Technology University Dublin
M.Sc. Advanced Software Development

Systems Architectures
Assignment 2

Identity Management System

Richard Madden

Lecturer: Giancarlo Salton

April 15, 2022

Contents

1 Review

1.1 Introduction

An identity management (IDM) system ensures that only people who have been provided authorisation can access an application, web resource or computer system. It combines policies and technologies for creating an organisation-wide process to identify, authenticate and authorise people, groups of people or software applications through attributes such as user access rights and restrictions[1]. Protecting identity, particularly in an era where e-commerce and network applications are used extensively throughout the internet, is one of the most critical security concerns that modern software systems architectures must adhere to.

Access rights, authentication and authorisation are all key components of any IDM system and while these properties are just as relevant for Cloud-based IDM systems as they are for traditional ones, the Cloud has a number of unique characteristics such as access control, scalability, virtualisation, provisioning, de-provisioning and multi-tenancy that need to be taken into consideration when designing an IDM system for the Cloud[2]. The conventional approach to IDM mainly deals with managing users and services and is quite static in nature, however Cloud IDM can be much more complex as it must also secure dynamic machines, virtual devices and control points among others[3]. Additionally, sensitive information needs to be appropriately managed in a Cloud environment, which raises a number of privacy and security concerns that can lead to a reluctance of organisations to move their critical identity information to the Cloud. Despite the challenges however, Cloud-based IDM solutions are growing in popularity and the market is currently estimated at $5.3 billion and expected to grow to $13.6 billion by 2026[4]. The advantages of outsourcing IDM to the Cloud, such as a consistent access control interface, superior security levels, granular access control to resources[5] as well as higher scalability and cost savings[6], are among the many reasons in the increased take-up rate of these solutions in recent years.

1.2 Cloud Identity-as-a-Service

Cloud Identity as Service (IDaaS) is essentially the management of identities in the Cloud, outside the organisational boundary and applications that use them rather than deployed on-premises[7]. The service is generally offered by a third-party provider for IDM functions such as user provisioning/de-provisioning, account changes/management, log monitoring as well as single sign-on (SSO) and multi-factor authentication (MFA). IDaaS is quite a

broad term however and can exist in a number of hybrid forms.

TU Dublin could benefit greatly from adapting an IDaaS approach to IDM in terms of gaining access to all the benefits of the Cloud, as well as reduced hardware costs and easier management, with a range of integration options available. That being said however, when an organisation externalises any portion of IDM to a third-party IDaaS provider, it comes with a number of security and privacy challenges (e.g. identity data locality, confidentiality, trust establishment, availability etc.). In respect of this, a proposed hybrid option for TU Dublin could be that identities are managed internally within the organisation while other components such as authentication and authorisation are externalised through Service Oriented Architecture (SOA). Identity data should be kept on site by TU Dublin, since IDaaS vendors don't take on the risks associated with losing critical identity information, other than perhaps the reputational damage they might incur if such a situation arose. On the other hand, TU Dublin's whole IT infrastructure could be compromised by such an event, as staff and students would be unable to access important resources such as Brightspace and Bongo, or an even worse scenario could unfold, if this identity data fell into the wrong hands.

1.3 Classification of Cloud-Based IDM Systems

There are various types of Cloud IDM solutions in existence, each of which has a number of strengths and weaknesses and each one usually involves four interacting entities; an end user, a service provider (SP), an identity provider (IdP) and a control party or regulatory body[6]. The following represent the most well known types of Cloud-based IDM systems:

- **Isolated Cloud IDM system:** This is one of the simplest models in which the SP and IdP are merged on a single server which is responsible for authentication and authorisation as well as the storage of identity information[6]. This type of system is generally adopted by small or medium-sized business, but unfortunately doesn't scale well for larger organisations and becomes unmanageable with a large amount of services and resources, as each service would need to know the credentials of authorised users.

- **Centralised Cloud IDM system:** Separates the functions of the SPs from the IdP. In this model, the IDM system is outsourced by several SPs to a single IdP that is responsible for the issuance, storage and management of identity data[8]. One drawback of this type of architecture is the single point of failure if the IdP goes offline.

- **Federated Cloud IDM system:** In the federated model, no single entity is fully controlling the identity information. Identity data is not stored on a central repository but rather distributed across multiple SPs and/or IdPs. In order to achieve such an architecture, all IdPs and SPs which take part in such a federation, must share a common trust relationship amongst each other and this therefore eliminates the need for individual authentication accounts[9].

