ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/binoy-revi/527

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 2

Research Article

Cloud Security: Application Security and Data Encryption

Binoy Kurikaparambil Revi*

Citation: Revi BK. Cloud Security: Application Security and Data Encryption. *J Artif Intell Mach Learn & Data Sci 2023*, 1(2), 2454-2457. DOI: doi.org/10.51219/JAIMLD/binoy-revi/527

Received: 01 April, 2023; **Accepted:** 28 April, 2023; **Published:** 01 May, 2023

***Corresponding author:** Binoy Kurikaparambil Revi, Independent Researcher, USA, E-mail: binoyrevi@live.com

ABSTRACT

In today's world, most applications are deployed and maintained in the cloud rather than on-premises. This transformation is driven by benefits such as reduced capital costs, improved security and greater scalability. As applications transition to the cloud, it's crucial to define application security from a network perspective. This is important because certain application components have to be accessible from the internet, while others may be restricted and only accessible by components within the same application. Most major cloud providers offer tools and services to support application security implementation. This paper focuses on the impact of application security on data encryption using Microsoft Azure as the cloud service provider. The key network security services include Virtual Network (VNet), Subnet, Network Security Group (NSG) and Application Security Group (ASG). Designing the infrastructure for an application with a security-oriented mindset is essential for ensuring overall application security. Simultaneously, effectively handling data encryption within the network groups plays a crucial role in safeguarding data security.

Keywords: Cloud Security, Data Encryption, Virtual Network, Cloud Apps

1. Introduction

In the beginning, cloud service providers needed a way to group a set of IP addresses belonging to one organization and isolate them from the resources of other organizations within the same data center. This need led to the creation of Virtual Networks (VNets). VNets isolate an organization's resources to ensure they are separate from others in the same data center.

As applications became more complex and data security concerns grew, an enhancement to the VNet became inevitable. Initially, there were two main scenarios:

- Application resources that needed to be accessed externally
- Application resources that should remain inaccessible from external sources.

To address this, the concept of subnets was introduced. In a VNet, resources that require external access are grouped into one subnet, allowing external entities to reach them. Conversely, resources that should not be accessed from outside are placed in a different subnet. This second subnet can only be accessed by resources within the first subnet, preventing any external applications or systems from gaining access. This approach functions effectively to a certain degree. A prime example of effective network organization is the separation of database servers and business logic applications into their own subnet, which remains inaccessible to external sources. In contrast, the web applications that must be accessible to users outside the network are placed in a separate subnet. This separation helps illustrate the overall structure of this simple application, as shown in **(Figure 1)**.

Fitting data security modules that handle the encryption and decryption of data for storage or transmission is crucial for safeguarding that data. In the simple application described in Figure 1, the data security modules or applications should not be placed in the web application subnet, as it is accessible to external entities. While it may be somewhat safer to position

them in the business logic application subnet, the most secure location would likely be in the database server subnet or in an additional subnet positioned between the business logic subnet and the database subnet.

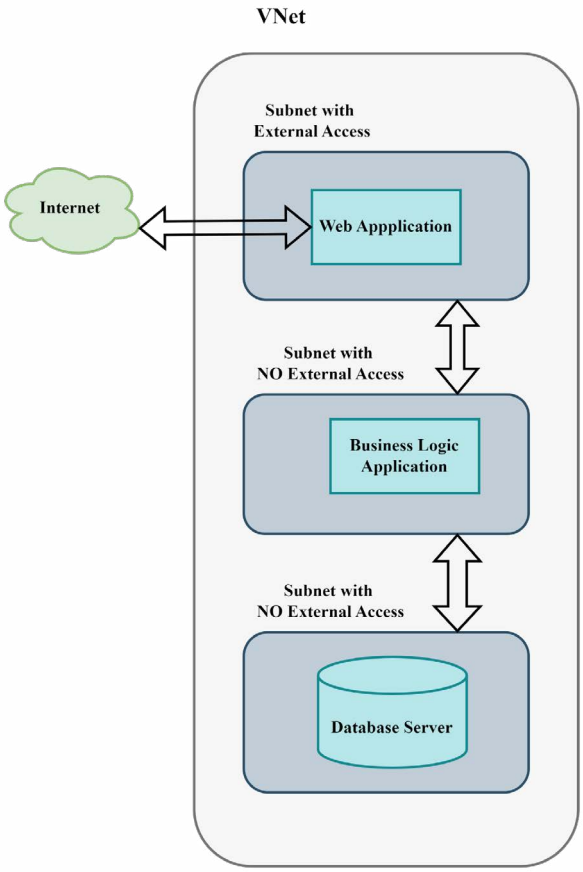

Figure 1: A Simple Application on V-Net.

