SOLUTION ARCHITECTURE

DATE	25-10-2023
TEAM ID	4.1
PROJECT NAME	NETWORK ANOMALY DETECTION

MENTOR : P MANOJ

Team Members :

C DEVAKI NANDAN REDDY

S NIHAL AHMED

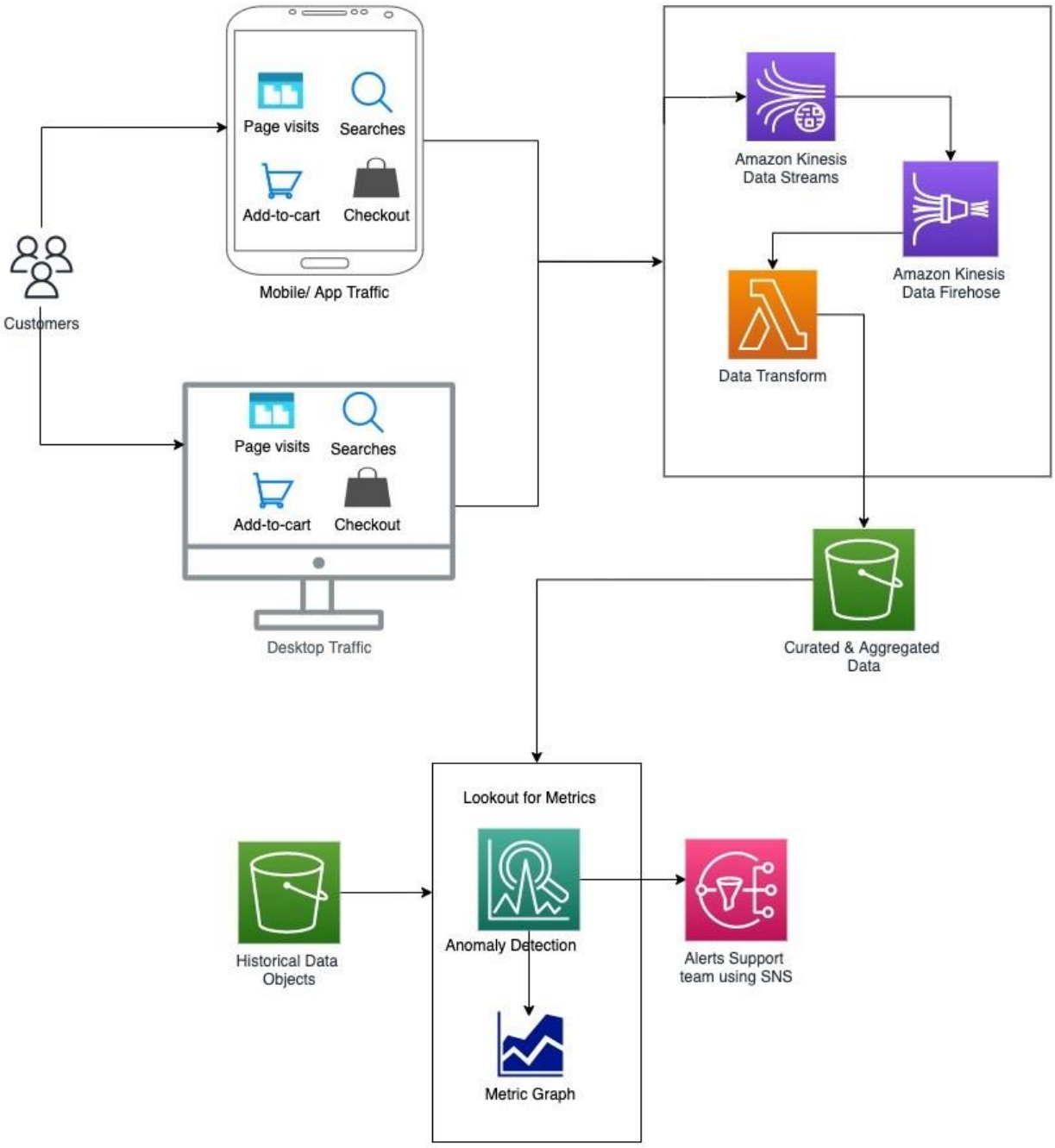
Designing a solution architecture for network anomaly detection involves defining the components and their interactions to effectively identify and respond to anomalies in a network.

