University of Prince Mugrin

College of Computer and Cyber Sciences

Department of Software Engineering

SE495 - Cloud Computing & Security

Course Project – Semester I (Fall 2023 - 2024)

Team Members:

Salwa Shamma | 4010405

Samah Shamma | 4010403

Sana Shamma | 4010404

Instructor:

Dr. Ali Ahmed

December 21, 2023

Abstract

This report broadly reviews cloud computing literature in the context of cybersecurity. It also introduces several AWS security services, discussing their pros, cons, and potential use cases. Additionally, the report highlights some security best practices in the cloud.

Table of Contents

I. Literature Review of Cybersecurity in Cloud Computing 4

A. Cybersecurity in the AWS Cloud 4

B. Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network 4

II. Analysis of AWS Security Services 5

III. Best Security Practices in The Cloud 8

IV. Conclusion 10

I. Literature Review of Cybersecurity in Cloud Computing

This section summarizes key literature reviews that played a vital role in shaping the project. Two important reviews focused on the latest trends in cloud security were examined. These academic papers carefully explore the current state of cloud security, offering insights into pros, cons, use cases, and outlines some best practices to achieve security in the cloud. By incorporating the findings from these reviews, the project gains a strong foundation based on the latest developments and diverse perspectives in cloud security.

A. Cybersecurity in the AWS Cloud

This paper reassesses the standard content in advanced Cybersecurity courses, focusing on core concepts within the AWS Cloud environment. It covers an Approaches to Cybersecurity, Objectives of Cybersecurity, Basic Attack Examples, and Cryptography, with a special emphasis on Symmetric encryption. The paper also explores AWS best practices in Cybersecurity, aiming to align foundational principles with contemporary cloud computing paradigms. The paper aims to bridge theoretical Cybersecurity knowledge with practical applications in cloud-based systems, emphasizing the evolving landscape of information security.

B. Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network

This paper presented an AWS-based (Amazon Web Services) security architectural configuration technique that can be utilised throughout the complete life cycle (design, implementation, and operation) of cloud services for improved security in AWS Cloud Services, the world's most popular cloud service. The suggested AWS security guide for a secure social network includes five sections: Security Solution Selection Guide, Personal Information Safeguard Guide, Security Architecture Design Guide, Security Configuration Guide, and Operational Security Checklist.

The AWS Security Architecture was designed with three reference models in mind: Standard Security Architecture, Basic Security Architecture, and Essential Security Architecture. The AWS Security Guide and AWS Security Architecture suggested in this article are anticipated to assist many enterprises and institutions in establishing and operating a safe and dependable AWS cloud system in the social network environment.

II. Analysis of AWS Security Services

This section of the report will highlight some security services available through AWS, namely Network Access Control Lists (NACLs), and AWS Key Management Service (KMS). It will discuss their pros and cons and attempt to relate them to the literature reviewed in the previous section and the knowledge acquired from this course on cloud and security. Additionally, potential use cases for these services will be mentioned.

In terms of network security, one security solution is to use a firewall. A firewall refers to a network security measure that filters and controls incoming and outgoing network traffic based on predefined rules. In the context of AWS, there are two types of firewalls: Network Access Control Lists (NACLs) and Security Groups (SGs). In this discussion, we will focus on Network Access Control Lists (NACLs).

NACLs are stateless firewalls that operate at the subnet level. They allow you to define rules that control inbound and outbound traffic based on IP addresses, protocols, and ports. NACLs provide fine-grained control over network traffic, enabling you to allow or deny traffic based on source/destination IP addresses, protocols, and ports. Furthermore, they offer flexibility, allowing you to enforce different security policies for different subnets based on their requirements. However, NACLs have a few limitations. Firstly, they are stateless, which means you need to maintain separate rules for inbound and outbound traffic, resulting in increased difficulty in management. Secondly, if the rules are not properly ordered, it can lead to unintended consequences. NACLs evaluate rules based on their order, so if a rule allows or denies traffic, subsequent rules may not be evaluated. Additionally, NACLs have a maximum limit on the number of rules that can be applied, as AWS imposes a restriction on the number of rules that can be added to a NACL [1]. In summary, the table below summarizes the advantages and disadvantages of NACLs:

Advantages	Disadvantages
Fine-grained control over network traffic.	Stateless nature requires separate rules for inbound and outbound traffic.
Flexibility to enforce different security policies for different subnets.	Improper rule ordering can lead to unintended consequences.
	Maximum limit on the number of rules that can be applied.

