Eamonn McClelland
C08776105

CLOUD COMPUTING - INTRODUCTION

- Cloud computing is a catch all term used to describe computer service provision over the internet (defined as the "cloud")
- Systems that utilise the cloud boast resource flexibility, scalable services and can deliver faster innovation
- Reduce or eliminate the need to maintain physical computer or networking hardware
- Accelerate delivery of new features and services through resource provisioning

CLOUD COMPUTING - FEATURES

- Services on the cloud are scalable, which can have their computational power increased or decreased depending its volume of usage
- Cloud services can be cost efficient, where a customer pays only for the services and scale they require

CLOUD COMPUTING - BENEFITS

- Some key benefits of leveraging a cloud computing service are:
  - Reliability
    - Cloud services are typically almost available and accessible
  - Scalability
    - Servers and applications on the cloud can be scaled, meaning their computing power, memory and networking capacity can be increased or decreased depending on user demand
  - Flexibility and cost efficiency
    - Anyone adopting a cloud service pay only for what they require, and cost can be reduced by automatically scaling during off-peak times

CLOUD COMPUTING - VIRTUALISATION

- Virtualisation is a term given to running a "virtual" computer inside of a real computer.
- It is a technology used to optimise available hardware resources
- Virtualised resources can be isolated from one another, potentially increasing security and scalability

CLOUD COMPUTING - CONTAINERISATION

- Containerisation, or containers are applications and components grouped together
- It allows for greater scalability through deployment of lightweight, portable applications
- Facilitates scalability and faster development and deployment turnaround

CLOUD COMPUTING – SERVICE MODEL

- Cloud services are typically provided as a service-oriented model
- Some concepts of service-oriented models:
- Infrastructure as a Service (IaaS):
  - Provides virtualised computing over a network
- Platform as a Service (PaaS):
  - Allows users to run and manage applications without needing to manage infrastructure
- Software as a Service (SaaS):
  - Deliver subscription based cloud software applications

Cloud Computing – Service Model

- Infrastructure as a Service examples:
  - Azure, Amazon Web Services (AWS), Google Cloud
- Platform as a Service examples:
  - Vercel, Heroku, Google App Engine
- Software as a Service examples:
  - Dropbox, Okta, Microsoft Office 365, nVidia GeForce NOW

Identity Management Solutions

An identity management solution, or IdM is a key aspect of security in a cloud environment where digital identities for individuals, or applications are used to restrict and secure access to a cloud environments resources. An identity management solution can assist in securing access to users data, providing access control to resources and help ensure data privacy is maintained.

Microsoft Entra ID

In the context of a popular cloud provider: Microsoft Azure, an identity management solution named Microsoft Entra ID (formerly Azure Active Directory) is available (Microsoft, 2024). Some of the core features provided by Microsoft Entra ID include:

- Single sign-on (SSO) and multifactor authentication
- Role-based access control (Azure RBAC)
- Consumer identity and access management
- Device registration
- Security monitoring and reporting
- Identity protection

Single sign-on (SSO)

A key feature of an identity management solution is single sign-on, whereby users can access all applications available to them utilising a single account, or method of signing on. This is a widely used concept in Software as a Service (SaaS) applications, where users can register and sign-on using an account from other providers (i.e. Google, Apple). This mitigates against the need for users to recall multiple usernames and passwords (Microsoft, 2024).

Multifactor authentication

Access security to a resource using single sign-on is one important factor in identity management, and this can be bolstered utilising multifactor authentication. Multifactor authentication requires that an authenticating user provide a secondary method of proving who they are when attempting to access a system. In terms of the IdM solution provided by Microsoft Entra ID, an SMS message, phone call, or the use of the Microsoft Authenticator mobile application are all used in conjunction with a password to complete an authentication journey (Microsoft, 2023).

Once a user is authenticated with Microsoft Azure, they are provided with a screen showing what exactly they have access to. Administrators can control what subscriptions and resources a user has via a conditional access. Role-based access control (RBAC) is another method of controlling what groups of users have access to which cloud resources. An example use case of employing RBAC in the Azure cloud environment is to grant database administrators access to database, or data lake

resources only, while restricting application developers access to resource groups where application services, container apps or Azure functions are deployed.

IdM in TU Dublin

Data privacy and access control are two key ethical considerations to make when planning to adopt any IdM in a University. One primary consideration to make in the context of data privacy is to ensure that user roles are absolutely clearly defined so that unauthorised intrusion on other students data is not a possibility. Carefully designed roles and use of role based access control (RBAC) are two important areas to emphasise.

Data storage location is another consideration to take into account. Since Azure is a cloud platform, it is possible to define where cloud components are located across the world. Ensuring that data protection (and ultimately GDPR) laws are adhered to, and user data is not being exported from the jurisdiction in which it is supposed to be stored must be taken into account.

Transparency and security are two other points to take into consideration. The cloud provider should employ clearly defined data storage auditing and reporting features. It should be possible to configure and deploy monitoring and alerting functionality, and the University should be clear on whom has access to these reports (Microsoft, 2023).

