DOI: https://doi.org/10.5281/zenodo.12227563

ASSESSING THE RISKS AND CHALLENGES OF ON-PREMISES INFRASTRUCTURE

Istamov Mirjahan Muminjan
Tohirov Quvonchbek Musurmon o‘g‘li
Sultonov Hayotjon Baxodir o‘g ‘li
Student at the Tashkent University of Information Technologies named after Mukhammad al-Kharezmy

Abstract: *Delving into cloud security intricacies, it emphasizes the importance of transitioning to cloud environments for security. Scrutinizes the rationale behind cloud migration, highlighting security imperatives. Explores architecting secure solutions in AWS, discussing design considerations and implementing various AWS security services to fortify the infrastructure against potential threats.*

Key words: *Job Management, Economic Considerations, Resource Management and Efficiency.*

This multi-tier architecture leverages various AWS services to provide a scalable, secure, and efficient infrastructure. The use of public and private subnets ensures proper network segmentation, while security groups, IAM roles, and other security services protect resources from unauthorized access. Monitoring and logging services like CloudWatch and SNS ensure that the infrastructure remains reliable and performant, with prompt notifications in case of any issues. This design supports robust growth and enhances the overall security posture of the application. The use of managed services like Amazon RDS and Amazon S3 further simplifies infrastructure management and allows the team to focus on application development. Additionally, the incorporation of AWS Lambda and Amazon API Gateway enables a serverless approach, improving scalability and reducing operational overhead.

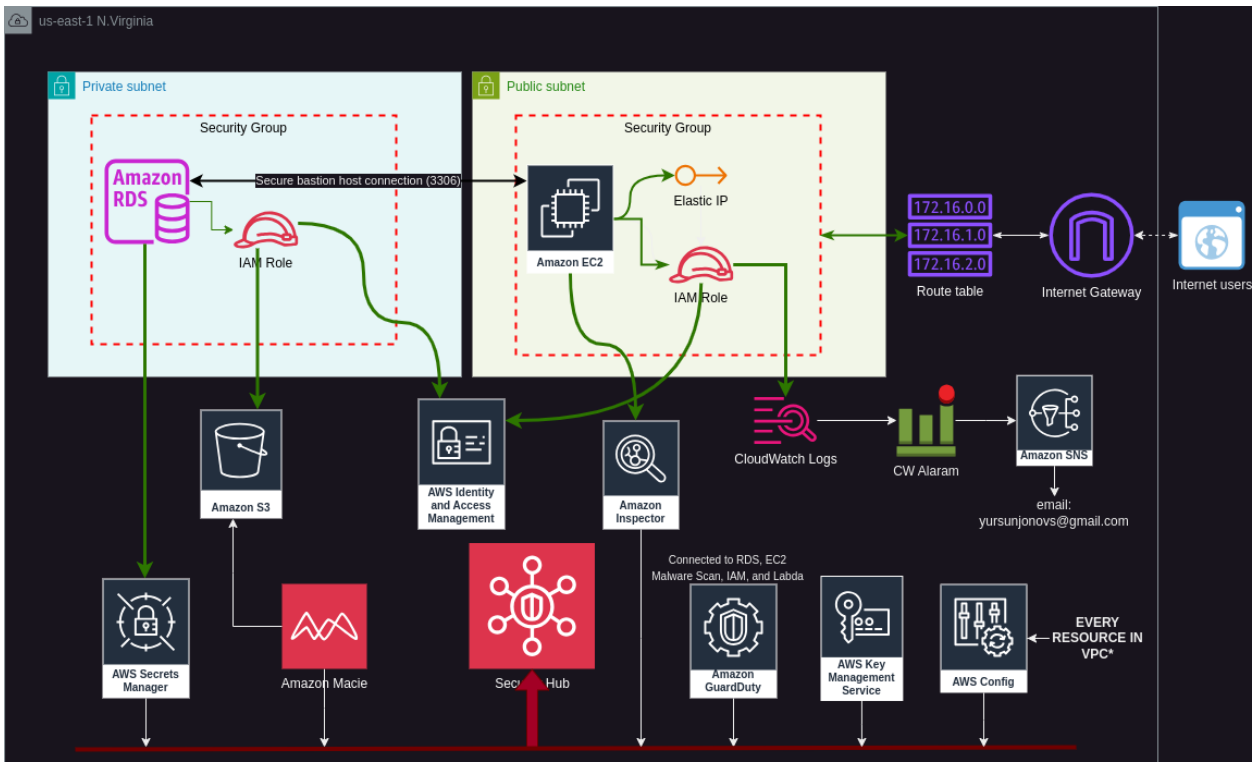

Fig 2.1. My project infrastructure illustration in draw.io

In this setup, the Virtual Private Cloud (VPC) is divided into public and private subnets to manage the network architecture effectively. The public subnet hosts an Amazon EC2 instance with an Elastic IP, making it publicly accessible and allowing internet access to its applications or services. In contrast, the private subnet houses an Amazon RDS database, which is shielded from direct internet access, enhancing security.