Table 1 – advantage and disadvantages of NACL

One use case of NACLs is in a multi-tier web application deployed on Amazon Web Services (AWS). The application consists of a web server, an application server, and a database tier. Each tier is deployed in a separate subnet within an Amazon Virtual Private Cloud (VPC). To protect the web server, we can create a NACL for the web subnet that allows inbound HTTP and HTTPS traffic (ports 80 and 443) from the internet, while limiting outbound traffic to specific destinations. For the application server subnet, we can configure a NACL that allows inbound traffic only from trusted sources, such as the web servers. Similarly, for the database subnet, we can set up a NACL that allows inbound traffic only from the application servers and denies all other inbound connections. By implementing these NACLs, we add an additional layer of security. As shown in Figure 1, we can add NACL in each tier of the system and apply the pervious configurations.

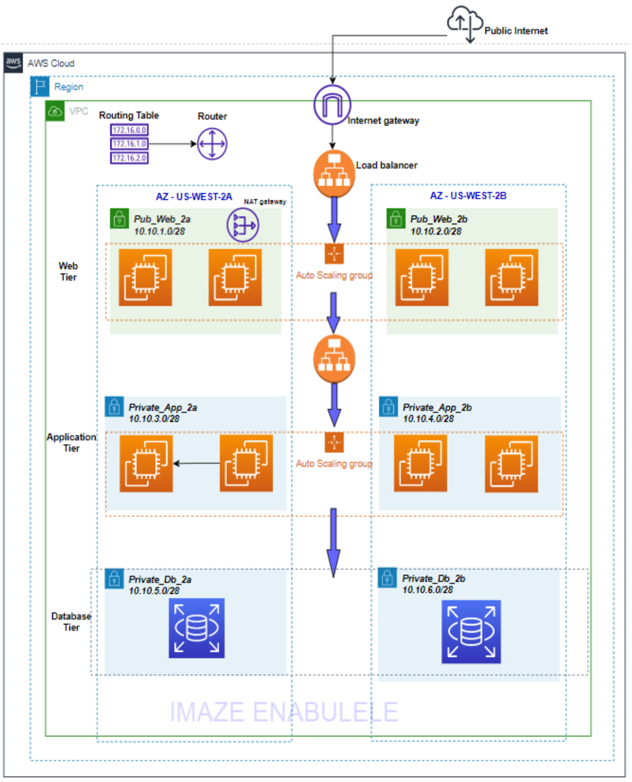

Figure 1- Multi-tier Web Application [2]

In terms of security in the area of DB/storage, one approach is to utilize data encryption using AWS Key Management Service (KMS). Data encryption involves converting plain, readable data into an unreadable format called ciphertext, using an encryption algorithm. This process ensures that sensitive data remains confidential even if it is accessed by unauthorized parties. Within the context of AWS, Key Management Service (KMS) is a managed service that assists in creating and managing encryption keys. KMS can be employed to apply block encryption, which safeguards data at rest.

Before delving deeper, let's introduce some terms. Block encryption entails encrypting entire blocks of data, such as files or disk volumes, using an encryption key. KMS provides a secure and centralized way to generate, store, and manage encryption keys for this purpose. On the other hand, field encryption refers to a more granular approach where specific fields within a dataset or database are individually encrypted. Instead of encrypting entire blocks of data, only specific fields containing sensitive information, such as credit card numbers or social security numbers, are encrypted. This approach enables more targeted protection of sensitive data elements while leaving other non-sensitive fields in plaintext.

KMS offers strong encryption and security controls to safeguard keys and data. It is designed to meet various compliance requirements, including PCI DSS, HIPAA, and GDPR. However, there are some limitations. KMS provides a predefined set of cryptographic operations and algorithms. It may lack the same level of flexibility and customization as building your own key management solution. If you have specific cryptographic or key management requirements, you may need to explore alternative solutions. Additionally, while AWS KMS provides robust encryption capabilities at the block level, implementing field-level encryption may require additional steps using third-party encryption solutions. This approach ensures specific fields are encrypted before being stored in the database, offering an added level of security for sensitive data elements which might be considered from a third-party review perspective [1].

In summary, the table below presents the advantages and disadvantages of Key Management Service (KMS):

Advantages	Disadvantages
Compliance with various regulations (e.g., PCI DSS)	Limited customization compared to building a custom key management solution.
Strong encryption and security controls.	May require additional steps for field-level encryption using third-party solutions or custom development within the app.

