**DEEP LEARNING APPROACHES TO PROFILING ORGANIZATIONAL THREATS (NEXTGEN SOC)**



**Software Requirements Specification (SRS) of 24-25J-075**

**Project ID: 24-25J-075**

|  |  |
| --- | --- |
| **Names** | **Student IDs** |
| Senevirathna D.H. | IT21298608 |
| Gunasekara W.M.M. | IT21226496 |
| Gunawardhana K.P.A.T. | IT21058196 |
| Ashra M.F.F. | IT21380396 |

**Supervisor: Dr. Harinda Fernando**

**Co Supervisor: Mr. Kavinga Yapa Abeywardena**

BSc. (Hons) in Information Technology Specializing in Cybersecurity

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

**Table of Contents**

[**1.** **Introduction** 3](#_Toc184240888)

[**1.1 Purpose** 4](#_Toc184240889)

[**1.2 Scope** 5](#_Toc184240890)

[**1.3.** **Definitions, Acronyms, and Abbreviations** 7](#_Toc184240891)

[**1.4.** **Overview** 8](#_Toc184240892)

[**2.** **Overall Descriptions** 11](#_Toc184240893)

[ **Main Goals of the Software** 13](#_Toc184240894)

[ **Primary Functionalities** 14](#_Toc184240895)

[ **Environment and Context:** 15](#_Toc184240896)

[ **Non-Functional Considerations:** 17](#_Toc184240897)

[**2.1** **Product perspective** 18](#_Toc184240898)

[2.1.1. System interfaces 19](#_Toc184240899)

[2.1.2. User interfaces 19](#_Toc184240900)

[2.1.3. Hardware interfaces 21](#_Toc184240901)

[2.1.4. Software interfaces 21](#_Toc184240902)

[2.1.5. Memory constraints 22](#_Toc184240903)

[2.1.6. Operations 22](#_Toc184240904)

[2.1.7. Site adaptation requirements 23](#_Toc184240905)

[**2.2. Product functions** 23](#_Toc184240906)

[**2.3.** **User characteristics** 24](#_Toc184240907)

[**2.4.** **Constraints** 25](#_Toc184240908)

[**2.5.** **Assumptions and dependencies** 26](#_Toc184240909)

[**2.6.** **Apportioning of requirements** 27](#_Toc184240910)

[**2.7 Testing** 29](#_Toc184240911)

[**3.** **Specific Requirements** 30](#_Toc184240912)

[**3.1. External interface requirements** 30](#_Toc184240913)

[3.1.1. User interfaces 30](#_Toc184240914)

[3.1.2. Hardware interfaces 31](#_Toc184240915)

[3.1.3. Software interfaces 32](#_Toc184240916)

[3.1.4. Communication interfaces 32](#_Toc184240917)

[**3.2 Classes/Objects** 33](#_Toc184240918)

[**3.3 Performance requirements** 34](#_Toc184240919)

[**3.4. Design constraints** 35](#_Toc184240920)

[**3.5. Software system attributes** 37](#_Toc184240921)

[3.5.1. Reliability 37](#_Toc184240922)

[3.5.2. Availability 37](#_Toc184240923)

[3.5.3. Security 37](#_Toc184240924)

[3.5.4. Maintainability 39](#_Toc184240925)

[**3.6. Other requirements** 39](#_Toc184240926)

[**5.** **References** 40](#_Toc184240927)

**List of Figures**

[Figure 1 21](#_Toc184241100)

[Figure 2 21](#_Toc184241101)

**List of Table**

[Table 1 8](#_Toc184241138)

# **Introduction**

## **1.1 Purpose**

This document, which is the Software Requirements Specification (SRS), provides a basis that will guide the NextGen SOC (Security Operations Center) system development and implementation. This system is built based on the latest Deep Learning (DL) and Machine Learning (ML) to improve the way of threat profiling in the organization.

The main objective of the NextGen SOC system is to respond to the changing nature of threats, ensuring enterprises have necessary protection for their resources through a flexible and intelligent system. As opposed to the conventional SOC systems, which offer a possibility of applying standards, norms, or using specialists’ wide and time-consuming approach to threats’ identification in case of figuring out the security threats and their parameters, this system employs DL/ML algorithms to optimize those processes.

Specifically, the system focuses on four critical dimensions of threat profiling:

1. Endpoint Data Analysis- Watching and analyzing data created by endpoints like computer, host, server, and other internet enabled devices to discover any suspected malicious activities or behaviors.
2. Physical Security Systems-Improving surveillance capacity using data from security systems such as Closed-Circuit Television (CCTV) to identify intruders or other anomalous activity in closed environments operationally immediately.
3. Human Behavior Analysis- The regular observation of employee behaviors or activities in an organization with a view of tracking any insiders during compliance with legal and ethical standards.
4. Network Traffic Analysis: Monitors and analyzes network traffic patterns to detect anomalies and potential cyber threats.

It gives the developers an understanding of the system’s functional and non-functional requirements, giving the project direction towards the fulfillment of its goal and meeting the stakeholders’ needs. This SRS serves as the standard for assessing the final system and proves that the offered solution complies with the requirements specified in this document. It creates the foundation for a system which could accommodate future developments in threat detection and mitigate new cyber threats.