2. Related Work

Rui Zhang and Ling Liu have conducted impressive research in their paper titled "Security Models and Requirements for Healthcare Application Clouds."[1] This paper outlines a comprehensive approach to data security and management. It emphasizes the importance of ownership, authenticity, authentication, integrity, confidentiality and the availability of data when handling sensitive information. Additionally, the paper highlights that data management is user-driven and user-centric, meaning that applications accessed by specific users, in this case, patients, can only access unencrypted data.

Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire and Pedro R. M. Inácio conducted an important study on evaluating security issues in various cloud environments.

A significant contribution to cloud computing security comes from Mazhar Ali, Samee U. Khan and Athanasios V. Vasilakos. In their article "Security in Cloud Computing: Opportunities and Challenges," they discuss the architectural framework of cloud computing and the security challenges that accompany it. They also describe V-Net and the issue of misconfiguration, which is an area of particular interest.

3. Problem Description

As the number of application and database servers within each subnet continues to grow, the task of managing the mapping of these applications becomes increasingly challenging. This escalating complexity often paves the way for human errors, which can trigger severe security vulnerabilities with heavy consequences. Moreover, the process of implementing specific rules and configurations for each individual application and database server can turn into a tedious and error-prone undertaking. The prospect of scaling and efficiently managing such a system loom dauntingly for administrators, leading to potential operational nightmares and increased risk of misconfiguration and cyber security. In real-world applications, there are scenarios where applications within the same virtual network (v-net) must not be allowed to access one another, especially when it comes to sensitive resources like databases. For instance, as illustrated in **(Figure 1)**, it is logical and safe to ensure that the subnet for a web application does not have access to the subnet for a database application. Such requirements can complicate infrastructure implementation, particularly when relying solely on v-nets and subnets to create an infrastructure for a large number of applications. When we consider the encryption and decryption of data for storage in a database or for sending it back as a response from a web application, the process becomes even more complicated. This complexity in managing security rules arises for applications that perform encryption and decryption[2]. Often, relying solely on virtual networks (v-nets) and subnets makes this management very challenging.

4. Solving Subnet Overcrowding Problem Using NSG and ASG

When the system has several applications, services and database servers running on the cloud, managing the security rules for these applications can be simplified by using the Network Security Group (NSG) and Application Security Group (ASG). This basically solves 2 different problems.

- To efficiently apply uniform security rules across multiple applications, you can utilize a Network Security Group (NSG). An NSG is a powerful tool that enables you to establish a set of security rules detailing which subnet addresses are granted access to the applications hosted within that particular subnet. These rules serve as a gatekeeper, defining inbound and outbound traffic permissions to safeguard your resources. It's crucial to understand that the security rules associated with an NSG are comprehensive; they govern all applications as well as every resource within the subnet linked to the NSG. This centralized management not only simplifies the enforcement of security policies but also enhances the overall security maintenance of your network infrastructure.
- What if we want certain applications within a subnet to restrict access to other applications in the same subnet? This concept is best illustrated by examining the simple application shown in Figure 1. In a different scenario, we can consider having both a web application and a business logic application located in the same subnet and we need to prevent external applications from accessing the business logic application. Relying solely on a Network Security Group (NSG) won't be sufficient to achieve this. This is where Application Security Groups can help. Application security groups can group a set of applications in one subnet and define security rules for that application group alone.

In real-world applications, a more effective cloud security

infrastructure is built by implementing both NSG and ASG together. **(Figure 2)** provides a simple security architecture model that shows how the NSG and ASG are configured.

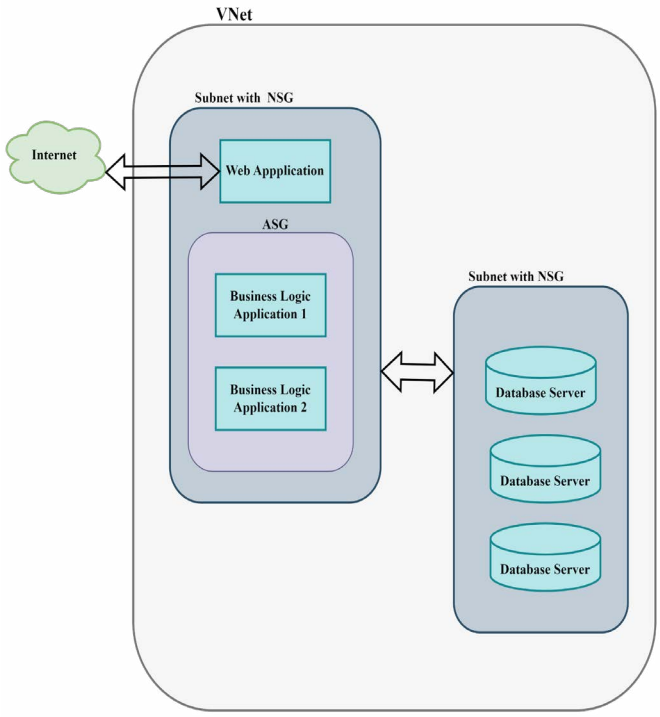

Figure 2: Cloud Security Architecture using NSG and ASG.

