of provide the necessary platform for collaboration. In this work authors investigate trust requirements for identity federation topologies, and they began their investigation from the classical structure of a Circle of Trust (CoT) then they identify more complex patterns such as overlapping federations. the necessary trust requirements that must be met to allow trusted constellations, and risks for identity and service providers are identified for each pattern in this research.

R. Horbe. Et al. [35] elaborate in their work the important requirements required to ensure a privacy by design for Federated Identity Management (FIdM) of systems. Which is minimum identification, closures data based on need to know, inhibit linking across privacy domains, transparency and control the user in Information security. Then they have transposed these requirements into specific architectural requirements. in addition, the authors have evaluated several FIdM models with respect to these requirements. The have took into consideration the viewpoints of business, legal and system architecture.

5. LIMITATIONS IN FEDERATED IDENTITY MANAGEMENT SYSTEM

FIdM is a technique that allows the participating entities i.e., Service Providers (SPs) and Identity Providers (IdPs), to collaborate on identity operations, technologies, and policies. FIdM also enables users of heterogeneous IT environments to share each other's resources[32]. All the user identities in a FIdM system are federated at a central position, i.e., the Identity Provider (IdP). IdPs are responsible to proceed the authentication tokens to SPs, and after that SPs can provide their services to the requestor i.e., the user. It is also possible that the user has accounts with various IdPs, and the SP communicates with the relevant IdP for the set of attributes required[33]. While FIdM is in general seen as a good thing, it does have some disadvantages. Based on how it effects user we determine the following limitations:

5.1. Trust

Any Federated Identity system is based fundamentally on mutual trust. The interactions in federated identity management systems occur only between pre-configured entities or closed CoT. Due to the use of static establishment of trust, which is the method where entities' trust relationship such as that between IdPs or SPs must be pre-configured that done either during the registration phase to the system or via a trust negotiation process offline. Such limitation especially for a huge number of participating (IdPs and SPs) makes the system impractical, unscalable, and hard to establish a trust relationship at runtime[36][33].

In any identity federation, each participating member must create and identify policies and security protocols which poses another challenge. Every member then is obligated to follow these rules, which may cause problems when various companies have different rules and requirements. Furthermore, since an organization can be a member of different federations, following these several policies and rules may become a challenging.

Current specifications of FIdM provides only the basic technical mechanisms to establish trust between participating members. However, they do not detail the requirements that need to be met before establishing these relationships.

5.2. Privacy

Privacy and data protection are a major concern in FIdM system due to personally identifiable information that shared between entities. where the premier goal of FIdM models is to share identity attributes[32] there is no guarantee to prevent SPs and IdPs from misusing of identity information of users. Even though there are regulations such as [37] and [38] and privacy policies that protect the privacy of user's sensitive data but unfortunately there are no requirements to enforce these regulations and policies. Furthermore, many studies [33][9][34] proved that many SPs and IdPs sites are collecting, processing, and sharing data of users without user consent.

5.3. IdP discovery

The IdP discovery is the process of determining where authentication requests are going to be forwarded whenever a user wants to access an identity-based service [9]. One of the major significant security limitations in most of FIdM standards such as Shibboleth, Liberty, and OpenID is that IdP discovery is performed on the SP server. This limitation could be exploited by a malicious SP to redirect a user to a web site masquerading as the IdP, which could then acquire the user's security credentials.[13]

Furthermore, FIdM systems rely on the constant communication between individual users and a centralized identity provider (IdP) for purpose of authenticating and grant authorisation. If the metadata used to authenticate a user to the IdP was compromised, through leaks, or any sort of attacks such as phishing attacks, an adversary would gain the same access to the federated identity provides to all other participating members.

5.4. Lack of attribute-aggregation support

Another limitation of FIdM systems is that users can only choose one of their IdPs in any single working session with an SP, after that the IdP sends authentication and attribute assertion to the SP. Therefore, authorization is restricted to a subset of the user's identity attributes. This isn't sufficient especially for Web-based services. There is a huge need for a mechanism that allows users to aggregate attributes from multiple IdPs in a single service session. This model could effectively help to protect the user's identifiers and prevents IdPs from exchanging data about users without their permission. However, each IdP still knows that a federated user has several attributes at the other IdP[39].

In Liberty, only one IdP can be queried in a single working session, and for any IdP in shibboleth, the authorisation framework only allows a single attribute authority (i.e. the Attribute Authority Service (AAS)) to be queried for user attributes. OpenID is also suffering from a lack of attribute-aggregation support[13].