## **1.2 Scope**

As for this document, here, the main goals and scope will be described, and the focus will be drawn on the necessity to use new DL and ML techniques to create an efficient cybersecurity system.

Key Areas of Threat Profiling

The system will provide a comprehensive framework for detecting and mitigating threats across four critical dimensions:

1. **Endpoint Data Analysis**:
   * Endpoints, such as desktops, laptops, mobile devices, and servers, generate vast amounts of data, including system logs, application events, and user activities.
   * Random Forest and Neural Networks are then trained for identifying the behavior for normal and anomalous behavior. Random Forest is more suitable for various treatments of data while Neural Networks are more sensitive to recognizing the complex patterns that specifically identify anomalies.
2. **Physical Security Systems**:
   * The system will integrate with CCTV cameras and access control systems to enhance physical security.
   * There are few-shot learning models that it will utilize for analyzing the video feeds in real-time, identifying activities which are shooting near ‘no go’ zones or forced attempts to breach barricaded doors.
3. **Human Behavior Analysis:**

* For insiders’ threats, the system will monitor how employees conduct themselves in their day-to-day activities and also how they relate with other employees if they show any signs of being a threat to the business, the system will record them.
* A Random Forest model, with decision trees, will be used to identify insiders. This model is not sensitive to nature and can seamlessly handle complex interactions within data and is also able to detect behavioral outliers.

1. **Network Traffic Analysis**:
   * The system will be comprised of means for identifying existing and emerging cyber threats based on analyzing the flow of traffic through the network.
   * Feedforward Neural Network, Decision tree Classifiers and Generative Adversarial Networks (GANs) will be used for the learning of new threats in cyberspace since the threat continues to evolve over time.

**Implementation of modern Technologies**

The scope entails operation and management of an advanced technology platform to strengthen and improve the system.

* **Random Forest Model**: The data analysis involves passing data through a model to discover threats and anomalies, to provide a strong and accurate threat identification method.
* **Graph Neural Networks (GNNs)**: Enables the identification of complex interconnection between individuals in organizational structures.
* **Neural Networks**: A type of multi-layered models that help find multiple layers and patterns in the traffic and users’ activities for accurate anomaly differentiation and threats prediction.
* **Feedforward Neural Networks:** Analyze patterns in labeled network traffic for efficient anomaly detection.
* **Decision Tree Classifiers:** Provide interpretable and fast classification based on feature splits.
* **DenseNet121 (Transfer Learning)**: A trained deep learning model that has been applied in feature extraction and classification in real-time videos for threats to physical security systems.

**Right Time Operational Application**

The system is developed to work in real-time operation environments characteristic of present SOCs.

* Real-time surveillance of the organizational assets and informational flows to counter threats on-going.
* Investigation of security alerts and giving timely notifications to contain specific attacks as much as possible.
* Compatibility with other security tools and processes in order to create one consistent cybersecurity platform.

**Target Environment**

It is particularly designed for deployment within a Security Operations Center or SOC, where it will-

* Function as an application for threat identification and assessment.
* Increase awareness of the organization with regards to risk coming from ‘inside threats’ and ‘outside threats.
* Offer SOC analysts a set of practical tips and best practices on how to handle security risks in advance and bring them to a standstill.

## **Definitions, Acronyms, and Abbreviations**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| SOC | Security Operations Center |
| DL | Deep Learning |
| ML | Machine Learning |
| CCTV | Closed-Circuit Television |
| GDPR | General Data Protection Regulation |
| IDS/IPS | Intrusion Detection and Prevention Systems |

Table 1

## **Overview**

NextGen SOC system is likely to be progressive, smart formation for providing organization’s security if and when DL & ML are in the process. This document is the reference point of how to identify, assess and control risks that affect organizations by outlining the techniques and tools that will be employed when implementing risk management within organizations.

The document also defines how the system is to monitor the organizational threats based on different parameters of the organization which includes the Endpoint devices, Network Traffic, Physical Security systems, and Human Behavior Analysis. All these dimensions are interrelated and give a perspective view of threat existence in an organization.

Typically, conventional security analyzers are based on specific patterns, so they are sluggish to adapt to new threats. The NextGen SOC system does not have such limitations because it uses the DL and ML algorithms that learn new threats from experience. It can also possibly participate in threat detection because it is capable of recognizing patterns and actions.

There is another significant shift with the system, which is it can be operated in real time. This capability helps in preventing potential damage in security threats in that time is the only thing that will set an organization between success and failure in the event of an attack.