The network and security configuration includes several critical components. Security groups define inbound and outbound rules for EC2 and RDS instances, ensuring controlled communication. Route tables and an internet gateway manage routing and internet connectivity within the VPC. A secure bastion host facilitates secure access to the RDS instance over port 3306. Additionally, IAM roles are assigned to the EC2 and RDS instances, granting them permissions to interact securely with other AWS services.

Monitoring and logging are vital for maintaining infrastructure health and performance. CloudWatch Logs collect and monitor logs from EC2 and RDS instances, offering operational insights. CloudWatch Alarms trigger actions based on predefined metrics and thresholds, ensuring timely issue responses. Additionally, SNS (Simple Notification Service) sends notifications, including email alerts, when alarms are triggered, promptly informing administrators of critical events.

Data management and security are reinforced through various AWS services. AWS Secrets Manager securely manages secrets like database credentials, while Amazon S3 provides robust data storage integrated with security services. AWS Identity and Access Management (IAM) ensures that only authorized users and services can access sensitive data.

Several advanced security services further bolster security. Amazon Inspector identifies application vulnerabilities, and Amazon Macie protects sensitive data in Amazon S3. AWS Security Hub offers a comprehensive view of security alerts and compliance, while Amazon GuardDuty monitors for malicious activity. AWS Key Management Service (KMS) manages encryption keys to secure sensitive data, and AWS Config tracks configuration changes and compliance to maintain security posture and governance.

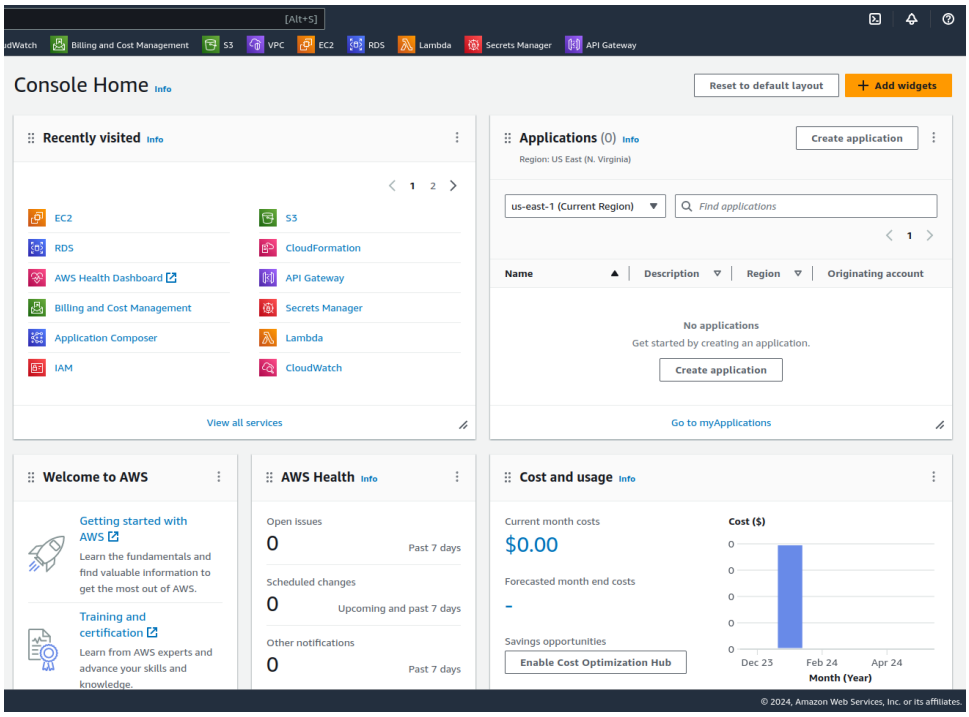

Fig 2.2. Management Dashboard

This screenshot depicts the AWS Management Console Home, providing a centralized interface for managing AWS resources. Key sections include "Recently visited" services like EC2, S3, RDS, and IAM, facilitating quick access. The "Applications" section in the US East (N. Virginia) region shows no current applications but offers options to create and manage applications. Additional panels display AWS Health with zero open issues or scheduled changes, and "Cost and usage," indicating no costs for the current month. The console also includes links to AWS documentation, training, certification, and cost optimization tools, supporting users in efficient AWS resource management.

