DOI: https://doi.org/10.30837/csitic52021232170

Security of Web Applications Using AWS Cloud Provider

Vladyslav Lysakov[1]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: vladyslav.lysakov@nure.ua

Oleksandr Sievierinov[2]

[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: oleksandr.sievierinov@nure.ua

Igor Taran[3]

[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: igor.taran@nure.ua

Abstract. *The services of the AWS cloud provider on information security are analyzed. The paper deals with a method of authentication of web application users using the AWS Cognito service. There is described the process of verifying access to a web resource.*

Keywords: *web application, authentication, cloud provider, AWS, Cognito, User pool, Identity pool.*

I. INTRODUCTION

At the current stage of the development of society, information is the most valuable product, one of the most important sources of the prosperity of any organization. Large-scale implementation of information technology requires considerable attention to security issues, as unauthorized leakage of information can lead to loss of market position and significant financial losses.

Nowadays, the science and technology direction has reached such a scale that any bank provides users with a mobile or web application for making payments, transfers via the Internet. This significantly increases the importance of information security when using these applications.

According to statistics, the process of user authentication is one of the most spread vulnerabilities. However, the danger of this threat may be reduced by using the AWS Cognito service - a way to restrict access for users.

Today, most of the world's leading companies specializing in commercial software development implement and recommend the services provided by AWS, as this cloud provider has passed a great number of security certifications. Therefore, the study and analysis of the capabilities of AWS services to ensure security in web applications is a topical subject.

II. AWS SECURITY SERVICES

In 2006, Amazon Web Services (AWS) began offering IT infrastructure services to businesses in the form of web services - the model known today as "cloud computing". Cloud computing is a model of delivering computing power, databases storage, applications, and other IT resources on request using the online platform of cloud services and charging upon consumption. The cloud services platform provides quick access to flexible and cost-effective IT resources for any purpose. Cloud safety is a top priority for AWS [3].

Today, Amazon Web Services provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that hundreds of thousands of enterprises in 190 countries around the world use in daily work.

AWS customers enjoy all the benefits of data centers and network architectures that have been developed for organizations with high-security requirements. One of the AWS cloud advantages is that you can scale your system and implement innovations while maintaining a high level of environmental security by paying only for the services use. This means that the required level of security can be provided at a lower cost than in the on-premises environment. Besides, AWS provides specialized tools and components with security features across network security, configuration management, access control, and data encryption.

Internet technologies are developing really fast and new web resources are appearing every day – so that this cloud platform provides a wide range of advanced technologies for their orchestration. In terms of security, AWS offers the following services: AWS Identity and Access Management (IAM), Amazon Inspector, AWS Certificate Manager (CM), AWS Web Application Firewall (WAF), AWS Cognito, AWS Secrets Manager, AWS Key Manager Service (KMS), AWS Shield. This is not a full list of services to be integrated with web resources.

To ensure sufficient stability of the application, it is suggested to use the next security technologies:

- IAM, allows you to control access to AWS services and resources. IAM provides the ability to create users and groups of users, manage them, and allow or restrict users and their groups access rights to a specific resource.
- AWS Certificate Manager (CM) is a new service that allows you to provision and deploy SSL and TLS certificates for AWS services and manage them. These certificates implement secure network exchange of information and are used to identify web applications over the Internet.
- AWS Key Manager Service (KMS) is a service that allows you to create and control encryption keys. KMS also provides logs of the key usage, ensuring compliance with regulations.
- AWS Web Application Firewall (WAF) is a firewall that helps protect web applications from common Internet threats that can affect availability and security.
- AWS Cognito is the service that provides the secure process of registration and logging in to a user account. It also allows you to integrate authentication using popular social networks - Facebook, Twitter, Amazon. One important point

is to ensure data synchronization between users' devices, thus avoiding application failures regardless of the device being used.

– AWS Shield is a service that provides protection against DDoS attacks on web applications running on AWS. AWS Shield ensures continuous detection and automatic inline neutralization of attacks, reducing application downtime and latency and getting rid of the need to engage AWS Support in case of DDoS attacks [1].

Having considered services to ensure the security of web applications, AWS Cognito should be highlighted, as this service makes the authentication process more reliable and secure.

