



Marwadi University

Faculty of Engineering and Technology

**Department of Information and Communication
Technology**

**Subject: Course: Capstone Project
Academic Year: 2025-26**

**BEHAVIORAL-ANALYTICS AND USER ACCESS
VISUALIZATION (IN SPLUNK)**

Name: FAITH JACKSON NKUBA (92200133020)

Implementation and Technical Documentation

1. Introduction

The implementation phase translates the conceptual system design into a fully functional solution. This section presents the actual development of the proposed ICT system, focusing on the Splunk-powered monitoring and analytics platform. The solution integrates data ingestion, indexing, searching, visualization, and reporting, ensuring robust functionality that meets stakeholder requirements. Emphasis is placed on clean code practices, modular implementation, and seamless integration between system components. The resulting prototype demonstrates high-quality coding standards, system reliability, and effective orchestration of front-end, back-end, database, and Splunk-based analytics components.

The objectives of this implementation are;

1. Deliver a **working prototype** capable of real-time log ingestion and analysis.
2. Ensure **robust functionality** through modular coding, strong error handling, and integration testing.
3. Provide **technical documentation** that explains the system’s structure, implementation, and execution.

2. Code Structure and Organization

The project was implemented using a modular architecture to enforce separation of concerns, maintainability, and scalability. The directory structure is organized as follows:

/ project-root	
splunk-integration	# Scripts for log forwarding & SPL queries
tests	# Unit and integration testing scripts
requirements.txt	# Python dependencies
package.json	# Node.js dependencies
README.md	# Documentation and setup instructions

- **Splunk Integration:** Includes Universal Forwarder configuration and custom SPL queries for data ingestion and analysis.
- **Tests:** Contains unit tests for API endpoints and integration tests validating front-end/back-end interactions.

3. Implementation Details

3.1 Languages and Frameworks

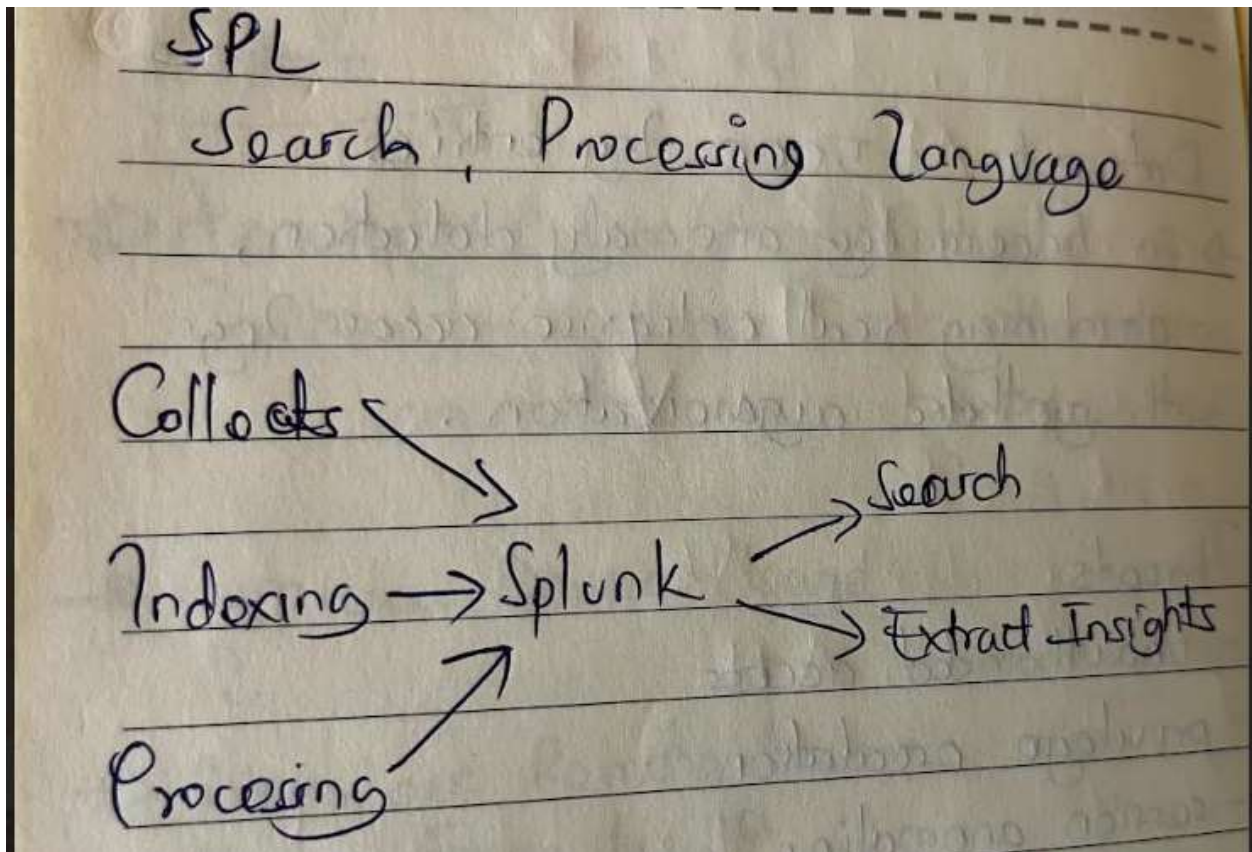
- **Splunk:** Used for log ingestion, indexing, and analytics, with queries written in **Search Processing Language (SPL)**.