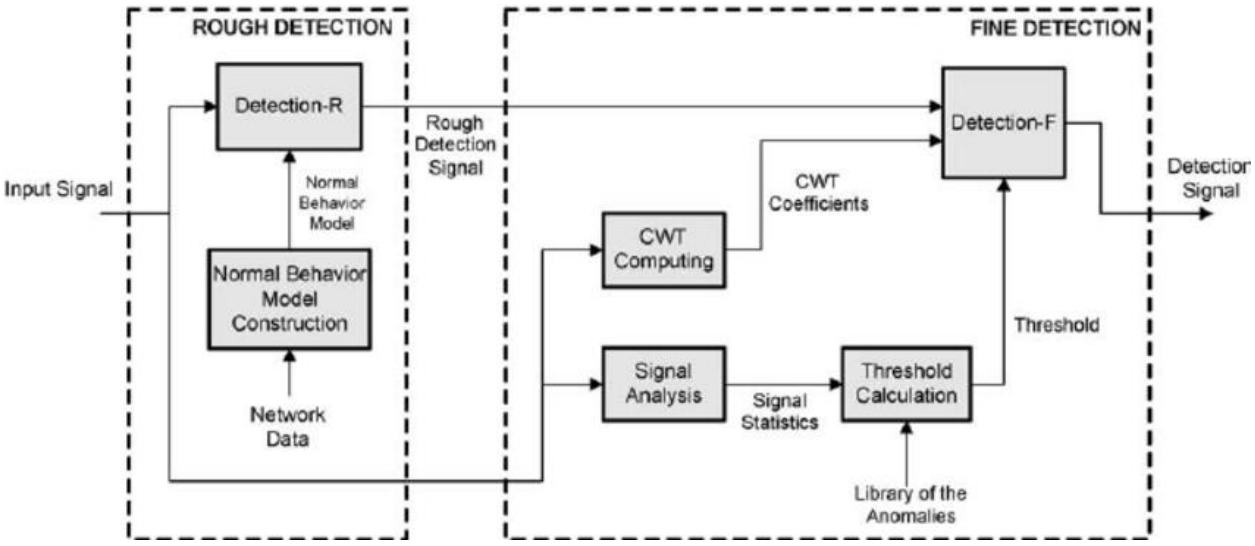
1. **Data Sources:**
   - Ingress points for network data, including routers, switches, firewalls, and servers.
   - External data sources like threat intelligence feeds and cloud services.
2. **Data Ingestion Layer:**
   - Data collection from various sources in real-time or batch modes.
   - Protocols and connectors for data retrieval.
3. **Data Processing and Transformation:**
   - Preprocessing of raw data, including cleaning, normalization, and format conversion.
   - Feature extraction to prepare data for analysis.
4. **Data Storage:**
   - A scalable and reliable storage system for raw and processed data.
   - Long-term storage for historical data for trend analysis.
5. **Machine Learning Models:**
   - Implementing machine learning models for anomaly detection.
   - Training, updating, and optimizing models with historical and real-time data.