- **User-Centric Cloud IDM system:** All identity data is stored directly in the users' domain (e.g. on a secure token such as a smartcard) and in this way the user remains in full control of their identity data, which can only be transferred by an IdP to a SP if the user explicity provides consent. User-centric IDM systems thus improve privacy by considering user preferences before disclosing identity information to the SPs however for Cloud-based SOA, it leads to quite a cumbersome user-experience in that each application/service must perform authentication and authorisation in order to permit user access[7].

- **Anonymous Cloud IDM system:** Capabable of keeping identity information secret from users and providers alike, however they suffer from a lack of trust between IdPs and SPs in order to achieve anonymity. Such systems can also be difficult to implement adequate logging and monitoring due to the use of users performing actions using a temporary identity[7].

The Federated Cloud IDM system is quite a popular architecture model and I believe it would be the most suitable solution for TU Dublin. When used in conjunction with the hybrid IDaaS aproach discussed previously, TU Dublin could establish a system of trust between their in-house system managing identity data and third-party IdPs/SPs (Brightspace, Bongo, Microsoft Outlook etc.). It would provide a smooth experience for end-users by allowing for cross-domain access and avoid students and staff having to manage individual accounts for multiple services. This model also follows the distributed storage architecture, where identity information is stored at multiple locations and information is linked across multiple IdPs in order to enhance security and reduce the risk of loss of data due to a natural disaster or terrorist attack at an individual data centre housing identity data.

2 Comparative Analysis

A number of commercial smart Cloud-based IDM offerings are available from key industry representatives. Some big names in this space include Cisco's Duo Secure Access, Microsoft's Azure Active Directory and Tenfold's IAM Solution. These Cloud-based IDM solutions all promote the concept of SOA, which defines a way to make software components reusable and interoperable via services that use a common interface standard and an architectural pattern so that they can be rapidly incorporated into an organisation[10]. These services are exposed using standard network protocols such as Restful HTTP and offer significant benefits to institutions such as faster time to market, greater business agility through reusability and the ability to leverage in-house applications and systems with one of these Cloud-based IDM platforms.

2.1 Duo Secure Access (Cisco)

Cisco's Secure Access with Duo Security is an IDM solution that is Cloud-managed and delivered and is designed to protect an organisation's applications using MFA, to verify user identity before granting access[11]. MFA requires a user to provide two or more verification factors in order to gain access to a system resource. When MFA has been embedded into an application, the extra layer of security that this method of authentication imposes makes it extremely difficult for a hacker to compromise a software system. One of the main benefits of MFA nowadays is that it is relatively cheap to deploy, largely due to the widespread use of software tokens on smartphones whereas previously hard tokens such as those distributed by RSA Secure ID would have significantly driven up deployment costs[12] and created a financial barrier for higher educational institutions to overcome in the past. Duo is designed to provide a simple and streamlined login experience for users and applications alike via a single, easy to use dashboard that works with SSO and can protect any application on any device. SSO is a mechanism that enables users to gain access to multiple applications or services using a single authentication action with an IdP[13]. This removes the obligation of users having to retain multiple sets of credentials and helps prevent bottlenecks in the authentication process, while at the same time leaving a system less vulnerable to phising attacks. In other words, students and staff within TU Dublin could access all the Cloud services and resources they need with one set of login credentials. Duo also uses the Security Assertion Markup Language (SAML) protocol to communicate between the IdP and the SP in order to authenticate a user. It relies on digital signatures and eliminates the use of passwords for user verification purposes. It is also a popular browser-based protocol since it does not rely on active content or cookies, as many users are not willing to use protocols that do rely on these

features due to security and privacy reasons[14].