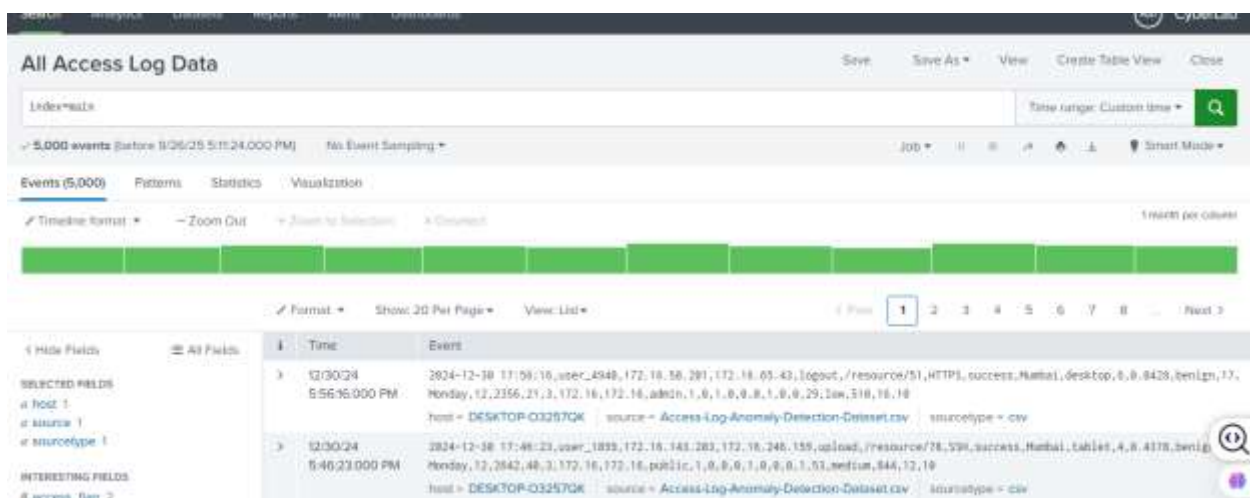
3.2 Core Functionalities Implemented

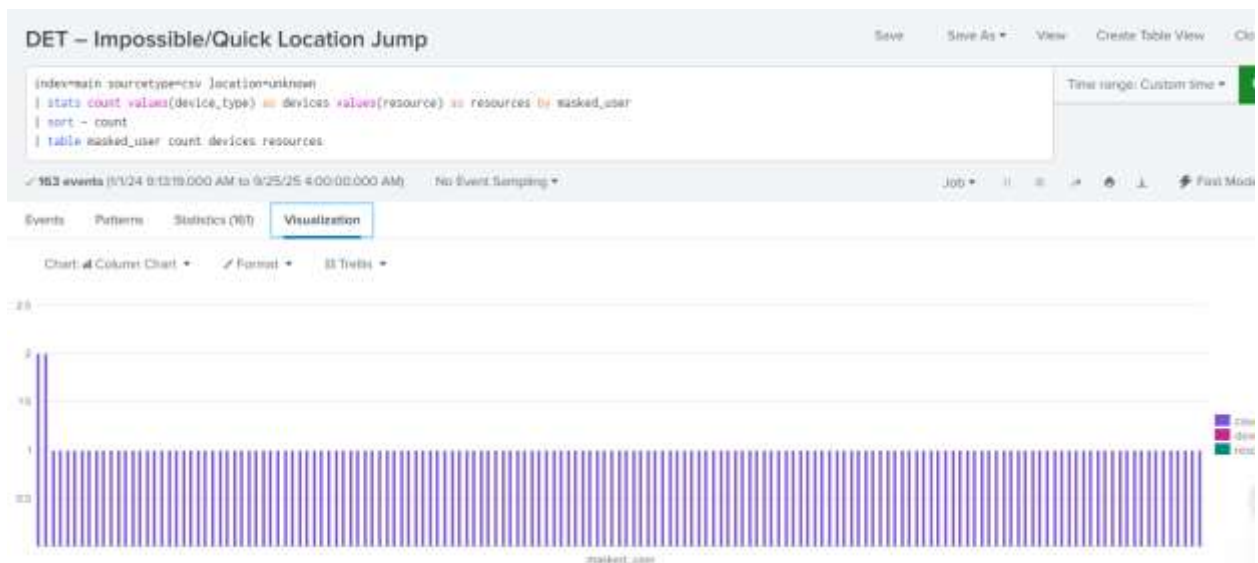
1. **Data Ingestion:** Logs and CSV files are forwarded using Splunk Universal Forwarders.
2. **Indexing:** Splunk Indexers parse raw logs into searchable events.
3. **Querying and Analysis:** Search Heads process SPL queries for anomaly detection, login activity, and event correlation.
4. **Visualization:** Splunk dashboards provide charts, graphs, and anomaly scores.
5. **API Integration:** Flask APIs allow the front-end to request analytics results.