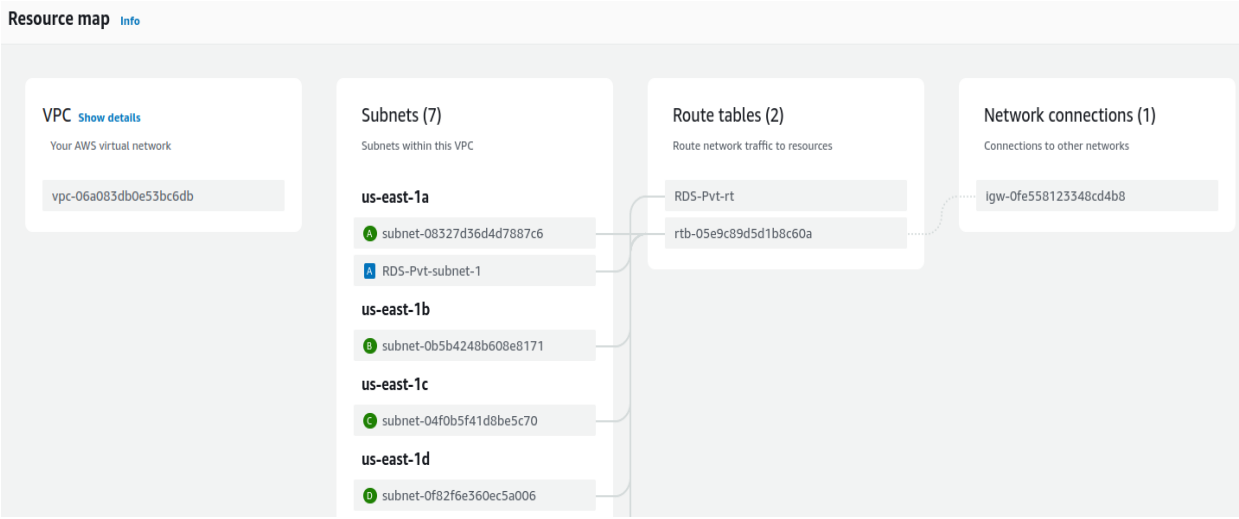

Fig 2.3. VPC resource mapping

This image displays the AWS Resource Map for a specific VPC configuration. The VPC (vpc-06a083db0e53bc6db) includes several subnets distributed across different availability zones (us-east-1a to us-east-1d), with one highlighted private subnet for RDS. Two route tables, "RDS-Pvt-rt" and "rtb-05e9cd95d1b8c60a," manage traffic within the VPC. Additionally, there's a network connection (lgw-0fe55812348cd4b8) facilitating connectivity to other networks. Security groups and IAM roles are configured to ensure secure communication and access control within the VPC. This map offers a clear visualization of the VPC's networking components and their interconnections, helping administrators understand and manage the network architecture efficiently. Moreover, the highlighted private subnet ensures the isolation and security of sensitive resources such as the RDS database, safeguarding it from external access. The best practice here is to deploy your EC2 web application in public subnet and RDS database in private subnet so that attackers cannot penetrate your database or make any direct attacks. It is also worth nothing about the usage of SQL ORM mode in code.