5.5. Complexity for The User

The usage of online services and transactions is growing every day, it is becoming necessary to grant the users and the service providers the tools they needed to make more transactions and expand the available services and the level of interaction and trust [40].

A drawback of FIdM based on SAML is the complexity of the protocol and resulting effort for configuration. Another limitation is the complexity for the user, especially because of the need from the user to choose their IdP at the Discovery Service (DS) and the users have to remember which federations they belong to, along with username and password. On the user side, the management of the identity is getting more complicated if the user uses multiple federations[41].

5.6. Security

Identity theft is a serious concern in FIdM[1]. Security issues regarding a stolen identity will affect all federation partners, credentials (e.g. username and password pairs) must be protected in federated systems.

Common attacks are impersonation attacks with stolen credentials. FIdM enabled systems to authenticate service requests by a security token attached to the request message. Therefore, impersonation attack can also be conducted by stealing user's security token which has been authenticated, this token can be used to access resources in the federated environment.[32]
An important property of FIdM is SSO. However, a crucial challenge was addressed by Madsen et al. [42] they claim that federated SSO makes the job of attackers easier. That because after the attackers conduct a successful identity theft within a federation, they could compromise resources of all federated SPs, which leads to exposure of critical data.

Another important aspect is message security, improper message security result in concerns for identity theft. Regarding identity management, techniques to protect message confidentiality and

integrity are crucial to protect sensitive identity attribute and prevent modification of identity attributes. According to Maler and Reed[9]. Systems are vulnerable if it does not provide security tokens to service request messages, through digital signatures, and check the message integrity before use.

OpenID does not support any proof-of-rightful-possession methods, while in shibboleth the use of proof-of-rightful-possession methods is optional. Therefore, an IdP might not provide a user with the means to prove rightful possession of security token to an SP. Such an approach increases the risk of an attacker using a stolen token to earn access to SP resources. [13]

5.7. Revocation

In FIdM, revocation means disabling identity data, often represented as identity attributes in security tokens, therefore they can't be used for identification and authorization purposes anymore. Current FIdM systems lack practical and efficient revocation techniques, this may lead to security violations. Revocation is an important issue in credential-based systems[40].

6. DISCUSSION AND RESULTS

This section presents the existing solutions for the challenges and limitations that been discussed in the previous section. In table 3 we provide a summary of the solutions suggested to each limitation discussed in section 4:

Table 3. Solution suggested for each limitation

LIMITATION	SOLUTION SUGGESTED	REFERENCES
Trust	Dynamic trust establishment	[43][44][33]
	Independent trust establishment mechanisms	[32]
	Ensure identity trust through SAML credential	[45]
	Trusted Computing Technologies	[46]
	Identity assurance	[47][48]
Privacy	Pseudonyms	[9][48]
	Undetectability	[49]
	Unlinkability	[40][49]
	Decentralized identity	[42]
	Privacy by design	[35]
IdP discovery	List of IdPs	[41]
Lack of attribute-aggregation support	Supporting attribute-aggregation	[39]
Complexity for the user	User-centric approaches	[33][48][41]
	Smart contract	[50]
Security	Encryption	[32]
	Digital Signature	[51]
	User identity distribution	[1]
	Zero-knowledge proofs	[1]
	Channel security	[52]
	Authorisation policies	[48]
Revocation	Limit token lifetime	[32]

In systems like cloud computing systems or web services, trust relationship needs to be processed on-demand, and at runtime which cannot be done in static trust establishment. So, the dynamic establishment of the trust relationship between entities (IdPs or SPs) in FIdM systems with the help of factors like data on the SLA and reputation of the IdP/ SP could solve such issue. In [43] and [44] a FIdM systems with dynamic trust establishment was proposed.

In this paper [33] the researchers identified a set of factors that are fundamental for developing a holistic FIdM framework or model. These factors are Trust Management, Trust Establishment, User Privacy, Consistent User Access Rights across CoTs, Continuous Trust Monitoring, and Adaptation to Environmental or Unanticipated Changes. Based on these factors, they also presented a comparative analysis that helps identifies challenges and areas of improvements in FIdM. Choosing a Trust Management and Trust Establishment scheme depends on the user requirement. However, user privacy and alignment of user access rights across different CoTs need to be handled with both Trust Management and Trust Establishment schemes.

