TAMILNADU SKILL DEVELOPMENT CORPORATION

Naan Mudhalvan Niral Thiruvizha

Declaration Form

1. Name of the College: Theni Kammavar Sangam College of Technology

2. College code: 9222

3. Theme: Smart Manufacturing

4. Problem statement: Develop robust cybersecurity measures in safeguarding sensitive data in IIoT systems, ensuring secure data transmission, addressing threats, and implementing stringent access controls.

5. Faculty Guide Details: Dr.M.Rajashanthi (AP/CSE)

Team Leader Name	Reg.No	Year	Department	Mobile No
1. M.K Charu Prakash	922220104303	IV	CSE	9092917762
Team members				
1. S. Mohamed Faisal	922220104021	IV	CSE	6383094437
2. M. Ragul Prasath	922220104315	IV	CSE	9080449976
3. R. Thirumalai Raj	922220104318	IV	CSE	9600317311

6.Detailed Work Plan from 12th March-2024 to 30th May-2024

Strengthening IIOT Cybersecurity through SSH and VPN integration

Phase 1: Preparation (March 12th - March 25th)

Project Kick-off and AWS Account Setup:

- Hold a kick-off meeting to introduce team members, define objectives, and set expectations.
- Set up an AWS account and configure IAM roles for team members with appropriate permissions.

Requirement Gathering and Analysis:

- Gather requirements for SSH and VPN integration, including the need for a physical router to establish VPN connections between AWS and on-premises networks.
- Risk Assessment and Compliance:
- Perform a risk assessment considering physical router deployment, ensuring compliance with security standards and regulations.

Resource Allocation and Budget Planning:

- Allocate resources and budget for the physical router procurement, installation, and configuration.

Phase 2: Planning (March 26th - April 8th)

Solution Design and Router Selection:

- Design the architecture for integrating the physical router with AWS VPCs for VPN connectivity.
- Select a physical router model that supports VPN protocols compatible with AWS VPN services.

Procurement:

- Procure the selected physical router model from a trusted vendor or supplier.

Timeline and Milestone Definition:

- Define a timeline with milestones for each phase of the project, considering router procurement, installation, and configuration.

Phase 3: Implementation (April 9th - May 10th)

Physical Router Installation:

- Install the physical router in the on-premises network infrastructure, ensuring compatibility and proper placement for VPN connectivity with AWS.

Router Configuration:

- Configure the physical router to establish VPN connections with AWS VPN services, including setting up VPN parameters, encryption settings, and authentication methods.
- Configure routing policies on the router to direct traffic between on-premises networks and AWS VPCs through the VPN tunnel.

Integration with AWS:

- Configure AWS VPN services (e.g., AWS VPN Gateway) to establish VPN connections with the physical router.
- Verify VPN connectivity and traffic routing between the physical router and AWS VPCs.

Phase 4: Optimization and Documentation (May 11th - May 24th)

Performance Optimization:

- Optimize router configurations for performance and reliability, adjusting VPN parameters and encryption settings as needed.
- Monitor router performance metrics to ensure efficient use of resources and minimal latency.

Security Hardening:

- Implement security measures on the physical router, such as access control lists (ACLs), firewall rules, and intrusion prevention systems (IPS), to protect against potential threats.

Documentation:

- Document the physical router configuration details, including VPN settings, routing policies, and security configurations.
- Create operational documentation for router management, maintenance, and troubleshooting procedures.

Phase 5: Deployment and Training (May 25th - May 30th)

Deployment:

- Deploy the configured physical router into production on-premises environments.
- Test VPN connectivity and traffic routing between on-premises networks and AWS VPCs, ensuring proper functionality.

Training:

- Provide training sessions for network administrators on managing and maintaining the physical router, including VPN configuration, monitoring, and troubleshooting.

7.Details of Financial Assistance required.

Strengthening IIOT Cybersecurity through SSH and VPN integration

Estimated Project Budget

S.NO	SERVICES	COST ESTIMATION
1.	VPC	1300
2.	Subnets	300
3.	Network Address Translation (NAT) Gateway	500
4.	Gateway Load Balancer Endpoint	480
5.	Internet Gateways	500
6.	NAT Gateways/NAT Instances	456
7.	Elastic IP Addresses	270
8.	Route Tables	505
9.	AWS Private Link	345
10.	Data Transfer	500
11.	Gateway Load Balancer	433
12.	Load Capacity Units (LCUS)	395
13.	Traffic Mirroring	200
14.	Cloud WAN	500
15.	Transit Gateway	500
16.	Client VPN settings	500
17.	Network ACLs	445
18.	Security Groups	375
19.	Router	1500
20.	EC2 Instance	600
	TOTAL	**10,104**

UNDERTAKING

1. The college will provide the basic infrastructure and other required facilities to the students for timely completion of their projects.

2. The college will undertake the financial and other management responsibilities of the project also the college will be responsible in following the timelines.

3. The college will ensure that the funds provided are utilized only for the purpose provided and any remaining amount will be returned to the University after thetime of completion of the project.

4. I hereby declare that the details furnished above are true and correct.

M. Rajashanthi

Signature of Faculty Guide

Signature of Principal

PRINCIPAL
Theni Kammavar Sangam College of Technology
Koduvilarpatti, Theni - 625 534