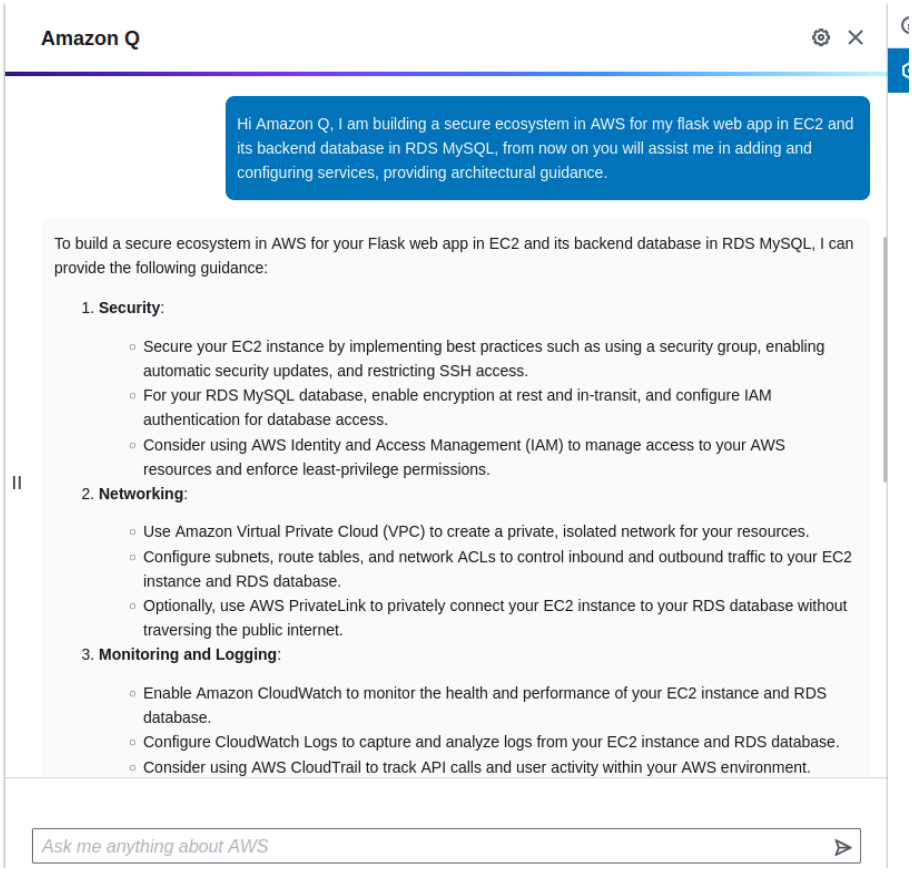

Fig 2.4. AI-powered chat in AWS console

Amazon Q is an AI-powered chat feature designed to enhance user interaction and support within the AWS Management Console. It provides a conversational interface where users can ask questions related to their AWS resources and receive instant, contextual responses.

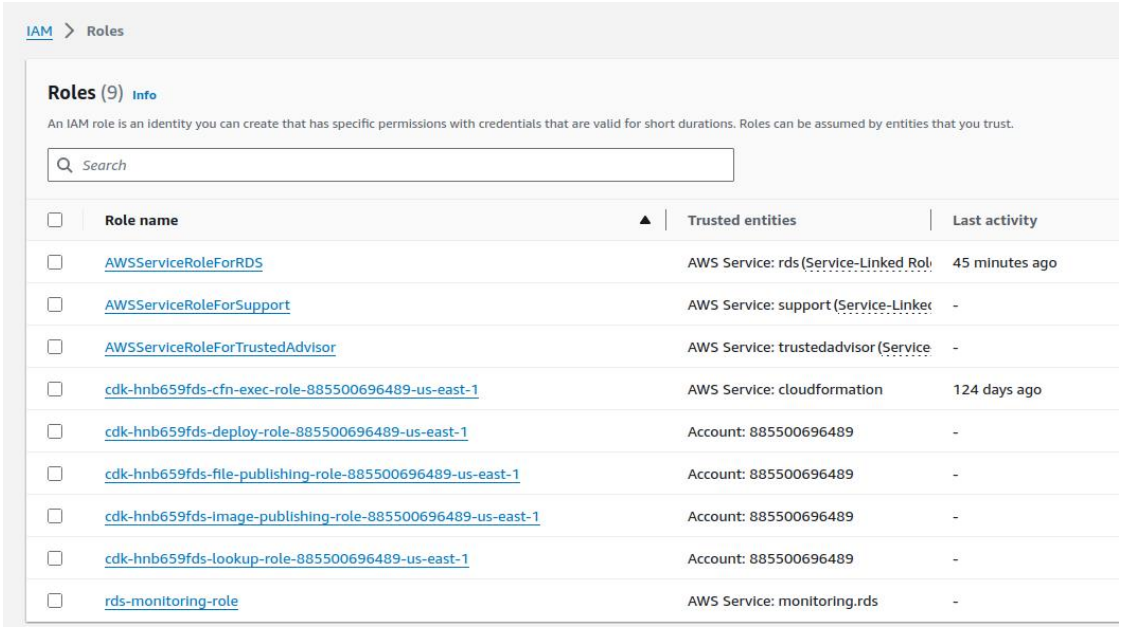

Fig 2.8. IAM roles list

The image shows a list of IAM (Identity and Access Management) roles associated with various AWS (Amazon Web Services) services. These roles provide specific permissions and credentials that are valid for short durations. The roles can be assumed by entities that the user trusts. The information displayed includes the role name, the trusted entities that can assume the role, and the last time the role was used. This allows the user to manage and monitor the usage of these roles within their AWS environment.