In this paper, [45] presented a trusted federated identity management mechanism. This mechanism helps to ensure identity trust through SAML credentials, to guarantee the trustworthiness of the federated identity management procedure.

Trusted Computing Technologies can help to solve authentication, privacy and trust concerns in federated identity management systems. Khattak et al. in [46] have presented three threats in federated systems: Identity theft, Misuse of Information gathered by malicious IdPs and SPs, and trust relationship issues due to no or weak trust among users, IdPs and SPs. A Trusted platform (TP) is presented that confirms the rules of the Trusted Computing Platform Alliance (TCPA) specification to counter these threats. The presented framework can help to secure user privacy; however, it doesn't help for situations that unidentified at requirements engineering time [35.].
For preserving privacy and protect user identities, pseudonyms are an important technique, especially when multiple web services cooperate to provide an aggregated offering that requires user-attribute sharing. [9]

If SPs are trusted to link authorization requests to identities, Pseudonymous authorisation is implemented by Project Liberty, OpenID, Passport, and Client-Side Federation. [48]

However, If SPs are not trusted with links between authorisation requests and identities, then anonymous authorisation is employed. Anonymous authorisation implemented by eliminating all unique identifiers from messages or credentials that the service provider doesn't explicitly require. For example, Shibboleth supports anonymous authorisation, although users can choose to reveal a persistent identifier. Project Liberty lets a service provider request an anonymous, temporary, identifier for a user if the service provider elects to support anonymous authorization [49].

Undetectability and Unlinkability are privacy properties that help to preserve user privacy. Undetectability means users' ability to conceal actions from other parties. While Unlinkability concerns hiding correlations between combinations of actions and identities either permanently or temporarily, making it impossible to recognize two separate usages of the same credential [40]. Whether the linking between two identities was between action and identity, or between two actions, the level of trust that users grant to other parties determine the most appropriate design choice. In Project Liberty, the IdPs with established business relations create Circles of Trust (CoT). Within a CoT, a user can choose to federate two identities, in this case, the IdPs exchange information and the identities are linked[49]

In[49]the researchers identify crucial design choices essential to current identity management systems. They adopt a privacy-driven approach, which focuses on three privacy properties: Undetectability of authorisation requests which is concealing the user actions, Unlikability which is concealing correlations between combinations of actions and identities, and Confidentiality which means enabling users' control over dissemination of their attributes.

The most appropriate choice if IdPs can be trusted only with attributes that are specifically issued to them but not trusted with identity linking is a decentralized identity management system in which various, distinct IdPs each function separately using different protocols and not aware of each other. This architecture lets users select which IdPs to trust with which attributes, and spreads critical attributes across distinct IdPs, thus ensuring unlikability of distinct identities. Most existing identity management systems, including Idemix, PRIME, Shibboleth, Higgins, CardSpace, OpenID, P-IMS, and U-Prove have adopted this approach [49].

Though FIdM has mitigated the significant privacy flaws of the current situation by several techniques such as pseudonymous authentication and limited attribute release. However, at the same time it also introduces new privacy issues, essentially by centralizing user data and making the track of user behavior easy and to link data of the same user together.

To mitigate these privacy risks the design process of FIdM systems needs to consider privacy requirements from the start. R. Hörbe and W. Hötzendorfer in.[35]focus on privacy by design requirements for FIdM systems. They presented a catalogue of privacy-related architectural requirements, joining up legal, business and system architecture viewpoints. Furthermore, the demonstration of concrete FIdM models showing how the requirements can be implemented in practice.

A common solution to the problem of IdP discovery is to provide a list of IdPs to the user from which the user must select the proper IdPs. However, this could be a problem especially when the list of possible IdPs gets extensive and the user, who usually ignorant about these issues, must conduct a choice. This is called the "where are you from" problem and is a significant concern regarding usability. Rieger. [41]mentions this problem and adds that because the users can be part of numerous federations this will complicate the situation more.