**Technologies and Methodologies:**

The document explains the current practice methods by which the system will be developed, and these include:

* **Random Forest Model:** This is a powerful technique in which many decision trees are built and results from all of them are combined, so that improved accuracy and stability of forecasts might be achievable. The first decision tree is trained on a random subset of the data and makes a separate decision from all the other trees. The final result is the fusion of all the different trees, which is often the mode for classification problems, or mean for regression. The above approach is specifically important in minimizing chances of overfitting thus improving the reliability of the model. Random Forest model allows analyzing more complex characteristics of threat and its detection, as well as effectiveness of threats and anomalies recognition.
* **Transfer Learning (DenseNet121)**: This technique involves using another model which has been pretrained from a large data such as ImageNet then its features, edges, textures, and shapes are learned. In this approach an initial model is reused for a new task so as to select relevant features in the input data. These adjustments may be made to make the model suited to more specific tasks like detecting threats, enhancing the rates at which it functions. This is especially preferred because compared to training a new model from scratch, this method takes less training time as features that the model needs to learn have already been extracted, and therefore converges faster with better results.
* **Generative Adversarial Network (GAN):** this is a type of machine learning model in which two neural networks are built, the generator and the discriminator which compete in order to enhance its performance. The generator then generates data samples, for instance, cyber threat patterns, while the discriminator analyses the newly generated data to distinguish it as either real or fake. And in this way, the generator can mimic generation of realistic high-quality data that did not exist initially in the data set used in training algorithm. This is useful in cybersecurity because it can synthesize threat data so that security detectors can learn from the data and recognize emergent threats that it may have never seen before.
* **Feedforward Neural Networks:** Feedforward Neural Networks are a deep learning model developed to analyze patterns in labeled network traffic data. These networks can find complex relationships between features by processing the data through several layers of interconnected neurons, hence turning out to be highly effective for anomaly detection tasks. Their capability for generalization from labeled examples enables them to accurately predict normal and abnormal network behavior, hence enhancing overall detection capability.
* **Decision Tree Classifiers**: Decision Tree Classifiers are a breed of interpretable machine learning models that split data using feature thresholds for network-traffic classification. Every branching is done such that a decision results in the largest gain of information, ensuring that the model has identified the most significant patterns from the data. The ease and simplicity of their structure allows fast classifying, enabling real-time applications. In this particular case, these models come with an added benefit, with their clear explanations for each predicted class being invaluable to fully understand and mitigate potential network threats.
* **Neural Networks:** Neural networks are the complex types of machine learning that allow computers to copy the brain structure and function and learn from data just like people do. In this project, multiplicative layer perceptron (MLPs) is used, and they contain layers that provide non-linearity such as ReLU and at the final layer a Sigmoid function for binary classification problems. These models are able to manually parse through the often large and complex logs of the endpoint and the observed network traffic in a search for telltale signs that might easily escape identification by simpler models.
* **Convolutional Neural Networks (CNNs)**: Employed image classification with DenseNet121 model to predict the presence of breast cancer, provided its dense connections enhance the learning of auxiliary features.

The system will immediately detect threats and will make the protection of assets much more proactive rather than reactive. It will be capable of identifying risks and preventing them from happening in the first place since it will be applying intelligent computational processes for this purpose.

The proposed approach should be valuable for SOC teams that would receive predictive information for improved response. Adapt to new threats in a way that the current structure of the organization does not fall to the new invading intruders in the world of cybercrimes.

* For developer – It is a kind of technical blueprint of the system development plan of the system that is featuring out.
* For Stakeholders- It gives them a particular view of the organizational targets of the system, its advantage, and the overall signification to the organization.
* For Security Teams-It describes how the system will integrate into the current processes to ease and improve on security related tasks, for instance threat detection.

# **Overall Descriptions**

NextGen SOC (Security Operations Center) system is a new advanced form of cybersecurity software solution that aims to deal with unprecedented development of threats in organizations. It improves the way organizations can identify and mitigate insider and external risks, with the use of advanced deep learning (DL) and machine learning (ML). This system moves away from the conventional linear, prescriptive methods of analysis employed in security by giving an intelligent, statistical structure that gives crucial information and protection against threats as they happen.

As the world becomes more computerized and complex even in the face of developing technology, organizations experience various security issues such as,

* From insider and outsider threats to increased volume and variety of cyberattacks, analysts report on perils that are becoming more imminent as modern technologies are adopted in organizations.
* Some of the weakness of traditional SOC systems includes Their inability to respond to new types of cyber threats or changing attack patterns.
* Due to the increased amount of data and data heterogeneity from network traffic, endpoints, human behavior, and physical security systems that require analysis.
* Privacy and ethical issues related to the collection and analysis of important user and organizational data.

NextGen SOC system is built on using different methodologies and techniques to describe and detect all types of threats.

**Endpoint Threat Detection**

Neural Networks: Identify endpoint data correlation that are not linear but digital and could be complex. It has been identified that they are especially useful in identifying new or emerging threats where it can identify hidden correlation in high dimensionality feature space datasets.

Random Forest: Offers a more accurate and interpretable classification model of endpoint activities as either legitimate or malicious. Its task operates by training numerous decision trees concurrently and then compilation their decisions in manner that reduces the false positive.

**Physical Security Threat Analysis**

Few-Shot Learning:Works with other physical security systems, for instance Closed Circuit Televisions for analyzing video streams to identify individuals exhibiting unusual activities in real-time basis. Incorporate Few-Shot Learning to teach models how to identify suspicious movements given a few labeled examples which include intrusions or lingering around prohibited terrains. Allows for fast transition to new conditions, and as a result it is especially good when working with environments where there is little labeled data on abnormal.

