Better Cloud Security

José Salazar, Isabella Roth, Yi Hu.
Northern Kentucky University

Abstract

With enterprises moving their IT infrastructure to the cloud using providers like **Amazon Web Services** (**AWS**), security problems are not reduced. In fact, cloud computing brings new security challenges. Our research investigates better solutions on how companies can securely and easily integrate applications in the cloud as well as aplications running on a local server.

A third party authentication service was designed to an application running on a local server; A cloud-based Active Directory (database of user credentials) service was linked to an AWS virtual computer run ning an application; and a local Active Directory was proposed to be connected to an AWS virtual computer.

Implementing authentication through a third party application was the easiest and least expensive solut ion. However, implementing any of the other solutions ensures more layers of security given the focus on information security of the cloud service provider, AWS.

Introduction

When we talk about Cloud Computing, we are refering to companies such as **Amazon**, **Google**, and **Microsoft** creating a solution to the high costs of computationally powerful computers, by replicating such computers in their servers, and making them available as a service anyone can rent at very reasonable prices.

However, that also brings other types of challenges and vulnerabilities to be addressed. We will particularly be investigating and proposing alternatives to the manage and storage of user credentials to access resources like email, applications, and sensitive information without putting that information at risk.

Methods and Materials

We based our research in the Empirical Method. We followed an AWS Active Directory tutorial **[1]** and an implementation guide from the service provider Auth0 **[2]**. We created an AWS-managed AD in **AWS**, linked it with a previously created and deployed AWS instance (Virtual Computer) and modified the instance's security group to allow access from our computers. Both the instance and the AWS-managed AD were located in the same network domain, and established a relationship of trust among every entity within the domain with the purpose of being able to securely share information and resources between all of them without the need of revealing sensitive information like username or password.

We also created an Angular web application and implemented a service, which is basically a piece of code, that calls **Auth0**'s API requesting it to communicate with social networks like Facebook, Twitter, or even Gmail on behalf of the web application to perform authentication using the profile's credentials.

Regarding materials used, we used our personal computers to host an authentication application built on Angular, and Amazon Web Services (**AWS**) instances (Virtual Computers) to host Active Directory User Credentials, to which we could connect remotely by using computer programs that handle Remote Desktop Protocols.

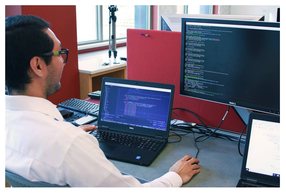


Figure 1. Working at the Lab.

Figure 2. Also working at the lab.

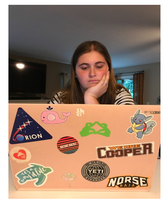
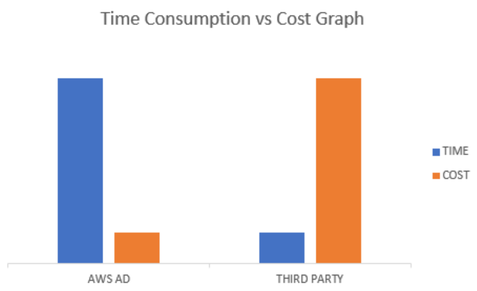


Figure 3. Working from home.

Results

The implementation of a third-party service, like **Auth0**, for authentication proved to be less time-consuming, but more economically expensive in the long run. Whereas, implementing an **AWS**-managed Active Directory in the cloud is more time-consuming but less economically expensive in the long run.



Discussion

- It is thought that for smaller companies, in terms of users and budget, using a third-party service provider is more convenient.
- For larger companies, it is more convenient to implement a more robust solution that involves using already existing user credentials, even with the extra layer of more configuration steps.

Conclusions

Implementing a third-party service like **Auth0** to perform user was the easiest, and most economic option, money-speaking. However, once the barrier of 7000 active users is passed, **Auth0** begins charging for their services.

The other option, an AWS-managed Active Directory in the cloud, was much more difficult to implement and more time consuming. The fact that AWS's documentation was neither very well organized nor straight-forward, adds an extra layer of difficulty to the configuration. On the other hand, in the long run, this option seems more convenient to larger companies given the fact that most of them already host on-premise (In-house) their own Active Directories, and moving their infrastructure to the cloud could significantly reduce their operational costs.

Future Directions

With the purpose of experimenting with other options to find a suitable solution for any kind of business, it is proposed to connect an existing on-premise Active Directory to a **Simple Active Directory** in the cloud, and the next steps could be directed on this direction.

References

AWS Active Directory. c2018. Amazon Web Services; [accessed 2018 Jun 20]. https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_tutorial_test_lab_deploy.html .
Auth0. c2013-2018. Auth0 Inc; [accessed 2018 Jul 5]. https://auth0.com/docs .

Acknowledgements

We would like to thank **CINSAM** and the **UR STEM** program for the funding, the resources, and giving us the opportunity of having this experience which for some of us worked as eye-opener for our future careers. And, on top of that, we had so much fun.