Liberty solves this problem by using the Liberty-Enabled Client (LEC) profile. This profile requires the participation of a Liberty-Enabled User Agent (LEUA) to handle the messages sent and received during the federation and authentication processes. [13]

It would enhance the practicality of FIdM if SPs could acquire user attributes from multiple independent attribute authority to be used in association with a particular IdP. Supporting attribute-aggregation will help to solve the limitation which users is limited to choose one of their IdPs in any single working session with an SP. [13]

The Liberty Alliance was the first group to address the problem of attribute aggregation through its model of identity federation. In this model, the first IdP to authenticate the user inquires if the user prefers to be introduced to other IdPs in the federation. Afterwards, when the user authenticates to another IdP, it invites the user to federate its second identity with that from the first IdP. If the user consents, the two IdPs each create a random alias for the user and exchange secretly. Thus, neither IdP have knowledge of the user's true login identifier at the other IdP, but each can refer to the same user through the random aliases, and thereby aggregate the attributes[39].

One solution to mitigate privacy concerns and the complexity of the user is to empower users to control their identities. Increasing users control over their information is a good solution to avoid the misuse of information and data leakage. A user-centric identity management system is developed essentially from the perspective of end-users, it aims to make the user task of managing digital identities easy by providing them with more control over their identities. [13] User-centric approaches extend the users' privacy as the user can decide which private information to send to the consumer (e.g., SP) as in [41]. There are many advantages of user-centric identity management such as higher usability and privacy for the users, simplification of the protocol and the configuration compared to SAML-based federated identity management and helps to create trust among cloud service providers in a federated environment[33].

In [40] the proposed system which enabling controlled access to and selective sharing of critical user attributes in FIdM solutions by integrating authenticated dictionary (ADT) into FIdM, can help to develop a user-centric and user-friendly attribute sharing system.

In this work,[50]they presented an identity management system that provides FIdM where the user can authenticate and transfer attributes to a relying party (RP) without the involvement of a credential service provider (CSP). They accomplish this by leveraging a smart contract running on a blockchain5. Their approach can increase privacy and reducing costs.

Regarding identity management, techniques to protect message confidentiality and integrity are essential to prevent compromisation of sensitive identity attributes or modification of identity attributes. This can be achieved through mechanisms such as encryption. [34]

Message security is essential in FIdM to prevent attackers and intermediaries from manipulating the messages that are in transit. Improper message security rises concern such as identity theft, false authentication, and unauthorised use of resources. Liberty Alliance specifications advised XML Digital Signature and Encryption[51] for encrypting a complete or a part of the SOAP message to preserve the integrity and confidentiality of its contents.

Bhargav-Spantzel et al. [1]recommended two kinds of techniques to protect the misuse of identity information: The distribution of user identity information among various entities and use techniques such as zero-knowledge proofs to prevent identity theft within an IdP or SP. They recommend that single central IdP is a problem in Shibboleth. Moreover, their work is also highlighting that Liberty does not consider untrusted SP or IdP within the specifications.

The availability of information in FIdM models can be ensured by having a common protocol or mechanism for communicating authentication and other information between parties and securing communication channels and messages. Channel security can be accomplished using protocols like TLS1.0/SSL3.0 or other protocols with security characteristics that are equivalent to TLS or SSL. However, these protocols can only provide security at the transport level and not at the message level. For channel security, Liberty specifications highly recommend TLS/SSL with well-known cypher suites[51]

FIdM requires communicating parties to provide controlled access to information to authorised users. Authorisation goal is to deals with what information a user has access to or which operations a user can perform. A permission-based attribute sharing mechanism, which enables users to specify authorisation policies on the information that they want to share is recommended by Liberty specifications. [48]

A common way to mitigate revocation challenges is to limit the security token lifetime. By reducing the time-to-live to seconds or minutes the vulnerability window in cases of

compromisation of the token will minimize. However, this may reduce the systems' usability as the user must reauthenticate to obtain a new valid security token. On the opposite side, when token expiration is set for a longer period, user will benefit from the seamlessness, but the risk of identity theft and compromising information will increase. [32]

7. CONCLUSIONS

FIdM is a concept that helps to link user's digital identities and attributes stored in several sits also allows cooperation on identity processes, policies, and technologies among various domains to simplifies the user experience. FIdM is considered a promising approach to facilitate secure resource sharing among collaborating participants in heterogeneous IT environments. In our paper, we discussed the concept of identity federations as well some FIdM architectures such as liberty alliance, security assertion markup language SAML v2.0, WS-Federation, and Shibboleth with a comparison between these architectures. Furthermore, we presented the limitations of federated identity management based on how it affects the user. We determine the following limitations trust, privacy, IdP discovery, lack of attribute-aggregation support, complexity for the user, security, and revocation. Finally, we discussed the solutions proposed to mitigate the risk of these limitations.

