**Architecting a Scalable and Cost-Effective Web Application on AWS**

# CSA1579 – Cloud Computing and Big Data Analytics for

Healthcare Industries

**Submitted to**

SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES

**In partial fulfilment of the award of the degree of**

# BACHELOR OF ENGINEERING IN COMPUTER SCIENCE

**By**

**Ch.Bhanu Prakash (192211091)**

**Supervisor**

# DR. BALAMANIGANDAN



**SAVEETHA SCHOOL OF ENGINEERING**

**SIMATS CHENNAI- 602105**

**JUNE-2024**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| S.NO | Title | Page. No. |
| 1 | Problem statement | 3 |
| 2 | Requirements  Gathering | 3 |
| 3 | **Choose Cloud Provider Best Fits**  **Your Needs** | 3 |
| 4 | Develop FrontEnd and BackEnd | 4 |
| 5 | Implementation and Performance | 5 |
| 7 | Conclusion | 5 |

# Problem Statement

As remote work becomes increasingly prevalent, organizations need secure and reliable solutions to enable their distributed workforce to access internal resources. This project focuses on designing and implementing a Virtual Private Network (VPN) solution on the AWS Cloud to facilitate secure remote access for employees located across various geographical locations.

# Requirements Gathering

## Identifying the Specific Requirements

* **Comprehensive Needs Assessment**: Conduct a thorough assessment to understand the organization's requirements and challenges.
* **Stakeholder Input:** Identify key stakeholders and gather input regarding connectivity needs, security requirements, and user experience expectations.
* **Network Infrastructure Evaluation:** Evaluate the current network infrastructure and determine integration points.

## Determine the Necessary Features

* **Secure and Encrypted Access**: Ensure remote access to internal resources is secure and encrypted.
* **Scalability:** The solution must support a growing number of remote users.
* **Redundancy:** Ensure high availability and reliability.
* **Geographic Distribution:** Provide optimal connectivity for users in different locations.
* **Integration:** Integrate with existing network infrastructure and security protocols.

# Choose Cloud Provider Best Fits Your Needs

* **Cloud Provider Analysis**: Analyse different cloud providers (AWS, Azure, Google Cloud) based on scalability, security, compliance, and cost.
* **Justification for AWS:** Select AWS Cloud as the preferred provider due to its robust security features, extensive compliance certifications, and comprehensive suite of networking services.

# Develop Frontend

## Layout

* **Intuitive Design:** Design an intuitive and user-friendly interface for VPN management.
* **Easy Navigation:** Ensure the layout facilitates easy navigation and quick access to essential features. **User-Friendly**
* **User-Friendly Elements:** Implement elements such as clear instructions, helpful tooltips, and responsive design to enhance the user experience.

## Colour Selection

 **Brand Alignment:** Choose a color scheme that aligns with the organization's branding and provides good visual contrast for accessibility.

# Develop Backend

## Database Implementation

* **Database Setup:** Set up a database to store user credentials, connection logs, and configuration settings.
* **Security and Optimization:** Ensure the database is secure, scalable, and optimized for performance. **Execution**
* **Backend Services:** Develop backend services to handle user authentication, VPN session management, and logging.
* **API Implementation:** Implement APIs for frontend-backend communication.

# Implementation and Integrate with Cloud Services

## Implementation

* **AWS VPN Gateway Configuration:** Configure AWS VPN Gateway to establish secure connections between remote users and the organization's AWS Virtual Private Cloud (VPC).
* **Encryption and Authentication:** Implement appropriate encryption and authentication mechanisms to ensure data confidentiality and integrity. **Cloud Integration and Deployment**
* **Service Integration:** Integrate the VPN solution with AWS services such as IAM for user management and CloudWatch for monitoring.
* **Deployment:** Deploy the solution on the AWS Cloud and ensure it is properly configured for high availability and scalability.

## Testing

* **Thorough Testing:** Conduct thorough testing to identify and fix any issues.
* **Security Testing:** Perform security testing to ensure the solution meets all security requirements and standards.

# Performance Evaluation

* **Performance Criteria:** Evaluate the performance of the VPN solution based on criteria such as connection speed, reliability, security, and user satisfaction.
* **User Feedback:** Collect feedback from users and make necessary improvements.

# Conclusion

* **Summary of Achievements:** Summarize the key achievements of the project.
* **Benefits:** Highlight the benefits of the implemented VPN solution for the organization's distributed workforce.
* **Future Enhancements:** Provide recommendations for future enhancements.