One of the unique selling points of Duo is its ability to establish device trust by providing visibility into every single device on an organisation's network and enforcing health checks at every single login attempt. This is an essential aspect of a strong zero trust strategy. Given that an institution like TU Dublin will have students and staff connecting to its services through multiple devices, this aspect of Duo would help enforce access control across both managed and unmanaged devices and easily identify security risks like out-of-date or jailbroken devices. Duo also allows organisations to create custom access policies based on role, device, location, and many other contextual factors. This feature would greatly assist higher education institutions with the authorisation stage of IDM by enabling them to separate out access control levels for staff and students and restrict access for unmanaged devices connecting into the institution's network and also those accessing the network from different countries or regions. Finally, Duo also offers a VPN-less remote access proxy, the Duo Network Gateway, which can assist in facilitating remote access and would allow TU Dublin's lectures to be delivered remotely while at the same time enhancing privacy as this is the intended purpose of proxies, as they are designed to request the desired Cloud resource/service on behalf of their registered users/systems. The identity information that is forwarded for authentication/authorisation purposes, is of the Cloud proxy system rather than the actual user who has requested the service[7].

2.2 Azure Active Directory (Microsoft)

Azure Active Directory is Microsoft's Cloud-based IDM solution that is designed to protect an organisation's internal and external resources. Similar to Duo, Azure Active Directory supports SSO and MFA however in contrast to Cisco's offering which only supports SAML-based SSO, Microsoft's IDM platform offers a number of different SSO protocol options, such as SAML, OpenID Connect and OAuth, and applications can use password-based or linked-based SSO[15]. OpenID Connect and OAuth are similar in that user's don't need to login and share credentials, but instead these protocols use tokens that are encrypted in transit and therefore provide a framework which ensures a degree of anonymity on behalf of the user, thus enhancing privacy. Whereas SAML uses XML to communicate between the user's browser and IdP/SP, OpenID Connect uses REST/JSON which is designed to work quite well with both native and mobile applications, whereas the primary use case for SAML is web-based apps[16]. Microsoft strongly promote the concept of Conditional Access with their IDM solution as part of MFA. Conditional Access enables organisations to use identity-driven signals as part of their access control decisions, which helps enforce organisational policies[15]. These policies are enforced once

first-factor authentication has been cleared and are intended to be an organisation's first line of defence for scenarios like denial-of-service attacks. Some common signals that Conditional Access can take into account include user/group membership, IP location information, device/application type and calculated risk detection. In this way, Conditional Access could assist an institution like TU Dublin in identifying risky sign-in behaviour and predefined organisational policies could block access or only grant a student or staff member access once MFA has been completed or a device has been marked as compliant by a member of the IT team that supports the IDM environment.

Another major feature of Azure Active Directory is its Identity Protection tool, which assists an organisation in automating the detection and remediation of identity-based risks. Given the global reach of Microsoft as an organisation, it allows them to use machine learning algorithms to provide risk scores for billions of login attempts across millions of distinct accounts. These identity-based risks include anonymous/malware-linked IP addresses, atypical travel, leaked credentials, unfamiliar sign-in properties, etc[15]. This type of automation tool could help TU Dublin reduce the administrative and management costs of their proposed Cloud-based IDM platform as it would provide key reports to administrators, identifying risky users and suspicious sign-ins and cut out any manual actions that may be required by alternative platforms in this regard. Microsoft guarantees a seamless user experience of their IDM solution by offering a self-service option for password-reset and user-registration, which would not only make life easier for students and staff, but would also further reduce TU Dublin's administrative costs. The option of Hybrid Identity with Azure Active Directory would fit TU Dublin's IDM model quite well and make managing a mixture of on-premises and Cloud applications significantly less challenging than alternative solutions, as a common user identity is created, for authentication and authorisation to all resources, regardless of location. Finally, given that TU Dublin already uses a number of Microsoft applications such as Teams and Outlook, this could potentially be a good fit in securing these as well as other external and internal resources.

2.3 Identity & Access Management (Tenfold)

Tenfold's Identity & Access Management (IAM) solution is similar in many regards to the other commercial offerings discussed and is largely aimed at mid-market organisations. Tenfold claims to help organisation's lower their IT workload while at the same time boost cybersecurity and transparency[17]. Tenfold's solution uses a Role-Based Access Control (RBAC) authorisation scheme. RBAC usually restricts access based on a specific user's department, position and/or authority level as this generally corresponds well with what

permissions and level of access a user requires to carry out their job function and responsibilities. For example, within a higher educational institution a staff member would have access to add resource materials and submit assignment scores based on submissions from students to a service like Brightspace whereas students would be restricted to a more read-only type role. The systematic approach of RBAC for defining and maintaining roles offers a streamlined process for organisations to grant access based only on what a user requires, while also mitigating data breaches. Other useful features of Tenfold's IAM are its change tracking feature, which provides full documentation of any changes to users and privileges, for compliance and auditing purposes, and its reporting feature, which logs who has access to critical data at any given time and who requested, approved or implemented any type of change. In a multi-tenant Cloud environment it can be a significantly more challenging task to identify the person responsible for any security breach or misbehaviour and therefore appropriate logging and auditing features like those just discussed compliment the security of Cloud applications and resources.