Bibliography

Microsoft. (2023, October 23). *Data protection considerations*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/entra/fundamentals/data-protection-considerations

Microsoft. (2023, October 23). *How it works: Microsoft Entra multifactor authentication*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

Microsoft. (2024, January 1). *Azure identity management security overview*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-overview

Cloud-based Identity Management Systems

A cloud based identity management system can be used to delegate responsibility for user registration, authentication and verification on an online platform. Cloud based identity management should reduce complexity of creating, configuring and deploying a portion of a system that handles user authentication and authorisation flows. For the purposes of this comparison, I've selected two cloud based providers: Microsoft Entra ID and Okta. Both platforms provide solutions that would suit use cases in an educational context.

Features

Okta and Microsoft Entra ID provide the following features, at least which would be applicable in an educational context with emphasis on security and ease of access:

Multifactor authentication – where user access requires a second mode of authentication to prove who they actually are
Single sign-on – users sign onto a single page, and have access to the range of resources to which they have been granted
Privileged access – access to certain resources can be sectioned off, permitting access only based on groups and user roles

Okta provides a user friendly way to interact with their workforce identity platform via an access gateway. The access gateway provides a convenient landing page, or dashboard from where users can access a plethora of external applications via Oktas integrations (Okta, n.d.).

Microsoft Entra ID is an identity management platform that allows users to access internal and external resources, including Microsoft 365 and has integrations with a large number of SaaS applications (Microsoft, 2024).

Security Features

Okta boast their workplace identity platform utilises zero trust when it comes to securing access to their platform (Okta). Zero trust is a security framework that essentially trusts nobody and no device on a network. With the level of traffic across an organisations cloud, and the potential for devices to move between or be connected to several clouds at a time, it's critical for a platform to prioritise protecting its own resources, with the mindset that trust should never be presumed and should be actively monitored (Dhiman, et al., 2024).

Microsoft do facilitate zero trust as a paradigm and guide users on how to configure their tenant to employ zero trust policies (Microsoft, 2024). Both platforms have ways of configuring monitoring and alerting should trust events arise, with Okta utilising their

own logging and monitoring tools, and Microsoft provide monitoring tools via Entra monitoring and health.

Data residency

Depending on the platform, and because both solutions from Okta and Microsoft exist on the public cloud, it is possible for data to be transported between, and stored at different geographic locations, depending on the users location. Typically user data would be stored on a node as close to their location as possible to ensure fast interaction when authenticating. Prior to choosing a solution, understanding data residency of the providers platform is of importance, and this should be transparently communicated to end users of the cloud system to ensure they agree to allow their data to be stored in processed in the manners defined by each system.

With Microsoft Entra ID, data is stored at the same location as the tenant, and the customer chooses where this will be upon creation of the tenant (Microsoft, 2024).

Within Okta, it is a similar scenario where the customer selects where user data will be stored. They have customer data stores in the USA, Japan, Australia and the EMEA region. They state that customer data protection is their top priority, where they meet industry standards and are certified to comply with FedRAMP, GDPR and HIPAA to name a few requirements (Okta).

It is vital to understand exactly where and how data will be processed and stored when it comes to end user data on a public cloud. It is also of importance to gain consent from, and inform individuals when their data might have been compromised. User data is unfortunately a commodity and should be treated as such.

Zero Trust Architecture

(Dhiman, et al., 2024)

This is a short summary and review of an article on a Zero Trust architecture.

A zero trust architecture is an emerging software security architecture paradigm. A zero trust architecture can be presumed as multi-faceted. There is no solitary technology or architecture that completely implements a zero trust model. In realising this, when designing an architecture, environment specific implementation strategies must be devised. The article referenced in this document discusses such implementation strategies and their logical components.

The paper delves into a comparative analysis of zero trust systems, where various technologies are assessed for their suitability. It discusses important parameters surrounding the importance of operational requirements over efficiency, delving into how open source software and microservices play a key part in enhancing security and rapid deployment of software, and maintenance simplification.

The paper further expands on the need to emphasize the inclusion of zero trust policies in future technologies and architecture types, including 5G/6G networking, edge computing deployments and further discusses intelligent zero trust applications as a security mechanism for untrusted networking components. It expands upon the use of artificial intelligence as a method of enhancing security measures in an architecture, which instigates a shift from reactive network security applications to proactive, where early detection is key.