**Human Behavior Analysis**

Random Forest:Captures employee behavior and communication to identify an insider threat, for instance, copying of files and documents, logging in at what Would be deemed odd hours, access to another’s device. Uses the Random Forest Algorithm, a more reliable and explicative type of ML tool, in order to predict whether an action constitutes normal behavior or deviation from the norm based on totalized behavior data. This method affords accurate detection of threats, eliminates false positives, and addresses privacy issues because the data is not identifiable.

**Network Traffic Analysis**

(Generative Adversarial Networks - GANs): It constantly scrutinizes and scrutinizes the traffic in the network to alert the oddity; cyber threats including network attacks. Simulates attack scenarios by using Generative Adversarial Networks (GANs) to create synthetic data not available in the original dataset facilitating in its accuracy on novel complex cyber threats. which are unseen in existing dataset, improving the model’s ability to detect novel and sophisticated cyber threats.

Feedforward Neural Networks and Decision Tree Classifiers form an integral part of the system's anomaly detection. Feedforward Neural Networks will analyze labeled network traffic data through multiple layers of interconnected neurons, identifying complex relationships and patterns that enhance the detection of normal and abnormal behavior. On the other hand, Decision Tree Classifiers will make the approach interpretable by splitting data according to feature thresholds, hence making the classification of network traffic efficient. Put together, these models provide a powerful combination of accuracy, efficiency, and explainability that contributes to robust threat identification and mitigation in real-time applications.

### **Main Goals of the Software**

* Real-time threat analysis and detection

It helps the system understand the threats as they are, and it is able to help organizations address any concerns in real time. Combined with endpoint data, physical security, behavior and networks, the system reduces the length of time in which an organization is vulnerable to a threat.

* Increased Incident Response and Reducing Task

The underlying idea of automating threat identification and categorization eases the SOC teams’ workload. Experts can spend their efforts on the important things and choices while the machinery handles results and notifications for better response efficacy.

* Highly adaptive and expandable threat identification

The system adapts itself to these new emerging threats through the progression of learning through new offerings of data, imitation scenarios, and feedback. It also helps the organization to be ready for anything new that comes along to attack it by comfortably handling new threat landscape.

* Improved Connectivity of Cyber and Physical Security

Being a combined means of strengthening physical security (for instance, studying video footage to identify suspects) and cybersecurity, the system provides a single strategy for safeguarding the organization’s assets.

* Proactive Protection Against External and Internal Threats

Insider threats are identified through human behavior analysis and external threats are identified based on the activity of the endpoint and network traffic. This dual layer of security adds another layer to making the organization more secure.

* Simplified Alert Notifications and Decision-Making

For quicker evaluation and analysis of the trends, it offers a convenient panel for the end-users. It does not present reports and is also more effective for providing real-time alert notifications that allow for quick decision-making in connection with threats.

### **Primary Functionalities**

* 1. Profiling and Threat Identification

The system analyzes diverse types of data streams to detect cybersecurity risks in four perspectives:

* + **Endpoint Data**: All endpoint activity is analyzed to identify instances of unauthorized access.
  + **Physical Security Systems**: Prevents and identifies unauthorized use and theft through services provided by CCTV video and access control records.
  + **Human Behavior**: keeps an eye on employee actions, such as logging in and accessing devices, in an effort to identify insider threats.
  + **Network Traffic**: Regularly scans network traffic streams to detect, for example, DoS or Distributed DoS threats.

Outcome - It helps the organization to prevent the insider as well as the outside threats before they get worse.

* 1. Supervising Endpoint Devices, Networking and Traffic, Physical Security Systems and People’s Actions

The system combines several data streams to provide comprehensive and consistent monitoring:

* **Endpoint Monitoring**: Records system activities, application activity, and device settings to such activities.
* **Network Traffic Analysis**: Network Traffic Analysis and characterization to identify invasive Network activity or Threats.
* **Physical Security Monitoring**: Analyzes Camera feeds in real-time thereby detecting irregularities or any insecurity threats within physical setting.
* **Human Behavior Analysis**: Employee tracking involves tracking their activity such as accessing files, working hours to identify the insiders’ threats.

Outcome - Offer a single, current picture of the security status of the organization, based on analysis of the countries digital systems, physical spaces, and employees for optimal threat protection.

* 1. SOC Teams Useful Information

The system produces clean and valuable analysis from massive amounts of information to help SOC teams make timely decisions.

* + Real-Time Alerts: Inform SOC teams of potential threats.

Outcome-IT can enable SOC teams to focus on delivering more tactical measures instead of having to provide manual efforts in the process, which then lowers response time.

### **Environment and Context:**

Integration of SOC:

The system will be installed in a single large Security Operations Center, or SOC, which will act as the primary nerve center for the organization’s threat monitoring and threat response. It will function together with current SOC tools like:

* Intrusion Detection and Prevention Systems (IDS/IPS): To identify those threats that are already known.
* Endpoint Detection and Response (EDR) Solutions: For improved Endpoint detection.
* Closed Circuit Television (CCTV) and Access Control Systems: Refers to physical security structures.
* Firewalls: For limiting and eradicating the access of unauthorized traffic and for the purpose of tracking the traffic entering and leaving a specific network.

