

Project Design Phase-I

Solution Architecture

	26 October 2023
Team ID	591486
Project Name	network anomaly detection
Maximum Marks	2 Marks
Team members names	Niraianbu kamalnath abirami Tharunya bala

Solution Architecture:

The solution architecture for our network anomaly detection system is designed for maximum efficiency and accuracy. Data from diverse sources is ingested, preprocessed, and stored for historical analysis, while real-time data is processed to enable immediate anomaly detection. Advanced machine learning models and feature engineering aid in anomaly identification.

- 1.Data Sources
- 2.Data Ingestion
- 3.Data Storage
- 3.Real-Time Data Processing
- 4.Anomaly Detection Models
- 5.Feature Engineering
- 6.Model Training and Evaluation
- 7.Alert Generation
- 8.Integration with SIEM System
- 9.Incident Response
- 10.User Interface and Visualization
- 11.Feedback Loop
- 12.Compliance and Reporting:

Link:

<https://drive.google.com/file/d/1PtONXmhtwYI4tKV06FVYqRCOf9rvvCJ/view?usp=sharing>

