Abstract: Identity as a Service (IDaaS) offers various Identity and Access Management (IAM) services like user authentication, authorization and Single Sign-on. These services have become an integral part of IDaaS these days for various business organizations. This paper focuses on the implementation of various IAM services like user authentication and authorization based on users roles and activities. A local cloud setup is established using a WAMP Server and a User Interface (UI) is also designed to implement the services. In this work, roles and activities have been assigned to students and Faculty of an organization and they are tested for various IAM activities. For added identity management, the users are checked for their identity credentials thrice and if they fail to enter the credentials correctly in these three attempts then their identity will be locked and will exited from the system and will not be allowed further.

Keywords: IDaaS, Identity and Access Management (IAM), WAMP Server, Single Sign-on (SSO), Authentication, Authorization, Cloud Service Providers (CSPs).

1. Introduction

Identity and access management (IAM) service is an important aspect of Identity as a service (IDaaS) in cloud environment. As most of the enterprises and organizations are migrating towards the deployment and use of various cloud service providers (CSPs) and cloud architectures for effective utilization of their resources, the security features of IDaaS plays crucial role in establishing integrity of the enterprise. Especially, features like Single sign-on (SSO) is one of the important security aspects of IDaaS that provides better user experience by entering the user’s authentication credentials only once and hence permitting the users to access multiple resources of an enterprise in a secured way. Single sign-on (SSO) is an application based on Security Assertion Markup Language (SAML). SAML is an XML based open standard developed by OASIS security Services technical committee. It asserts the identity of users to another system, without involving any other third party.

Security has always been a concern for many organizations and business enterprises and facing challenges in protecting their data and other business credentials in the cloud environment. This is because of the lack of trust mechanisms and proper concrete agreements between the enterprises and various Cloud Service Providers (CSPs). A lot of research is still going on to counter these security challenges in cloud environment. Especially dealing with the identity of their employees and other users and ensuring the integrity of their data is always important for a business enterprise to keep their data and other credentials confidential and secret from their competitors. In this context, user authentication and authorization is crucial and access management also becomes critical. These days many companies and organizations are now focusing on the deployment of various technologies and tools for effective handling of these issues. OAuth and SAML standard technologies that facilitate the effective implementation of features like Authorization, Authentication and Single Sign-on (SSO).
As the installation procedure of SAML and OAuth are complex, various smaller business organizations are showing interest to implement their IAM and IDaaS services in WAMP Server environment. WAMP is a web server stack that provides four key facilities namely the Operating System, Web Server, Web scripting language and the Data base. WAMP server stack environment is best suited to establish a cloud setup and implement various IAM services for smaller organizations.

2. Related Work and Literature Survey

Various commercial vendors already started working on the development of various tools and technologies to manage IAM and hence IDaaS services. Especially centrify developed its own licensed tool that integrates SAML technology [13]. Umme Habiba et all discussed about various identity management security issues and taxonomies at length[14]. Tri Hoang Vo at al presented the missing gap for moving enterprise applications in Inter-Cloud [15]. Securosis has presented a detailed study on various IAM cloud services [16]. David Nunez at al., has proposed a security model by integrating OpenID and proxy encryption scheme for better cloud based identity services[17]. Cloud Security Alliance discussed about various access management services in cloud[18]. Sean Deuby has mentioned in his article about the drawbacks of IDaaS. Tarek Kiblawi at al presented a closer look on the disruptive innovations in Cloud Computing and their impact on business and Technology [19].

Uthpala Subodhani Premaratne at al has designed and implemented a frame work for effective mechanism for trust negotiations. They proposed completely new metrics based on the potential attacks and the vulnerabilities. They have also demonstrated these metrics using historical data sets [20]. Dominick Bayer at al presented various authorization and authentication mechanisms and identity services based on identity [25]. OpenID technique also permits to implement Single Sign-On (SSO) service, without asking the user’s password credentials again and again [26]. Bharath Bhargava at al reviewed about the privacy techniques in Cloud Setup [27].