5. Embedding Data Encryption and Decryption Module in Cloud Security Architecture

This topic often sparks important discussions among the software standards, security module development and cloud infrastructure teams when designing the overall system architecture. It's essential to recognize that while each module design may be correct, but not addressing the appropriate integration of security modules during the design phase can result in vulnerabilities within the system.

Some of the basic rules that may be followed by the security module development team are given below:

- If data can be handled as encrypted while entering, storing and exiting the system, this should be the primary option. This means that the encrypted data is never decrypted and hence not exposed in any module or application in the system.
- For the purpose of encryption or decryption never store the private key in the application code or storage. Use the Key vault service to securely handle this[6].
- Rule of minimum required data - Provide only the minimum data that is requested by other applications.
- Always authenticate before responding with valid data for transactions.
- Avoid persistent connection with other applications.

The cloud infrastructure design for placing the security module must be made by understanding the dependency and functionality of the security module. Some basic rules that can be considered are the following:

- Access to the security application or security module is denied by default.
- Avoid having the security module in the same v-net as the web applications that have NSG exposing the network to the internet.
- 2-Steps below rule: Cloud infrastructure offers better security when security modules are located in a subnet that has at least one non-exposed subnet between the subnet allowing external connections and the subnet where the security modules reside.
- Minimum and non-persistent access: Infrastructure should provide access to the application when necessary and must timeout once the job is completed.

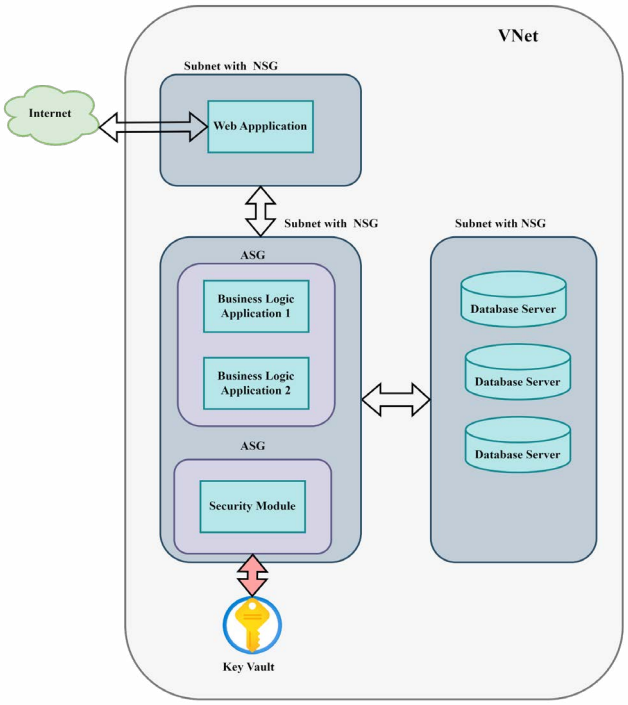

Figure 3: Cloud Infrastructure Design with Security Module.

Figure 3 illustrates a typical cloud security design that incorporates the security module. An important aspect to note is that the security module is placed in its own ASG and is isolated from the web application. Additionally, the security module utilizes a key vault for managing its secrets.

6. Conclusion

Cloud infrastructure provides an excellent platform for deploying applications, allowing for scalable resources based on demand while ensuring high availability without significant capital investment. However, it is crucial to understand the security tools, packages and principles necessary for designing a secure application.

A Virtual Network (VNet) is the first line of defense in controlling traffic to an application. Analyzing and discussing this topic revealed that subnets facilitate the grouping of applications, while Application Security Groups (ASG) and Network Security Groups (NSG) are essential tools for managing access to a large number of applications as an application group or as a subnet itself. NSGs define the security rules for all applications within a subnet, while ASGs take it a step further by allowing the grouping of related applications within the same subnet.

When adding security modules that perform encryption and decryption functions, it is important to ensure that this application is included in the correct subnet with NSG/ASG.

7. References

1. Zhang R and Liu L. Security Models and Requirements for Healthcare Application Clouds, 2010 IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 2010: 268-275.
2. https://link.springer.com/article/10.1007/s10207-013-0208-7
3. https://www.sciencedirect.com/science/article/abs/pii/S0020025515000638?via%3Dihub
4. https://www.mdpi.com/2073-431X/3/1/1
5. https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5
6. Gai K, Qiu M and Zhao H. Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing, in IEEE Transactions on Big Data, 2021;7: 678-688.
7. Yang P, Xiong N and Ren J. Data Security and Privacy Protection for Cloud Storage: A Survey, in IEEE Access, 2020;8: 131723-131740.