Sources of Data and Interaction:

The system will be capable of extracting data from various sources and-

* + **Endpoint Devices**: Login, system events, usage patterns.
  + **Network Traffic**: Packet captures, flow logs, packet length.
  + **Physical Security Systems**: CCTV video feeds.
  + **Employee Behavior Data**: logon access, device access, access of decoy file

Changing Threat Environments:

The system is able to reduce its effectiveness against new threats by integrating self-learning models to ensure its relevance against new forms of cyber threats.

* **Target Users**

Determine the main users and their requirements:

* 1. **SOC Analysts**

Real-Time Alerts: Alerts of the threats as they occur in end points, traffic, physical security, and people’s actions.

Visualization Dashboards: Simple graphical interfaces that indicate threat patterns, geographical distribution of threats, and recorded occurrence of threats to aid in decision making.

Customizable Alert Rules: This means that the user can set the number of alerts he or she will require and the importance of the alert as per their organization’s operations.

* 1. **System Administrators**

Seamless Integration: Integration with existing tools including firewalls, IDS/IPS, just to mention but a few, and endpoint detection tools.

Ease of Maintenance: A realistic framework for updating threat model, Red Teaming and updating of machine learning and application of patches.

* 1. **Security Researchers**

Flexibility: The flexibility which allows increasing the number of existing models or adding a new one to the system.

Transparency: Information to make model determination and detection rationale available for further study.

* 1. **Incident Response Teams**

Forensic Capabilities: Logs and Alert Notifications, Implements the holding and review of text-based post-event logs and alert messages.

Safety communication capabilities: Real-time alerts keep people on guard and safety, and also aid in audits and compliance checks.

* 1. **Risk Management Teams**

Security alerts: Using security alerts, risks and weakness in the endpoints, networks, physical and people are found.

### **Non-Functional Considerations:**

* Determine the guidelines on creating and developing software in the future by making it available and reliable for continuous monitoring.
* Ingredients like data protection regulations such as GDPR. The system needs to follow regulative standards like GDPR (General Data Protection Regulation) to better define the ethical and secure preservation of user and organization data.
* Cost-effective and easy to modify as well as expand in the future. The system has to be developed in such a manner that it can be justified and expanded in the future and modern technologies can also be incorporated.
  1. **Product perspective**

This section presents the analysis of the NextGen SOC against the backdrop of comparable solutions to outline its major advantages and distinctive features.

Traditional SOC systems are based on specific rules to address security threats and prior defined threat scenarios. Being reactive in nature, these systems are good for known threats that remain unchanged but fail on unknown ones. These solutions usually call for constant manual intervention and delivery of numerous configuration changes to respond to new threats, resulting in higher MLPTs – longer time taken to identify threats and respond to them.

On the other hand, NextGen SOC system incorporates sophisticated machine learning and deep learning to make it more of a smart security platform. It is able to learn from data continuously and even finds out new threats without reinforcement, hence more efficient than traditional systems. Important Differences and Special Qualities:

**Endpoint Data Analysis:**

Traditional Systems - Their monitoring relies mostly on signature-based or behavior-based systems and as such may fail to detect new forms or even newer varieties of malware and suspicious activities.

NextGen SOC - Incorporates Neural Network models with random forest algorithms to improve not only detection but also adaptability.

**Physical Security Systems:**

Traditional Systems - Employ simple motion detection or fundamental video surveillance equipment that do not offer actual time and complicated analysis.

NextGen SOC - Integrates CCTV footage to analyze sequential data in real time. This makes it possible for the system to identify suspicious activities such as theft or intrusions, and notify the security units, in the shortest time. Few-Shot Learning is applied to ensure that the system is configured to detect a few suspicious behaviors within a brief time and with minimal data.

**Human Behavior Analysis:**

Traditional Systems – Ineffective to identify sophisticated insider threats, employing only simple tracking of employees’ behavior against enforced rules.

NextGen SOC - Uses only Random Forest algorithms for human behavior prediction. This model is especially suitable for the identification of the regular employee pattern of activities and communications to detect unusual behavior that may predict insiders.

**Network Traffic Analysis:**

Traditional Systems - Usually employ pattern-based approaches which utilize signature and are not highly effective in identifying complexes.

NextGen SOC - Uses GANs to train a network similar to the cyber-attack scenarios in order to make the system learn and develop new strategies to fight new developing threats. More especially, these include use of models based on neural networks and a decision tree classifier for analyzing real-time traffic data for detecting anomalies.

### 2.1.1. System interfaces

The NextGen SOC system also embodies a reliable set of interfaces wherein it is acceptable to interface the existing structure in an organization. These interfaces facilitate data collection and analysis by the system to work efficiently from various sources:

Operating System Interfaces: The system connects with well-established operating systems like Windows and Linux in order to gather information from endpoints like system logs, application usage and also from the user.