Tenfold's IAM solution takes full advantage of Cloud SOA by offering a common interface to customers and ensuring easy implementation, allowing organisations to get up and running with their IAM platform in just a few weeks. It also offers seamless integration of third-party services via plugins. Tenfold's attractive licensing model could indicate a more cost-effective IDM solution for TU Dublin than Cisco or Microsoft's offerings, however they would probably need to integrate it with Azure Active Directory in order to secure on-premises applications and systems that exist outside the Cloud and a dual licensing model may not work as well.

2.4 Conclusion

All of the IDM solutions discussed are similar in a lot of aspects in that they ensure the security and privacy of an organisation's applications and resources but overall I believe Microsoft's Azure Active Directory would be the best fit for TU Dublin, offering different premium plans that could be tailored to the university's budget. I think Azure Active Directory's features such as it's Identity Protection tool and Hybrid Identity combined with the fact that TU Dublin use a number of existing Microsoft products mean that this platform could be implemented into the university in an efficient manner and also provide complete security protection from cybercriminals across its suite of in-house and Cloud-based applications and infrastructure.

3 Reflection

References

[1] https://www.vmware.com/topics/glossary/content/identity-management.html

[2] Habiba, U., Abassi A. G., Masood, R. & Shibli, M. A. (2013). Assessment Criteria for Cloud Identity Management Systems. *International Symposium on Dependable computing (PRDC 2013)*.

[3] Odun-Ayo, I., Falade, A. & Samuel, V. (2018). Cloud Computing and Open Source Software: Issues and Developments. *Lecture Notes in Engineering and Computer Science: Proceedings of The International Multi-Conference of Engineers and Computer Scientists, Hong Kong*, pp. 140-145.

[4] https://www.helpnetsecurity.com/2022/04/05/cloud-iam-market-2026/

[5] https://www.loginradius.com/blog/identity/identity-management-in-cloud-computing/

[6] Zwattendorfer, B., Zefferer, T. & Stranacher, K. (2014). An Overview of Cloud Identity Management-Models. *In Proceedings of the 10th International Conference on Web Information Systems and Technologies*, pp. 82-92.

[7] Habiba, U., Masood, R., Shibli, M. & Niazi, M. (2014). Cloud Identity Management Security Issues & solutions: A Taxonomy. *complex adapt syst model*, vol. 2, no. 1.

[8] Cao, Y. & Yang, L. (2010). A Survey of Identity Management Technology, *2010 IEEE International Conference on Information Theory and Information Security, Beijing*, 17-19 pp. 287-293

[9] Abayomi-Zannu T. & Odun-Ayo, I. (2019). Cloud Identity Management – A Critical Analysis. *Proceedings of the International MultiConference of Engineers and Computer Scientists 2019*, IMECS 2019.

[10] https://www.ibm.com/cloud/learn/soa

[11] https://duo.com

[12] Webb T (2013) An Architecture for Implementing Enterprise Multifactor Authentication with Open Source Tools.

[13] Belfaik, Y., Lmouhsndiz, A., Sadqi, Y. & Safi, S. C. (2022) Single Sign-On Revocation Access. In: Maleh Y., Alazab M., Gherabi N., Tawalbeh L., Abd El-Latif A.A. (eds) *Advances in Information, Communication and Cybersecurity*. ICI2C 2021. Lecture Notes in Networks and Systems, vol 357. Springer, Cham.

[14] Gross, T. (2003) Security Analysis of the SAML Single Sign-On Browser/Artifact Profile, *19th Annual Computer Security Applications Conference, 2003. Proceedings*, pp. 298-307, doi: 10.1109/CSAC.2003.1254334.

[15] `https://docs.microsoft.com/en-us/azure/active-directory`

[16] `https://www.sailpoint.com/identity-library/identity-management-protocols`

[17] `https://www.tenfold-security.com/en/`