6. **Rules Engine:**
    - Define custom rules and thresholds for specific anomalies or behaviors.
    - Rules can complement machine learning for fine-tuning detection.
7. **Real-time Monitoring Layer:**
    - Continuous monitoring of network traffic and events.
    - Integration with data analysis components.
8. **Alerting and Notification:**
    - Generate alerts when anomalies are detected.
    - Notifications to relevant teams or individuals.
9. **Incident Response:**
    - Automated or manual incident response workflows.
    - Actions such as isolating affected systems, capturing data, and analyzing the nature of anomalies.
10. **User Interface:**
    - A web-based or desktop interface for administrators and analysts.
    - Visualization of network activity and detected anomalies.
11. **APIs and Integration:**
    - APIs for integrating with other security tools and systems, such as SIEM and ticketing systems.
12. **Reporting and Forensics:**
    - Reporting tools for generating incident reports and compliance documentation.
    - Data forensics capabilities for post-incident analysis.
13. **Scalability and High Availability:**
    - Architect for scalability and redundancy to handle increasing data volumes and ensure system availability.
14. **Security and Access Control:**
    - Implement robust security measures to protect the anomaly detection system from threats.
    - Access control for authorized personnel only.
15. **Compliance and Audit Trail:**
    - Ensure the solution complies with relevant regulatory requirements.
    - Maintain an audit trail for tracking system changes and activities.
16. **Feedback Loop:**
    - Mechanism for collecting feedback on detected anomalies to improve the system over time.
17. **Cloud Integration (Optional):**
    - If applicable, integration with cloud services for network data analysis.
18. **Performance Monitoring:**

- Monitoring of system performance and resource utilization.

19. **Training and Documentation:**
    - Training materials and documentation for administrators and analysts.
20. **Maintenance and Updates:**
    - Plan for system maintenance, updates, and patch management.


Page visits
Searches
Add-to-cart
Checkout
Mobile/ App Traffic
Customers
Page visits
Searches
Add-to-cart
Checkout
Desktop Traffic
Amazon Kinesis
Data Streams
Amazon Kinesis
Data Firehose
Data Transform
Curated & Aggregated
Data
Lookout for Metrics
Historical Data
Objects
Anomaly Detection
Metric Graph
Alerts Support
team using SNS



The Anomaly Detection solution…

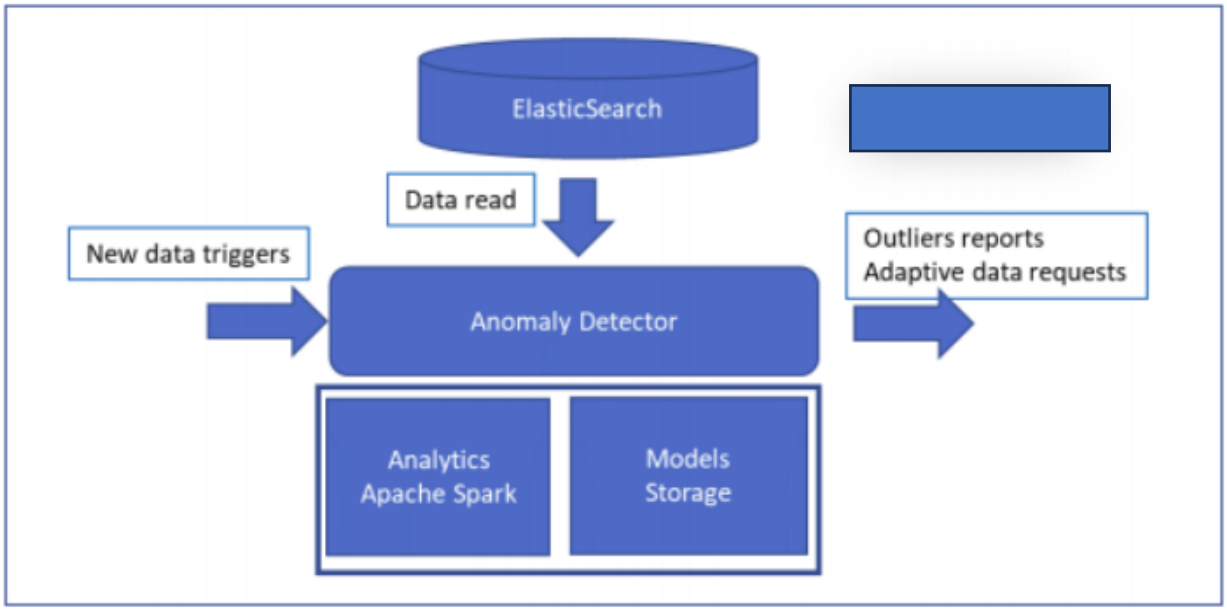


Figure 1 - Anomaly Detection component architecture