### 2.1.2. User interfaces

The NextGen SOC system provides intuitive and functional user interfaces designed to cater to the needs of different users:

**SOC Dashboard:**

* Provides a live interface to monitor and analyze threats, system notifications, and the Security and Event Management system situation.
* The application also must allow SOC teams to browse through and analyze their organizational network and assets efficiently.
* Users should be allowed to choose certain assets, logs, or network segment for scrutiny with regard to security assurance.
* Within the case of monitored objects, the Application should present the real-time status of entities; highlight the threats or deviations; and give recommendations for an immediate response.

A screenshot of a computer screen

Description automatically generated

Figure 1

**Admin Interface:**

* Login Page and Authentication: The admin interface includes a login page where system administrators are required to type their custom details. The right login credentials give permission to access the system.
* Redirection to SOC Dashboard: Having been authenticated, the administrators are taken to the SOC Dashboard where they can track the live threats and the overall management of security responses.

A screenshot of a login screen

Description automatically generated

Figure 2

### 2.1.3. Hardware interfaces

The NextGen SOC system establishes connections with key hardware components to enable seamless data collection and processing:

1. **CCTV Cameras**: Communicates with surveillance systems to capture live videos for physical security analysis on a real-time basis.
2. **Servers**: Deployed for running computationally heavy deep learning on models together with endpoint, network, and behavioral data.

### 2.1.4. Software interfaces

The NextGen SOC system integrates with various software products to enhance its functionality and compatibility within the organization:

1. **Data Collection Tools**: Connects with endpoint monitoring tools, network traffic analysis tools, human behavior analysis and physical security systems to collate and analyze information from various streams.
2. **Security Tools**: Seamlessly integrate with existing firewalls and intrusion detection/prevention systems (IDS/IPS) to enhance threat detection and response capabilities.

### 2.1.5. Memory constraints

The NextGen SOC system requires sufficient memory resources to support its real-time analysis and data-intensive operations:

1. **RAM**: Sufficient system memory is required here in order to manipulate large datasets and to provide real-time performance of the deep learning models.
2. **Disk Space**: Self-space is needed for model weights, system logs, historical threats and data or any other big data which needs to be processed or stored for further reference.

### 2.1.6. Operations

The NextGen SOC system supports both normal and special operations to ensure comprehensive and adaptive security management:

1. **Normal Operations**:
   * Continuous Monitoring: Endpoint monitoring in real-time, networks, physical security systems, and people.
   * Data Collection: Adding logs, videos, and network details of an occurrence for the purpose of analysis.
   * Threat Analysis and Alerting: Identifying real threats and triggering alarms for the SOC analysts to take required actions.
2. **Special Operations**:

* Model Retraining: Responses to the subsystem by updating detection deep learning models with new data to enhance accuracy.
* Threat Profile Updates: Adapts the current and potential threats in order to minimize new forms of cyber threats.
* Incident Response: Aids in the activities surrounding the incident investigation by generating logs and an analysis of the problem.

### 2.1.7. Site adaptation requirements

The NextGen SOC system is designed to adapt seamlessly to various organizational setups and infrastructures:

1. Network Topologies: Accepts various working topologies, either centralized or distributed, and is adaptable to current network formats.
2. Device Types: Supports all types of computer devices – desktops, servers, laptops, and tablets as well as hardware devices such as CCTV cameras and network routers.
3. Security Policies: Can be tailored to fit individual organizational security policies, regulation, and organizational specific business demands.

## **2.2. Product functions**

Real-Time Threat Detection: For generating an early risk signal, performing deep learning for the detection of anomalies in endpoint data, CCTV footage, network traffic, and behaviors.

 Application:

Endpoint Data: Accomplishes suspicion of unauthorized access tracing logs and system behaviors through the utilization of neural networks.

CCTV Footage: Uses physical security bandwidth and parameters detection to detect, prevent and report theft or intrusion into establishments or similar activities.

Network Traffic: Is able to use a neural network in order to identify complex cyber threats in network traffic.

User Behaviors: Also uses Random Forest algorithms to analyze consolidated employee activities for threat posed by insiders without violating ethical standards.

## **User characteristics**

**SOC Analysts**

* Role: Admins on the front line and agents who are to constantly observe the system, and if there is an intrusion, they are the ones to respond to it.
* Skill Level: A development level of knowledge of tools and techniques in cybersecurity.
* Responsibilities:
  + Review types of alerts and threat information that appear on the system in a real-time display.
  + Apart from this, check out for the abnormalities and categorize the threats into simple, moderate, and complex.
  + Organize the responses to the incidents with the help of the information identified by the system.

**Security Researchers**

* Role: Specialists who investigate the system detection models and concern themselves with new threats.
* Skill Level: Higher level of expertise in the subject areas of machine learning, cyber security, and system weaknesses.
* Responsibilities:
  + The models that may need enhancements include GANs, Random Forest, and neural networks used in detection.
  + Carry out attack scenarios using the system since it is capable of generating synthetic data.
  + Conduct research in order to increase its ability to respond to new threats.