In future work, an in-depth analysis of privacy, security, and trust challenges in a federated environment will be conducted. Also, we will propose a FIdM system taking into consideration the limitations and solutions we found in this paper.

REFERENCES

[1] A. Bhargav-Spantzel, A. C. Squicciarini, and E. Bertino, "Establishing and protecting digital identity in federation systems," *J. Comput. Secur.*, vol. 14, no. 3, pp. 269–300, Jun. 2006, doi: 10.3233/JCS-2006-14303.

[2] Roger Clarke, "Identity Management? Or (Id)Entity Mismanagement?," *rogerclarke.com*, Nov. 05, 2004. http://www.rogerclarke.com/EC/ACSID0411.html (accessed May 08, 2021).

[3] S. Clauß and M. Köhntopp, "Identity management and its support of multilateral security," *Comput. Netw.*, vol. 37, no. 2, pp. 205–219, Oct. 2001, doi: 10.1016/S1389-1286(01)00217-1.

[4] G. Roussos, D. Peterson, and U. Patel, "Mobile Identity Management: An Enacted View," *Int. J. Electron. Commer.*, vol. 8, no. 1, pp. 81–100, Oct. 2003, doi: 10.1080/10864415.2003.11044287.

[5] J. D. Bolter, "Sherry Turkle, Life on the Screen: Identity in the Age of the Internet (London: Weidenfeld & Nicholson, 1996), 347pp. ISBN 0 297 81514 8," *Converg. Int. J. Res. New Media Technol.*, vol. 3, no. 1, pp. 131–133, Mar. 1997, doi: 10.1177/135485659700300112.

[6] "Roger Clarke's 'Authentication Model,'" Dec. 26, 2001. http://www.rogerclarke.com/EC/AuthModel.html (accessed May 09, 2021).

[7] 14:00-17:00, "ISO/IEC 24760-2:2015," *ISO*. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/79/57915.html (accessed May 10, 2021).

[8] C. Satchell, G. Shanks, S. Howard, and J. Murphy, "Identity crisis: user perspectives on multiplicity and control in federated identity management," *Behav. Inf. Technol.*, vol. 30, no. 1, pp. 51–62, Jan. 2011, doi: 10.1080/01449290801987292.

[9] E. Maler and D. Reed, "The Venn of Identity: Options and Issues in Federated Identity Management," *IEEE Secur. Priv. Mag.*, vol. 6, no. 2, pp. 16–23, Mar. 2008, doi: 10.1109/MSP.2008.50.

[10] D. W. Chadwick, "Federated Identity Management," in *Foundations of Security Analysis and Design V*, vol. 5705, A. Aldini, G. Barthe, and R. Gorrieri, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 96–120. doi: 10.1007/978-3-642-03829-7_3.

[11] "Home - Liberty Alliance." http://www.projectliberty.org/ (accessed May 09, 2021).

[12] S. S. Y. Shim, Geetanjali Bhalla, and Vishnu Pendyala, "Federated identity management," *Computer*, vol. 38, no. 12, pp. 120–122, Dec. 2005, doi: 10.1109/MC.2005.408.

[13] W. A. Alrodhan, "Privacy and Practicality of Identity Management Systems," p. 262.