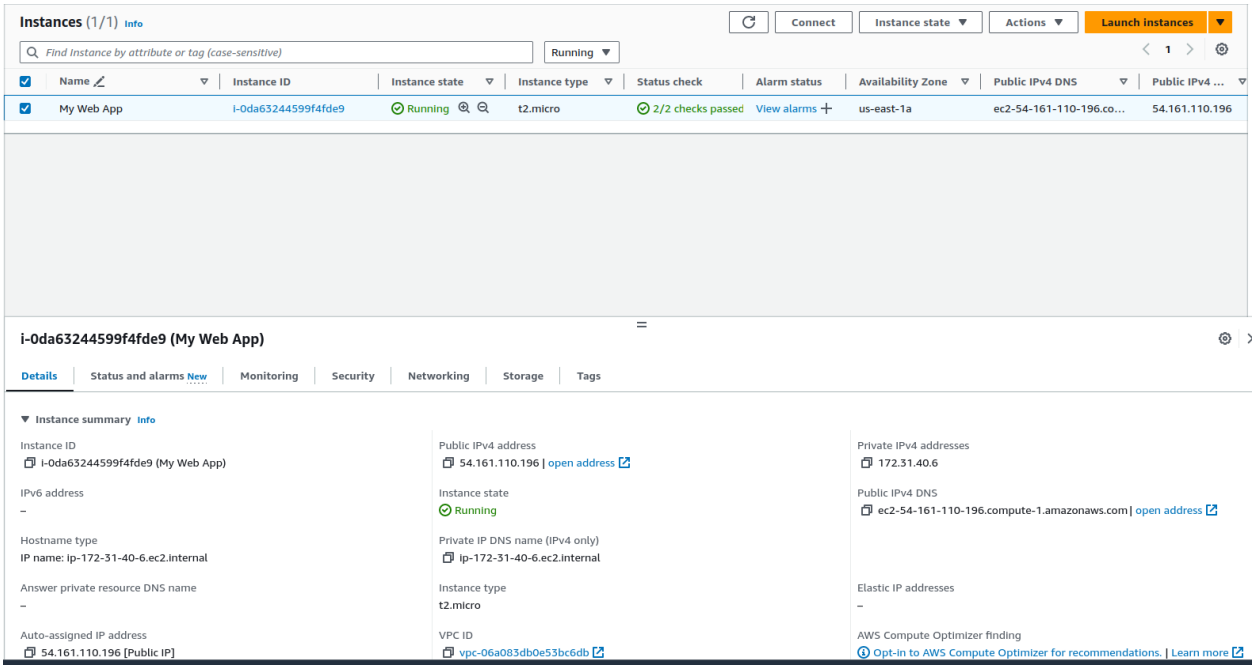

Fig 2.5. EC2 instance details

The image shows the details of an EC2 (Elastic Compute Cloud) instance named "My Web App" in an AWS (Amazon Web Services) environment. The key details provided are:

- Instance ID: i-0da632445994fd9e9
- Instance State: Running
- Instance Type: t2.micro
- Public IPv4 Address: 54.161.110.196
- Private IPv4 Address: 172.31.49.6.ec2.internal
- Hostname: ip-172-31-49-6.ec2.internal
- Auto-assigned IP address: 54.161.110.196 (Public IP)
- VPC ID: vpc-0b8b1bbcc3be6a16b
- AWS Compute Optimizer findings: Optimized for cost

This EC2 instance is part of the user's AWS environment and is currently in the

"Running" state, indicating that it is active and operational. The details provided cover various aspects of the instance, including its networking configuration, security, and optimization recommendations from the AWS Compute Optimizer.