**System Administrators**

* Role: Those most involved in the process of installing, configuring, and sustaining the system are technical staff.
* Skill Level: An expert in IT systems and networks, system integration, networks, and systems integration.
* Responsibilities:
  + Complement the organization by installing and applying the system to its security arrangements (firewalls, IDS/IPS, CCTV systems, etc.).
  + Monitor system health, apply updates, and ensure smooth operation.
  + Manage data back up and policy requirements on privacy.

**Executives and Decision-Makers**

* Role: Persons in charge of the institutional security plan and management of the organization’s security structure.
* Skill Level: System-level knowledge about cyber security and danger control.
* Responsibilities:
  + Endorse acquisitions in system improvements or expansion.
  + Integrate security operations with the goals and standards of the organization or with legal and outsourcing partners.

## **Constraints**

**Data Privacy**

* **Constraint**: While designing such a system, it is mandatory by laws like the GDPR to consider ethical ways to store and process organizational, and user-sensitive data.
  + The personal and behavioral data that are gathered for the study of human behavior must be depersonalized, and the data processing must be secure.
  + Access to the information requires to be controlled by the system and only the relevant staff member should be granted permission to access sensitive information.

**Real-Time Processing**

* **Constraint***:* Real-time threat detection and alerting cannot be compromised by the system’s capability to process massive amounts of data.
* The system analyzes substantial amounts of data originating from endpoints, traffic, cameras, and human actions which need to be processed swiftly, as well as algorithms and pipelines.
* Real-time threats can also guarantee that whenever threats are present, then they are detected immediately, reducing the amount of damage that any threats can cause.

## **Assumptions and dependencies**

**Assumptions**

1. **Availability of Labeled Data for Model Training**:
   * The system assumes having high quality multi-label assessment datasets that are used to build machine learning models such as neural networks, Random Forest as well as GANs.
   * Such datasets are required to track the patterns of illegitimate activity in endpoint data, network traffic, and physical security systems fitfully.
2. **Ongoing Access to Real-Time Data**:
   * The system demands logs, video feeds, human behavior and network traffic data for real-time threat identification and analysis.
   * For this IoT environment of integrated sources such as endpoints, cameras, routers, and others, the data stream should be continuous and non-leaky.
3. **Adequate Computational Resources**:
   * Further assumes that the organization has adequate supply of hard resources like high performance servers GPU for handling deep learning models and large data volumes.
4. **Integration with Existing Security Tools**:
   * Requires mutual compatibility in security tools some of which include security system, IDS, and endpoint protection.
5. **Network Connectivity**:
   * Enterprises Networks are assumed to provide reliable and secure connectivity for data gathering, System interfacing, and interface with outside systems.

**Dependencies**

1. **Organizational Infrastructure**:
   * The system’s effectiveness depends on the organization’s ability to support its deployment, including setting up interfaces with endpoints, network devices, human behavior, and physical security systems.
2. **Regulatory Compliance**:
   * The system depends on adherence to data protection regulations (e.g., GDPR).
3. **Technical Expertise**:
   * The organization must have personnel skilled in managing, maintaining, and customizing the system to meet operational needs.
4. **Data Quality and Availability**:
   * The models rely on timely and accurate data from endpoints, networks, human behavior, and physical security systems. Delays or inaccuracies in data collection can affect performance.

## **Apportioning of requirements**

**Phase 1**: **End point Data Analysis**

Dataset Used: Gather and process endpoint device’s logs and activity data and distinguish normal from anormal.

<https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection?resource=download>

Training Models: Neural Networks and Random Forest models should be trained on this dataset to detect unauthorized access and flag any abnormal system.

Implementation: Use the deployed models to always monitor endpoint data and cause an alert if there is any threat.

**Phase 2**: **Network Traffic Analysis**

Dataset Used: Include normal traffic data and examples of misuse as well as normal and anomalous traffic patterns in the network traffic logs.

<https://www.kaggle.com/code/syedali110/cicd-2017>

Training Models: Use GANs to generate realistic attack traces and further improve the learning of sophisticated, never before seen attacks.

Implementation: Use these models to analyze traffic data from network in real-time basis.

**Phase 3: Physical Security Monitoring**

Dataset Used: Utilized two data sets of video clips from physical security systems with typical (employees enter in the offices) and abnormal (robbery, intruder) behaviors.

<https://www.kaggle.com/datasets/odins0n/ucf-crime-dataset>

Training Models: Utilize Few-Shot Learning methods for training to ensure that the models can be trained all the same despite scarce labeled data.

Implementation: Use these models for monitoring live video streams received from CCTV cameras and raising alarms in case of suspicion.

**Phase 4: Human Behavior Analysis**

Dataset Used: Some sample and features of normal and abnormal behavior include logs of user activities as file access records, system usage records and working hours.

<https://www.kaggle.com/datasets/mrajaxnp/cert-insider-threat-detection-research>

Training Models: Develop Random Forest models to detect Anomaly access on devices, logs, and decoy files.

Implementation:Use the developed models in an online fashion to track employees’ behavior and trigger alarms in case some activity would indicate the existence of an insider threat.

## **2.7 Testing**

* **Unit Testing**

The different components or subsystems or the various functions of the system.