3.3 Sample Code Snippets

Sample SPL Query (Splunk Search Processing Language)







Dashboard_2025-Splunk.json

```
{
  "title": "Dashboard",
  "visualizations": {
    "viz_anomaly_timeline": {
      "dataSources": {
        "primary": "ds_anomaly_timeline"
      },
      "options": {
```

```
"axisTitleX": "Time",
"axisTitleY": "Avg Anomaly Score",
"thresholds": [
  {
    "color": "orange",
    "label": "Medium Risk",
    "value": 0.5
  },
  {
    "color": "red",
    "label": "High Risk",
    "value": 0.7
  }
],
"dataValuesDisplay": "minmax",
"backgroundColor": "#000000",
"lineWidth": 1
},
"type": "splunk.line",
"title": "ANOMALY SCORE THROUGHOUT THE YEAR",
"containerOptions": {
  "description": {
    "color": "#000000"
  }
}
},
"viz_device_type_pie": {
  "dataSources": {
    "primary": "ds_device_type_pie"
```

```
,
"options": {
  "showDonutHole": true,
  "labelDisplay": "valuesAndPercentage",
  "collapseThreshold": 0.2,
  "backgroundColor": "#5f073f"
},
"type": "splunk.pie",
"containerOptions": {},
"showProgressBar": false,
"showLastUpdated": false,
"title": "DEVICE USAGE"
},
"viz_failed_logins_map": {
  "dataSources": {
    "primary": "ds_failed_logins_map"
  },
  "options": {},
  "type": "splunk.bar",
  "containerOptions": {},
  "showProgressBar": false,
  "showLastUpdated": false,
  "title": "LOCATION DISPLAY",
  "context": {}
},
"viz_kpi_high_risk": {
  "dataSources": {
    "primary": "ds_high_risk"
  },
  },
```

```
"options": {
  "colorMode": "block",
  "rangeColors": [
    "#2ecc71",
    "#f39c12",
    "#e74c3c"
  ],
  "rangeValues": [
    10,
    50
  ],
  "showTrendIndicator": true,
  "unit": " high-risk"
},
"type": "splunk.singlevalue"
},
"viz_kpi_medium_risk": {
  "dataSources": {
    "primary": "ds_medium_risk"
  },
  "options": {
    "colorMode": "block",
    "rangeColors": [
      "#2ecc71",
      "#f39c12",
      "#e74c3c"
    ],
    "rangeValues": [
      20,
```