Table 2 – advantage and disadvantages of KMS

Let's consider a scenario where a .NET application processes sensitive user data. To ensure data confidentiality, the application integrates AWS Key Management Service (KMS). Using KMS, the application generates a customer master key (CMK) and requests KMS to generate a data encryption key (DEK) for encrypting the user data. The DEK is encrypted with the CMK and securely stored within KMS. The application employs .NET cryptographic algorithms to encrypt the data using the DEK. The encrypted data is stored at rest and transmitted securely over HTTPS. When accessing the data, the application sends a request to KMS to decrypt the DEK, retrieves it, and employs it to decrypt the data. This process shows in Figure 2.

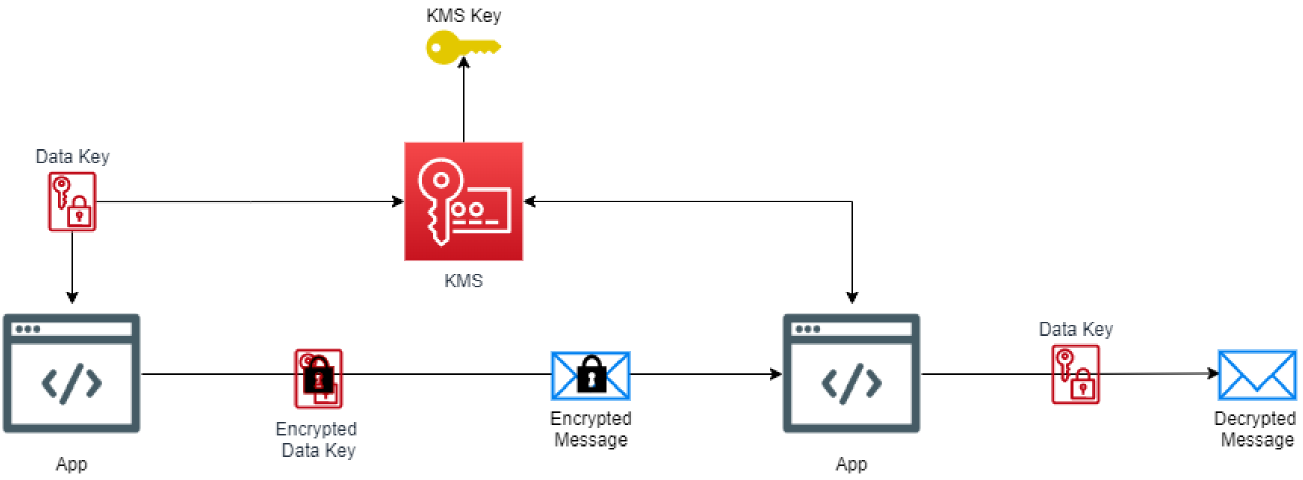

Figure 2- Encrypting Data in .NET apps Using AWS KMS [2]

III. Best Security Practices in The Cloud

Typically, cloud service providers offer a range of services designed to assist both themselves and their customers in meeting the three core principles of information security: Confidentiality, Integrity, and Availability (CIA). These principles are addressed by the 'three As' techniques, which refer to Authentication, Authorization, and Accounting as protection pillars. However, before delving deeper into how these pillars are achieved in the cloud and what cloud providers typically do to meet them, it's crucial to highlight that whatever they did, do, or will do, there is no perfect security system ever!

The three As pillars will be discussed in more breadth and depth:

Starting with authentication, the primary goal is to validate that the entities accessing the services are who they claim to be. A typical example of authentication checking, not limited to the cloud scope, is the username/password pair login. However, for any traditional system, these credentials could be subject to various risks, including legitimate ownership, stealing, guessing, or even generation through brute-force search, especially if the credentials are simple and short strings.

In the cloud, cloud providers privilege and mitigate these risks by offering best practices and services, which are often available at no cost. It becomes the customer's responsibility to activate these services. An example of such a service is the Identity and Access Management (IAM) service provided by AWS. IAM is designed to address authentication challenges mentioned earlier. Firstly, regarding credential theft, IAM employs encryption protocols (e.g., SSL/TLS) for transmitting usernames and passwords over the network, as well as encrypting stored data in databases. So, there's no need to worry more about credential theft.