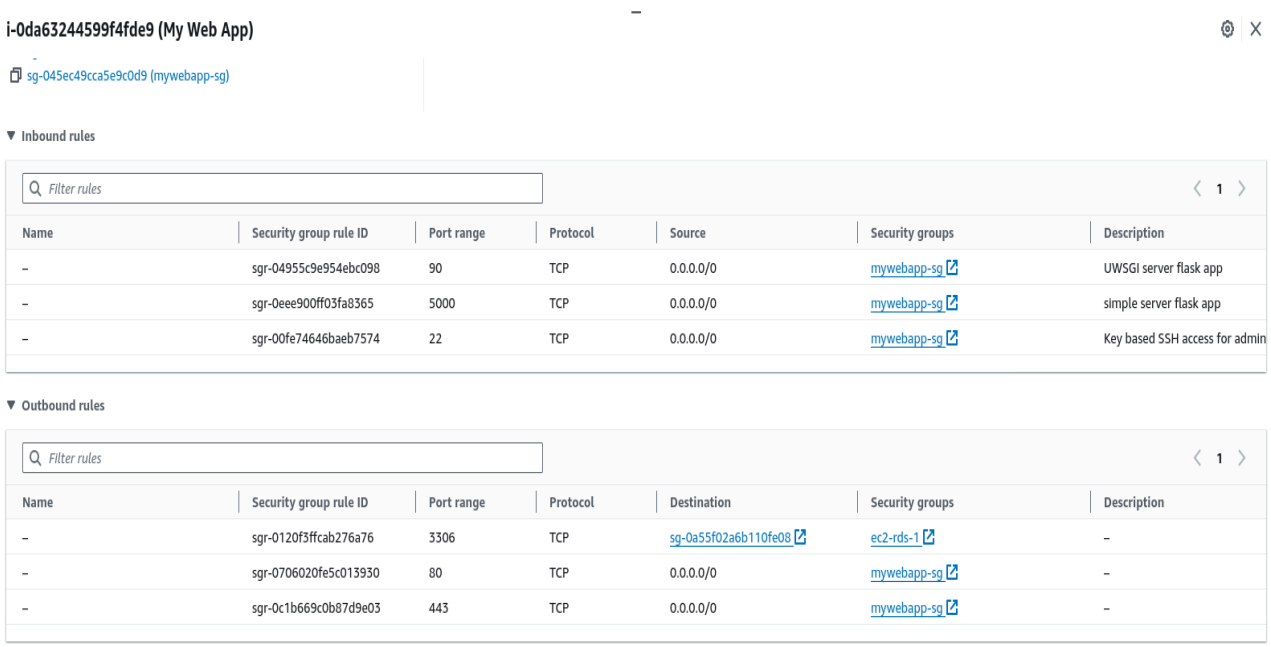

Fig 2.6. EC2 instance security group

The image shows the security settings and network rules configured for the EC2 instance named "My Web App". This includes both inbound rules, which control the traffic allowed to access the instance, and outbound rules, which control the traffic allowed to leave the instance.

Inbound rules:

➔ Allows TCP traffic on port 90 from the security group "sgr-049c5c6e954cb098"

➔ Allows TCP traffic on port 5000 from the security group "sgr-0bee0d01a1a3a3c9"

➔ Allows TCP traffic on port 22 from the security group "sgr-0be7464eb0eb7574"

Outbound rules:

➔ Allows TCP traffic on port 3306 to the security group "sg-0a55f0264eb110fe0"

➔ Allows TCP traffic on port 80 to the security group "mywebapp-sg"

➔ Allows TCP traffic on port 443 to the security group "mywebapp-sg"

CONCLUSION

The journey through this thesis has navigated the intricate landscape of cloud migration with a focus on security. We began by examining the risks and challenges of maintaining traditional on-premises infrastructure, identifying vulnerabilities such as physical security risks, scalability limitations, and high maintenance costs. This analysis highlighted the advantages of moving to a cloud-based infrastructure like AWS, which offers significant benefits in terms of scalability, cost efficiency, and security.

Amazon Web Services (AWS) was presented as a comprehensive suite of cloud services providing computational power, storage, and a range of tools designed to enhance security and scalability. By leveraging AWS, organizations can take advantage of economies of scale, cutting-edge technology, and a robust security framework that is continuously updated to counter emerging threats.

REFERENCES

1. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS) 1st Edition by Michael J. Kavis
2. Aws Solutions Architect Associate Sg (Aws Certified Solutions Architect Official: Associate Exam) Study Guide Edition by Joe Baro
3. https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html
4. https://aws.github.io/aws-security-services-best-practices/guides/security-hub/
5. An Analysis of Security Challenges in Cloud Computing, January 2013 International Journal of Advanced Computer Science and Applications 4(1) License CC BY 4.0 Ms. Disha H. Dr. R.
6. https://docs.aws.amazon.com/whitepapers/latest/best-practices-deploying-cliosoft-sos-on-aws/challenges-of-the-on-premises-environment.html
7. https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html