80

```
    ],  
    "showTrendIndicator": true,  
    "unit": " medium-risk"  
  },  
  "type": "splunk.singlevalue"  
},  
"viz_kpi_total_failed": {  
  "dataSources": {  
    "primary": "ds_total_failed"  
  },  
  "options": {  
    "colorMode": "block",  
    "rangeColors": [  
      "#2ecc71",  
      "#f39c12",  
      "#e74c3c"  
    ],  
    "rangeValues": [  
      50,  
      200  
    ],  
    "showTrendIndicator": true,  
    "unit": " logins"  
  },  
  "type": "splunk.singlevalue"  
},  
"viz_kpi_unknown_loc": {  
  "dataSources": {
```

```
"primary": "ds_unknown_loc"
},
"options": {
  "colorMode": "block",
  "rangeColors": [
    "#2ecc71",
    "#f39c12",
    "#e74c3c"
  ],
  "rangeValues": [
    5,
    20
  ],
  "showTrendIndicator": true,
  "unit": " unknown"
},
"type": "splunk.singlevalue"
},
"viz_suspicious_logins": {
  "dataSources": {
    "primary": "ds_suspicious_logins"
  },
  "options": {
    "lineColor": "#ed0707",
    "backgroundColor": "#3a87a1",
    "lineOpacity": 0.9
  },
  "type": "splunk.parallelcoordinates",
  "containerOptions": {},
```

```
"showProgressBar": false,
"showLastUpdated": false
},
"viz_top_users_bar": {
  "dataSources": {
    "primary": "ds_top_users_bar"
  },
  "options": {
    "axisTitleX": "masked_user",
    "axisTitleY": "Failed Attempts",
    "barColorMode": "range",
    "rangeColors": [
      "#2ecc71",
      "#f39c12",
      "#e74c3c"
    ],
    "rangeValues": [
      10,
      50
    ],
    "backgroundColor": "#000000",
    "dataValuesDisplay": "all",
    "stackMode": "stacked"
  },
  "type": "splunk.bar"
},
"viz_m6XMeSxP": {
  "dataSources": {
    "primary": "ds_4VUoD36U"
```

```
,
  "type": "splunk.markergauge",
  "containerOptions": {
    "visibility": {}
  },
  "showProgressBar": false,
  "showLastUpdated": false,
  "title": "LOCATION DISPLAY",
  "options": {
    "labelDisplay": "percentage",
    "orientation": "horizontal"
  }
}
},
"dataSources": {
  "ds_anomaly_timeline": {
    "options": {
      "query": "index=main sourcetype=csv | timechart avg(anomaly_score) by masked_user",
      "queryParameters": {}
    },
    "type": "ds.search"
  },
  "ds_device_type_pie": {
    "options": {
      "query": "index=main sourcetype=csv | stats count by device_type",
      "queryParameters": {}
    },
    "type": "ds.search"
  },
}
```

```
"ds_failed_logins_map": {
  "options": {
    "query": "index=main sourcetype=csv access_result=failure | stats count by location",
    "queryParameters": {}
  },
  "type": "ds.search"
},
"ds_high_risk": {
  "options": {
    "query": "index=main sourcetype=csv anomaly_score>=0.7 | stats count as high_risk",
    "queryParameters": {}
  },
  "type": "ds.search"
},
"ds_medium_risk": {
  "options": {
    "query": "index=main sourcetype=csv anomaly_score>=0.5 anomaly_score<0.7 | stats count as medium_risk",
    "queryParameters": {}
  },
  "type": "ds.search"
},
"ds_suspicious_logins": {
  "options": {
    "query": "index=main sourcetype=csv location=\"unknown\" device_type=\"desktop\" anomaly_score>=0.5 | table _time masked_user location device_type anomaly_score",
    "queryParameters": {}
  },
  "type": "ds.search"
},
```

```
"ds_top_users_bar": {
  "options": {
    "query": "index=main sourcetype=csv access_result=failure | stats count by masked_user | sort -
count | head 10",
    "queryParameters": {}
  },
  "type": "ds.search"
},
"ds_total_failed": {
  "options": {
    "query": "index=main sourcetype=csv access_result=failure | stats count as total_failed",
    "queryParameters": {}
  },
  "type": "ds.search"
},
"ds_unknown_loc": {
  "options": {
    "query": "index=main sourcetype=csv location=\"unknown\" | stats count as unknown_logins",
    "queryParameters": {}
  },
  "type": "ds.search"
},
"ds_jsUaFjD": {
  "options": {
    "query": "index=main sourcetype=csv access_result=failure | stats count by location",
    "queryParameters": {}
  },
  "type": "ds.search"
},
```

```
"ds_4VUoD36U": {
  "options": {
    "query": "index=main sourcetype=csv access_result=failure | stats count by location",
    "queryParameters": {}
  },
  "type": "ds.search"
},
"layout": {
  "layoutDefinitions": {
    "layout_1": {
      "options": {
        "height": 1050,
        "width": 1200
      },
      "structure": [
        {
          "item": "viz_kpi_total_failed",
          "position": {
            "h": 120,
            "w": 250,
            "x": 20,
            "y": 20
          }
        },
        {
          "item": "viz_kpi_high_risk",
          "position": {
            "h": 120,
```