In cases where credentials are stolen, AWS introduces an additional defense layer through Multi-Factor Authentication (MFA), requiring a second factor for access. Regarding password guessing, the cloud provides the ability to enforce constraints on passwords, such as minimum length and special characteristics, making it difficult to guess. Even if a password is compromised, MFA prevents unauthorized access through the guessing of passwords alone. These powerful features are just a click away for customers.

IAM also offers protection against brute-force attacks by automatically locking an account after a certain number of failed logins. In general, best practices in this pillar, when using cloud services, involve activating both IAM and MFA features.

Authorization, as the secondary aspect, involves determining the actions that the entity—whether it's a human user or a machine process—is allowed to perform. This is typically achieved through policies, which are documents that define which resources can be accessed and at what level. The golden rule here is applying the least privilege principle, advocating giving the minimal number of permissions required to get the job done. AWS and other cloud service providers comply with this principle by setting deny roles to as default settings to most services. Then, the customer's responsibility comes into play, requiring them to grant the minimal permissions necessary for entities to accomplish the task. By the way, this principle is embedded in IAM for the entity as well.

By activating IAM, you gain two benefits: authentication and authorization. Additionally, Security Groups act like firewalls, allowing the filtering of network traffic to the instance. Access Control Lists (ACLs) are assigned at the most abstract level—the subnet level—enhancing the layer of defense by applying the defense-in-depth principle. In summary, the best practice to achieve security in the cloud also involves using IAM groups and IAM policies to implement the least privilege principle. Furthermore, Security Groups and ACLs contribute to the defense-in-depth strategy.

Thirdly, accounting involves keeping record logs of what happens inside your cloud, alerting, and auditing actions. AWS provides many services to achieve that, such as CloudTrail, which traces all API calls and records them. The same applies to CloudWatch, a minor service that monitors service usage and captures unusual behavior. Customers can take advantage of these services, recording and setting actions to trigger according to their needs by using Lambda functions. In any case, CloudTrail and CloudWatch are widely used in AWS for better security.

In general, there are other services that help achieve security, even if they may not be considered at the core of cryptographic applications, such as load balancing. However, it is still considered good security practice when configured correctly. For instance, it can be a good defense against Distributed Denial of Service (DDoS) attacks by distributing traffic across multiple servers, making the DDoS attack harder to execute. Additionally, it has features to identify and block suspicious IP addresses. As a result, the system remains available and is not the target of the attack. Route 53 can play a similar role, providing DDoS protection. Therefore, Route 53 and load balancing can be added to the security services toolkit.

Also, we will add another important service that can enhance security in an implicit way, which is Technical Support service. This service provides you with expertise and knowledge for your security concerns.

As seen above, the context of the AWS Shared Responsibility Model is applied, where AWS is responsible for protecting its global infrastructure (security of the cloud), and customers are responsible for securing the resources they create (security in the cloud). Additionally, the mentioned services and best practices cover a wide range of common cloud services, including storage, networking, and computing [1].

IV. Conclusion

In conclusion, this project has undergone a comprehensive examination in two literature reviews: 'Cybersecurity in the AWS Cloud' and 'Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network.' The analysis covered both depth and breadth. The following services Network Access Control Lists (NACLs) and AWS Key Management Service (KMS) are analyzed extensively, covering both their pros, cons, and use cases. Finally, the report outlines some best practices to achieve security in the cloud. These practices include using IAM, MFA, Security Groups, Policies, ACLs, CloudWatch, CloudTrail, in addition to configuring both Route 53 and Load Balancer for enhanced security. Seeking Technical Support services for advice on cloud security is also recommended.

References

[1] Park, S.-J., Lee, Y.-J. and Park, W.-H. (2022) *Configuration method of AWS Security Architecture that is applicable to the cloud lifecycle for Sustainable Social Network*, *Security and Communication Networks*. Available at: https://www.hindawi.com/journals/scn/2022/3686423/ (Accessed: 21 December 2023).

[2] Enabulele, I. (2022) *Creation of a highly available 3 tier architecture*, *Medium*. Available at: https://aws.plainenglish.io/creation-of-a-highly-available-3-tier-architecture-30b2be0a871e (Accessed: 21 December 2023).

[3] .NET, P. byAWS with (2022) *Encrypting data in .net apps using AWS Key Management Service*, *AWS with .NET*. Available at: https://awswith.net/2022/01/01/encrypting-data-in-net-apps-using-aws-key-management-service/ (Accessed: 21 December 2023).

[4] M. Soltys, “Cybersecurity in the AWS Cloud,” Apr. 31, 2020.