[14] I. Friese *et al.*, "Bridging IMS and Internet Identity," in *2010 14th International Conference on Intelligence in Next Generation Networks*, Berlin, Germany, Oct. 2010, pp. 1–6. doi: 10.1109/ICIN.2010.5640948.
[15] G. Danezis and P. Golle, Eds., *Privacy enhancing technologies: 6th international workshop, PET 2006, Cambridge, UK, June 28-30, 2006: revised selected papers*. Berlin ; New York: Springer, 2006.
[16] "Liberty Alliance Releases Identity Assurance Framework / Press Releases / News & Events / Home - Liberty Alliance." http://projectliberty.org/liberty/news_events/press_releases/liberty_alliance_releases_identity_assurance_framework/ (accessed May 10, 2021).
[17] H. Eggleston and K. Ginanni, "Simplifying Licensed Resource Access Through Shibboleth," *Ser. Libr.*, vol. 56, no. 1–4, pp. 209–214, Mar. 2009, doi: 10.1080/03615260802686981.
[18] "Shibboleth Consortium - Shaping the future of Shibboleth Software," *Shibboleth Consortium*. https://www.shibboleth.net/ (accessed May 09, 2021).
[19] J. Paschoud and M. Garibyan, "Shibboleth for New Generation Access Management (uk Perspective)," *Proc. IADIS Int. Conf. WWWInternet*, pp. 365–370, Jan. 2005.
[20] J. Paschoud, "SHIBBOLETH AND SAML: AT LAST, A VIABLE GLOBAL STANDARD FOR RESOURCE ACCESS MANAGEMENT," *New Rev. Inf. Netw.*, vol. 10, no. 2, pp. 147–160, Nov. 2004, doi: 10.1080/13614570500053874.
[21] "Understanding WS-Federation." https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/bb498017(v=msdn.10) (accessed May 10, 2021).
[22] "ws-federation-1.2-spec-os.pdf." Accessed: May 10, 2021. [Online]. Available: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf
[23] J. Kallela, "Federated Identity Management Solutions," p. 8.
[24] I. Reid *et al.*, "Assertions and Protocols for the OASIS Security Assertion Markup Language," January 10, 2.
[25] S. Ferdous and R. Poet, "Managing Dynamic Identity Federations using Security Assertion Markup Language," *J. Theor. Appl. Electron. Commer. Res.*, vol. 10, no. 2, pp. 53–76, May 2015, doi: 10.4067/S0718-18762015000200005.
[26] R. Cover, "Security Assertion Markup Language (SAML)." http://xml.coverpages.org/saml.html (accessed May 10, 2021).
[27] N. Duan and K. Smith, "IDentiaTM - An Identity Bridge Integrating OpenID and SAML for Enhanced Identity Trust and User Access Control," presented at the Imaging and Signal Processing in Health Care and Technology, Baltimore, USA, 2012. doi: 10.2316/P.2012.773-032.
[28] "OpenID Connect | OpenID," Aug. 01, 2011. https://openid.net/connect/ (accessed May 10, 2021).
[29] J. Kang, Y. Elmehdwi, and D. Lin, "SLIM: Secure and Lightweight Identity Management in VANETs with Minimum Infrastructure Reliance," in *Security and Privacy in Communication Networks*, vol. 238, X. Lin, A. Ghorbani, K. Ren, S. Zhu, and A. Zhang, Eds. Cham: Springer International Publishing, 2018, pp. 823–837. doi: 10.1007/978-3-319-78813-5_45.
[30] U. Fragoso-Rodriguez, M. Laurent-Maknavicius, and J. Incera-Dieguez, "Federated Identity Architectures," p. 8.
[31] "wsfed-liberty-overview-10-13-03.pdf." Accessed: May 10, 2021. [Online]. Available: http://www.projectliberty.org/liberty/content/download/402/2765/file/wsfed-liberty-overview-10-13-03.pdf
[32] J. Jensen, "Federated Identity Management Challenges," in *2012 Seventh International Conference on Availability, Reliability and Security*, Prague, TBD, Czech Republic, Aug. 2012, pp. 230–235. doi: 10.1109/ARES.2012.68.
[33] A. A. Malik, H. Anwar, and M. A. Shibli, "Federated Identity Management (FIM): Challenges and opportunities," in *2015 Conference on Information Assurance and Cyber Security (CIACS)*, Rawalpindi, Pakistan, Dec. 2015, pp. 75–82. doi: 10.1109/CIACS.2015.7395570.
[34] U. Kylau, I. Thomas, M. Menzel, and C. Meinel, "Trust Requirements in Identity Federation Topologies," in *2009 International Conference on Advanced Information Networking and Applications*, Bradford, United Kingdom, 2009, pp. 137–145. doi: 10.1109/AINA.2009.80.
[35] R. Horbe and W. Hotzendorfer, "Privacy by Design in Federated Identity Management," in *2015 IEEE Security and Privacy Workshops*, San Jose, CA, May 2015, pp. 167–174. doi: 10.1109/SPW.2015.24.
[36] G. Bendiab, S. Shiaeles, S. Boucherkha, and B. Ghita, "FCMDT: A novel fuzzy cognitive maps dynamic trust model for cloud federated identity management," *Comput. Secur.*, vol. 86, pp. 270–290, Sep. 2019, doi: 10.1016/j.cose.2019.06.011.