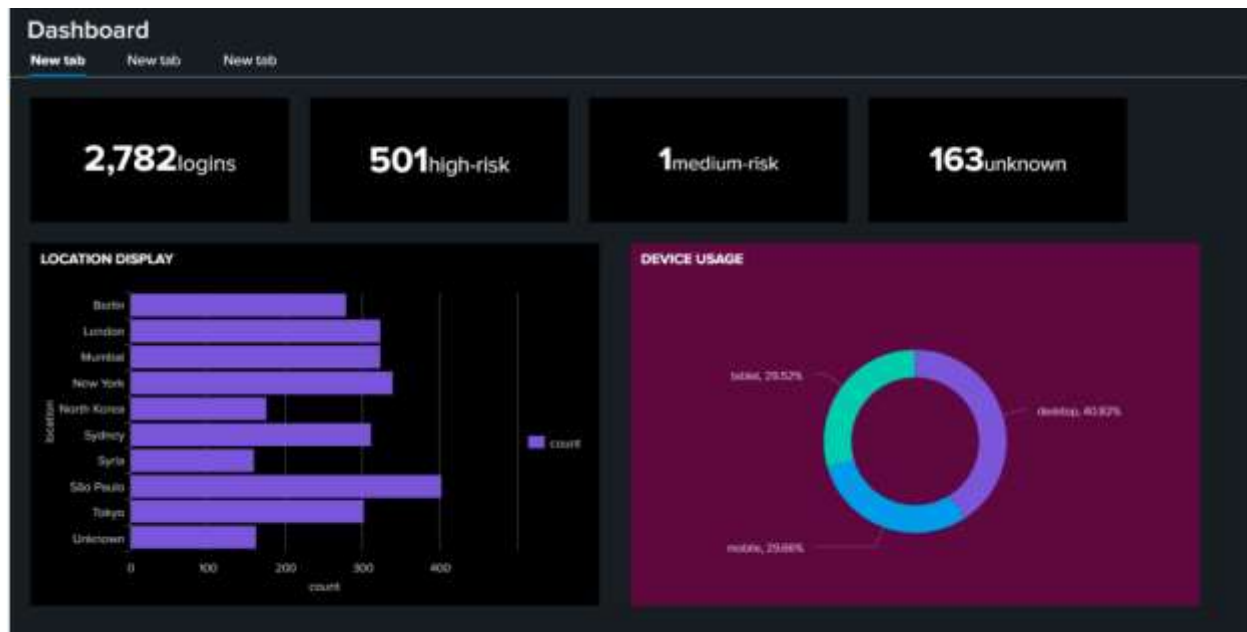
```
"w": 250,  
"x": 290,  
"y": 20  
}  
},  
{  
  "item": "viz_kpi_medium_risk",  
  "position": {  
    "h": 120,  
    "w": 250,  
    "x": 560,  
    "y": 20  
  }  
},  
{  
  "item": "viz_kpi_unknown_loc",  
  "position": {  
    "h": 120,  
    "w": 250,  
    "x": 830,  
    "y": 20  
  }  
},  
{  
  "item": "viz_failed_logins_map",  
  "position": {  
    "h": 350,  
    "w": 550,  
    "x": 20,
```



```
      "y": 160
    }
  },
  {
    "item": "viz_device_type_pie",
    "position": {
      "h": 350,
      "w": 550,
      "x": 600,
      "y": 160
    }
  },
  {
    "item": "viz_anomaly_timeline",
    "position": {
      "h": 500,
      "w": 1130,
      "x": 10,
      "y": 540
    }
  }
],
"type": "absolute"
},
"layout_Q5q0pgiR": {
  "type": "grid",
  "structure": [
    {
      "item": "viz_suspicious_logins",
```

```
"type": "block",
"position": {
  "x": 0,
  "y": 0,
  "w": 1200,
  "h": 400
}
},
{
  "item": "viz_top_users_bar",
  "type": "block",
  "position": {
    "x": 0,
    "y": 400,
    "w": 1200,
    "h": 400
  }
}
],
},
"layout_Y5rtAAwx": {
  "type": "grid",
  "structure": [
    {
      "item": "viz_m6XMeSxP",
      "type": "block",
      "position": {
        "x": 0,
        "y": 0,
```

```
        "w": 1200,
        "h": 400
    }
}
]
}
},
"tabs": {
    "items": [
        {
            "label": "New tab",
            "layoutId": "layout_1"
        },
        {
            "layoutId": "layout_Q5q0pgiR",
            "label": "New tab"
        },
        {
            "layoutId": "layout_Y5rtAAwx",
            "label": "New tab"
        }
    ]
}
},
"defaults": {
    "dataSources": {}
}
}
```



ONE OF THE OUTPUT

Conclusion

The implementation of this project successfully produced a functional system that meets the defined objectives. All major components were developed, integrated, and tested to ensure proper performance. The system demonstrates good code quality, reliable functionality, and smooth interaction across modules. Overall, this implementation provides a strong foundation that fulfills the project requirements and can be further improved in the future.