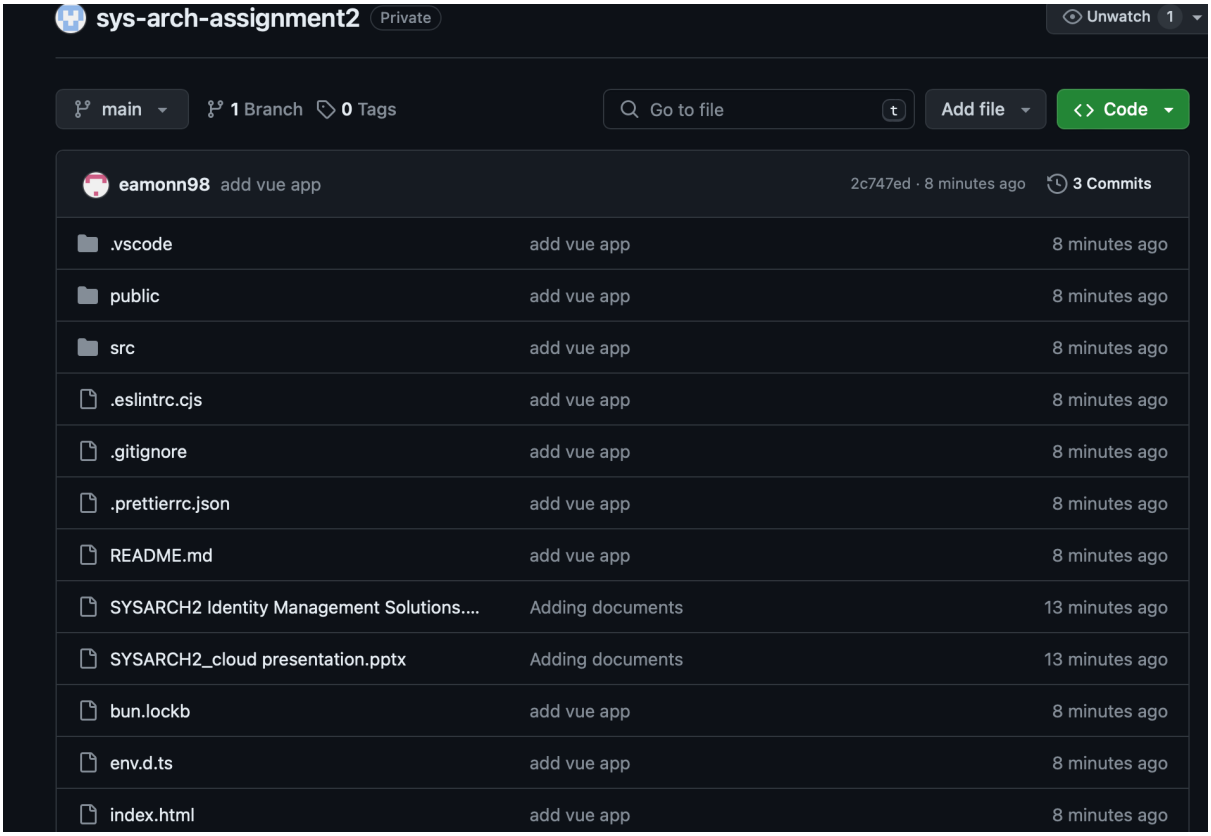
The study detailed in this paper emphasises the importance of correct application of authentication and access control approaches, where organisations constantly re-evaluate their trust in active connection points in their architecture. Since each organisation has their own unique implementation the application of a zero trust architecture will differ greatly from one use case to the next. The article elaborates on how it's important to make use of proper encryption techniques, and segment software into smaller components (micro services). Zero trust architecture is quite an emerging technology and will evolve with further studies such as this in the near and distant future.

Bibliography

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K., & Hamid, Y. (2024, February 19). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors, 24*(4), 1-19.

Deploying files to Azure

1. Created new resource group RG-SYSARCH-TUD
2. Create a free tier Create Static Web App to host some VueJS code
3. Created a repository on GitHub and pushed the PowerPoint document and the IdM document



4. Created a very basic VueJS application from the default template using bun
5. Push the VueJS application to the remote git repository on GitHub

6. During the configuration of the free tier static web app, pointed to the new GitHub repository

```
eamonn98@UNKNOWN sys-arch-assignment2 % bun create vue@latest

Vue.js - The Progressive JavaScript Framework

✓ Project name: … vue-project
✓ Add TypeScript? … No / Yes
✓ Add JSX Support? … No / Yes
✓ Add Vue Router for Single Page Application development? … No / Yes
✓ Add Pinia for state management? … No / Yes
✓ Add Vitest for Unit Testing? … No / Yes
✓ Add an End-to-End Testing Solution? › No
✓ Add ESLint for code quality? … No / Yes
✓ Add Prettier for code formatting? … No / Yes
✓ Add Vue DevTools 7 extension for debugging? (experimental) … No / Yes

Scaffolding project in /Users/eamonn98/Developer/TUD/sys-arch-assignment2/vue-project...

Done. Now run:

  cd vue-project
  bun install
  bun format
  bun dev
```

7. Ran into an issue - could not complete creation of the static web app without an error message
8. Began investigating alternative solutions, considering using Azure cli or a Bicep template to deploy the site
9. Added a tag for academic year, the application deployed successfully
10. New resource available at https://gentle-ocean-0d8491003.5.azurestaticapps.net Resource name for static web app: sysarch-c08776105
11. Accessing the site URI presents me with a screen saying the site will be ready later