3. Methodology & Experimental Setup

Cloud networking is sharing data or information among few networking devices through centralized devices or a third party devices. In order to setup a cloud network, a group of networking devices through a centralized device a local setup is first designed using a WAMP server. To make a replicated clouding process this technique of local setup is useful. This creates a total interface where all the assets, information of layouts, panels, widgets, js etc. are hosted locally. A system where this WAMP is installed acts as a centralized system and the remaining systems that communicate to this system are the neighboring systems. By installing WAMP server software in a system it provides all the services that a server on air produces. For example services like creating own batch files, providing database and its administration. Plug-ins, predefined commands are integrated and are available installed while installing. These plug-ins are helpful for the identification of the individual services.

![Figure 1](https://example.com/developer-utilizing-services-via-local-server-to-establish-cloud-platform.png)

**Figure 1** Developer utilizing the services via local server to establish cloud platform

3.1 Setting Up of a Private Cloud Platform

Through local setup of clouding it is easy to communicate between systems of discussing the same information or gathering the data. Though this is applicable unless the communicating systems are nearby or simple put the proximity is restricted to an extent. This can be helpful for the fast or quick response for our work. This WAMP setup is prepared after the installation for the hosting and the experiment to be done that we have prepared to do. PHP helps to create the connection between the database connectivity and client UI. The UI is designed for the purpose serving the authentication. Authentication like Login and registration. Because the cloud platform on the whole is depends on this concept. So the process goes this way. Checking whether the user is already registered or not. If not register and then login is required. The registered user is given the priorities and is set accordingly.

3.2 Connection using Sample IP address
Since the connection is through the local networking, the URL is subjected to be the same. For example the connectivity to be unified is through the hotspot. Then every system that is communicating is under one IP address. So it is helpful to establish the communication through same address. The systems that are to be communicated are now replicating the real cloud services. They use the same URL and are connected together communicating the same information but with the authorization and privacy.

Figure 2 is the diagram that shows the information passing to the UI via Server.

3.3 Work Flow of Authentication Forum

The user is asked for the requisites like logins and if the user is valid then only he will be allowed to go further. Roles and activities have been assigned to students and Faculty of an organization and they are tested for various IAM activities. For added identity management, the users are checked for their identity credentials thrice and if the fails to enter his credentials correctly in these three attempts he identity will be locked and will exited from the system and will not be allowed further. i.e. three invalid logins leads to locking user account and a warning email will be sent to user mail. Only to those whose login have the authorization of getting the notifications, retrieving messages, requests, query contribution and notifying happens accordingly and those who don’t have this flexibility will not be allowed the access to these resources. Status checking mechanism feature is also implemented in this paper to see whether the user is present or not. It was shown in figure 3, where the the user is given the registration ID and password in the name of authentication and authorization.

4. Results and Discussions

In this methodology, a student is a specific role authorized by the admin of the forum and is first registered providing his attributes and logged in once he completes registration. Here the student has the capability to view the posted notifications and page 3 has the updated forums posted by faculty that can be viewed by him/her only. Figure 4 shows the WAMP Server setup.

Figure 3. Workflow of Authentication Forum

Figure 4. WAMP Server Setup

Figure 5, 6, 7, 8 and 9 shows about the screen shots and user interfaces regarding various authentication and authorisation.

Figure 5. User authorization Interface (Page 1)
Figure 6. User authentication Interface (Page 2)

Figure 7. Notification forum after authorized as a student (Page 3)

Figure 8. User is given few rights of editing profile (page 3)

Figure 9. Posted by Authorized student

References


and Parallel Computing Workshops (NPC 2007), 2007 IEEE.


[22] Peter Mell and Tim Grace,“The NIST definition of cloud computing”, NIST Special Publication 800-145 (SP800-145), National Institute of Standards and Technology, Gaithersburg, January 2011, pp. 1-52.


