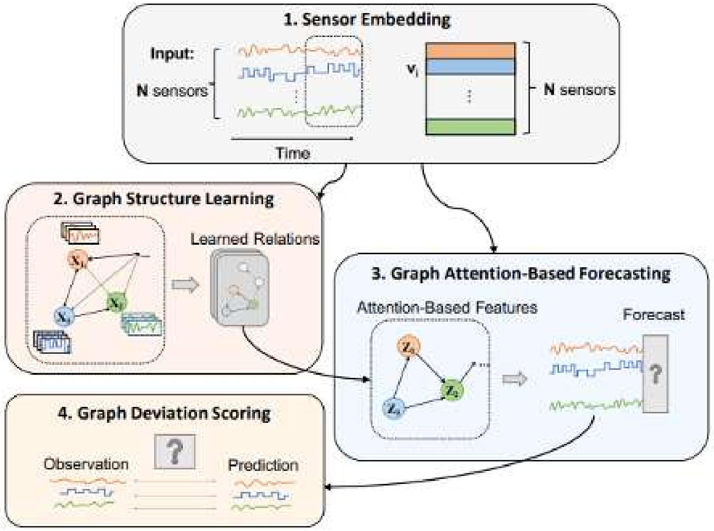
Project Design Phase-II
Technology Stack (Architecture & Stack)

Date	25 October 2023
Team ID	4.3
Project Name	Network Anomaly Detection
Maximum Marks	4 Marks

Technical Architecture:

Reference: https://www.ieeesem.com/researchpaper/Network_Anomaly_Detection_Using_Machine_Learning_A_Review_Paper.pdf



Guidelines:

1. Include all the processes (As an application logic / Technology Block)
2. Provide infrastructural demarcation (Local / Cloud)
3. Indicate external interfaces (third party API's etc.)
4. Indicate Data Storage components / services
5. Indicate interface to machine learning models (if applicable)

Table-1 : Components & Technologies:

SL.No	COMPONENT	DESCRIPTION	TECHNOLOGY
1	Data Collector	Collects network traffic data in real time.	Wireshark, tcpdump
2	Packet Decoder	Decodes network traffic packets into a format that can be processed by the feature engineering component.	Scapy, dpkt
3	Feature Engineer	Extracts relevant features from the decoded network traffic data.	Pandas, scikit-learn, Featuretools
4	Machine Learning Model	Detects anomalous network traffic patterns using machine learning algorithms.	TensorFlow, PyTorch, scikit-learn
5	Alert Generator	Generates alerts for detected anomalous network traffic patterns.	PagerDuty, OpsGenie
6	Model Manager	Manages the lifecycle of machine learning models, including training, deployment, and monitoring.	MLflow, Neptune
7	Model Registry	Stores and manages machine learning models.	TensorFlow Serving, Amazon SageMaker Model Registry
8	Data Storage	Stores the collected network traffic data and the extracted features.	Amazon S3, Google Cloud Storage
9	Data Processing	Processes the collected network traffic data and the extracted features to prepare them for machine learning.	Apache Spark, Amazon EMR
10	Monitoring	Monitors the performance of the network anomaly detection system and alerts the appropriate personnel if there are any problems.	Grafana, Prometheus
11	Visualization	Visualizes the collected network traffic data and the detected anomalies to help analysts understand the security situation.	Kibana, Tableau

12	Security	Protects the network anomaly detection system from unauthorized access and attacks.	AWS Identity and Access Management (IAM), Google Cloud Identity and Access Management (IAM)
13	Logging	Logs all activity in the network anomaly detection system for auditing and troubleshooting purposes.	Amazon CloudWatch Logs, Google Cloud Logging

Table-2: Application Characteristics:

SL.No	Characteristic	Description	Technology
1	Scalability	The ability to handle large volumes of network traffic data.	Distributed systems, cloud computing
2	Performance	The ability to detect anomalous network traffic patterns in real time.	High-performance computing, in-memory data processing
3	Accuracy	The ability to accurately detect anomalous network traffic patterns with minimal false positives and false negatives.	Machine learning algorithms, feature engineering
4	Robustness	The ability to operate reliably in the presence of noise and errors in the data.	Data preprocessing, model validation
5	Explainability	The ability to explain the reasons for detected anomalies to analysts.	Interpretable machine learning algorithms
6	Ease of use	The ability to be used by analysts with a variety of skill levels.	User-friendly interfaces, documentation
7	Integratability	The ability to be integrated with existing security systems.	Open APIs, standard data formats
8	Cost-effectiveness	The ability to be deployed and operated at a reasonable cost.	Cloud computing, open source software

9	Security	The ability to protect against unauthorized access and attacks.	Encryption, access control, security monitoring
10	Auditing	The ability to log all activity for auditing and troubleshooting purposes.	Audit logs, security information and event management (SIEM) systems
11	Compliance	The ability to comply with relevant security regulations and standards.	Industry-specific security certifications, compliance reporting tools

References:

https://www.mdpi.com/2504-3900/54/1/8

https://ieeexplore.ieee.org/document/9182197

https://rranjans.files.wordpress.com/2019/08/75.pdf

https://arxiv.org/pdf/2112.03315

https://dl.acm.org/doi/10.1007/s10586-017-1117-8

https://www.ieeesem.com/researchpaper/Network_Anomaly_Detection_Using_Machine_Learning_A_Review_Paper.pdf