This may be associated with, for example, scaling a simple database of user accounts, which small companies can deploy and manage personally. Problems with authentication may occur in the future when the number of users will increase to a hundred, a thousand, or even a million. Issues with the safety of user accounts most commonly arise at this stage. After all the authentication task becomes more complex since more complex identification methods, such as third-party social networks, are implemented [3].

To avoid possible vulnerabilities related to the user authentication process at any stage of web application development or maintenance, AWS offers to use the latest authorization system - Cognito.

III. . Solving a Problem Using Cognito

AWS Cognito consists of several functions for managing users, their sign-up, sign-in, and managing the account. This is a secure user directory that can expand with the development of needs and without having to configure any of the internal systems. In other management systems designed for user accounts, it is necessary to run a server and orchestrate IT infrastructure [2].

Cognito supports the use of third-party identity management providers. These include social networking platforms such as Facebook, well-known providers such as Google and Amazon, as well as enterprise-class identification data providers such as Microsoft Active Directory (using SAML, Security Assertion Markup Language) [1].

AWS Cognito uses well-known security providers such as Oauth 2.0 [4], SAML 2.0, and OpenID Connect. These are open-source providers that use standard-based authentication and access management services.

Figure 1 shows the way the AWS Cognito service works.

At the first stage of the service operating, the web application receives a token for user authentication. This JWT token carries important fields by which software developers can configure the access separation system by its own needs. Almost all data transmitted via such a token are configured on the service side when creating the Users Pool.

JWT Token is a conventional string encoded using the Base64 algorithm. It contains information about the user who made the request. According to the specification, the service returns three tokens: ID token, access token, refresh token. The ID token directly includes all the information on the account contained in the Amazon Cognito User Pool.

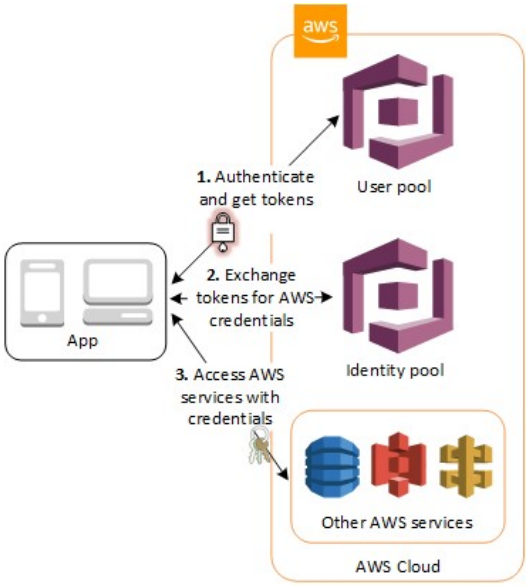

Figure 1. Scheme of operation of the AWS Cognito service

To correctly check the input token, first of all, you need to obtain a public RSA key, which will correspond to the field "kid", stored in the first part. Amazon Cognito generates a pair of RSA keys for each User Pool on its own. The private key of each pair is used to sign the corresponding ID or access token. The next step of validation is to check the lifetime, the "Exp" field. This is a time marker in seconds pointing to the expiry date. Also, if the software developer indicated some additional

data to the token, then on the side of the web application there is an opportunity to check them. For example, often a group or list of groups to which the user belongs is added to the token and it is the way the authorization is checked [3].

IV. Conclusions

The paper proposes a method of building a web application architecture using the AWS Cognito service, which provides efficient and reliable user authorization and authentication, with the latest cryptography technologies provided by AWS, shifting responsibility for scaling and delimiting access to the cloud provider.

REFERENCES

[1] AWS Documentation, Available at: https://docs.aws.amazon.com/ (accessed 02 April 2021)

[2] Amazon, Inc website, Available at: https://aws.amazon.com/ (accessed 05 April 2021)

[3] Kanikathottu H. Serverless Programming Cookbook, 2019. -C 482. ISBN 978-1-78862-379-7

[4] Власов, А.В., О.В. Сєвєрінов, and О.В. Слиш. Впровадження децентралізованої системи ідентифікації. НТУ «ХПІ», 2020.