[37] "General Data Protection Regulation (GDPR) – Official Legal Text." https://gdpr-info.eu/ (accessed May 10, 2021).
[38] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD." https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed May 10, 2021).
[39] D. W. Chadwick and G. Inman, "Attribute Aggregation in Federated Identity Management," *Computer*, vol. 42, no. 5, pp. 33–40, May 2009, doi: 10.1109/MC.2009.143.
[40] D. Shin, R. Lopes, and W. Claycomb, "Authenticated Dictionary-Based Attribute Sharing in Federated Identity Management," in *2009 Sixth International Conference on Information Technology: New Generations*, Las Vegas, NV, USA, 2009, pp. 504–509. doi: 10.1109/ITNG.2009.193.
[41] S. Rieger, "User-Centric Identity Management in Heterogeneous Federations," in *2009 Fourth International Conference on Internet and Web Applications and Services*, Venice/Mestre, Italy, 2009, pp. 527–532. doi: 10.1109/ICIW.2009.85.
[42] P. Madsen, Y. Koga, and K. Takahashi, "Federated identity management for protecting users from ID theft," in *Proceedings of the 2005 workshop on Digital identity management - DIM '05*, Fairfax, VA, USA, 2005, p. 77. doi: 10.1145/1102486.1102500.
[43] R. M. Alguliev and F. C. Abdullayeva, "Identity management based security architecture of cloud computing on multi-agent systems," in *Third International Conference on Innovative Computing Technology (INTECH 2013)*, London, United Kingdom, Aug. 2013, pp. 123–126. doi: 10.1109/INTECH.2013.6653643.
[44] M. V. Bhonsle, N. Poolsappasit, and S. K. Madria, "ETIS -- Efficient Trust and Identity Management System for Federated Service Providers," in *2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA)*, Barcelona, Mar. 2013, pp. 219–226. doi: 10.1109/AINA.2013.13.
[45] L. Liu and J. Gao, "Research on Trusted Federated Identity Management and Its Application," in *2009 First International Workshop on Education Technology and Computer Science*, Wuhan, Hubei, China, 2009, pp. 438–442. doi: 10.1109/ETCS.2009.627.
[46] Z. A. Khattak, S. Sulaiman, and J.-L. A. Manan, "A study on threat model for federated identities in federated identity management system," in *2010 International Symposium on Information Technology*, Kuala Lumpur, Malaysia, Jun. 2010, pp. 618–623. doi: 10.1109/ITSIM.2010.5561611.
[47] A. Baldwin, M. Casassa Mont, Y. Beres, and S. Shiu, "Assurance for federated identity management," *J. Comput. Secur.*, vol. 18, no. 4, pp. 541–572, Jun. 2010, doi: 10.3233/JCS-2009-0380.
[48] Dongwan Shin, Gail-Joon Ahn, and Prasad Shenoy, "Ensuring information assurance in federated identity management," in *IEEE International Conference on Performance, Computing, and Communications, 2004*, Phoenix, AZ, USA, 2004, pp. 821–826. doi: 10.1109/PCCC.2004.1395193.
[49] E. Birrell and F. B. Schneider, "Federated Identity Management Systems: A Privacy-Based Characterization," *IEEE Secur. Priv.*, vol. 11, no. 5, pp. 36–48, Sep. 2013, doi: 10.1109/MSP.2013.114.
[50] P. Mell, J. Dray, and J. Shook, "Smart Contract Federated Identity Management without Third Party Authentication Services," *ArXiv190611057 Cs*, Jun. 2019, Accessed: May 10, 2021. [Online]. Available: http://arxiv.org/abs/1906.11057
[51] "XML Encryption Syntax and Processing Version 1.1." https://www.w3.org/TR/xmlenc-core1/ (accessed May 10, 2021).
[52] "liberty-idff-guidelines-v1.2.pdf." Accessed: May 10, 2021. [Online]. Available: http://projectliberty.org/liberty/content/download/322/2378/file/liberty-idff-guidelines-v1.2.pdf

AUTHORS

Maha Aldosary is currently pursuing an M.Sc. degree in information security with Imam Muhammad ibn Saud Islamic University. She graduated with a bachelor's degree in computer science from the University of Tabuk. Her research interests include blockchain technology, IoT, identity management and information security.

Norah Alqahtani is currently pursuing an M.Sc. degree in information security with Imam Muhammad ibn Saud Islamic University. She graduated with a bachelor's degree in computer science from Shagra University. Her research interests include Cloud Computing, blockchain technology, identity management and information security.