* + Features that can be tested include Real-Time Threat Alerts and Interactive Elements on the SOC Dashboard.
  + Check that the Login Page and Authentication, of all the features inside the Admin Interface are functional.

Example: The application must make sure the login function carries out the check of username and password in the right manner.

Outcome: Ensures that each feature does not have any problems working on its own.

#### **Integration Testing**

Interfacing of numerous parts of the system.

* + Ensure that the Admin Interface seamlessly redirects to the SOC Dashboard after successful login.
  + Verify how different data processing impacts threat updates to check how it is displayed.

**Example**: Assure yourself that once users have been authenticated, they are not delayed or confronted with an error message when they try to enter the SOC Dashboard.

**Outcome**: Carries out effective and efficient transfer of information between the systems.

#### **Security Testing**

The measures put in place of security by this system to keep the data in as well as from outsiders.

* + Ensure that major threat risks are mitigated including SQL Injection, Cross-Site Scripting (XSS) and brute force.
  + Users should implement password policies based on the NIST guidelines, and make sure two factor authentications (2FA) will run properly.

Example: Check the fields on login page to see if they would discard SQL injection attacks.

Outcome: Secures the system to prevent any arbitrary access to information, especially in compliance with the GDPR act.

# **Specific Requirements**

## **3.1. External interface requirements**

### 3.1.1. User interfaces

**SOC Dashboard**

* Purpose: The prime console through which SOC analysts work and get abreast of the day’s security scenario.
* Features:
  + Real-Time Threat Visualization: Shown in real-time, it provides the SOC analysts with visual information of the security threats that are already running and their status.
  + Alerts and Notifications: Displays emergency notices and has features whereby more details regarding the apocalyptic challenges are given.
  + Data Processing Status: Demonstrates where the current position of the data analysis is, which assists the analyst since the system displays its performance and processing status.
  + Insights and Trends: Provides heat map, threat impact level and historical data that can assist the analyst to see pattern when evaluating the threats.
  + Interactive Elements: Options to further refine data visualization according to users’ preferences such as threat type, time limit, or threat level.

**Admin Interface**

Purpose: The Admin Interface is the initial screen displayed to the system administrators of the NextGen SOC system. It enables the administrators to log in and be redirected to the SOC Dashboard for the monitoring and handling of the Security ALERTS and Threats.

Features:

* Login Page: The interface starts from the Point of entry which is the login point where system administrators log in using their credentials to enter the system.
* Authentication: Once the user logs into the system, confirmation of the entered data is performed, and the user is authorized to enter the system.
* Redirection to SOC Dashboard: After successfully passing the authentication, the administrators again reach the SOC Dashboard where he can watch live threat notifications, data assessment as well as responses and actions to maintain security.

### 3.1.2. Hardware interfaces

The NextGen SOC system, therefore, depends on particular hardware elements to facilitate the functions of the SOC system together with information scraping, accumulation, and analysis. These interfaces include:

1. CCTV Cameras:
   * Function: Connects to surveillance systems to get control of live video feeds for instant physical security assessment.
   * Purpose: Records video information that is acted on by the system to identify potential violations or other unusual activities to improve the physical security of the organization.
2. Servers:
   * Function: To execute deep learning models and analyze big data from end points, networks, and users’ actions.
   * Purpose: Aids in the provision of the required processing capabilities to facilitate real-time threat detection and identification as well as the computing capabilities required for performing appropriate computations in real-time.

### 3.1.3. Software interfaces

NextGen SOC system integrates with several software products to improve its Data Collection, Analysis, Threat Intelligence, and Response. This integration ensures compatibility and functionality across the organization's existing infrastructure:

1. **Data Collection Tools**:

Composes data incoming from endpoint security software, network traffic analyzing tools, people behavior recognition software, and physical security systems to give an overall state of organizational security.

Acquires Training data sourced from Kaggle for the machine learning models thereby ensuring that the system can analyze and identify threats.

**Security Tools**:

This makes it possible to record real time traffic on the network, and use the data collected from these security instruments to identify threats and enhance the learning capability of the system.

### 3.1.4. Communication interfaces

This SOC system is the NextGen SOC system that integrates communication interfaces with other systems to ensure that they share data. These interfaces make communications secure, real-time and help the system to facilitate fast and fast data gathering and analysis.

Real-Time Threat Alerts:

* A dashboard that shows active notifications of threats that have been recognized is also used. There is also additional information you can see, for example, the type of threat, its level of threat and source.

## **3.2 Classes/Objects**

**Endpoint Data**

Description: One of this class deals with data that is gathered from computers, mobile devices, and servers, among others.

Purpose: Used for the investigation of carried out activities, logs of the system and application with the purpose of identifying threats such as unauthorized access.

Functionality: Serves as a database for the logs records endpoints.

Identifies abnormal patterns for threat analysis.

Helps in building models for threat identification during live session.

**Physical Security**

Description: Stands for physical security data from physical systems like physical security information from, for instance, CCTV cameras.

Purpose: Recognizes and identifies motions, video feeds, and security data to prevent any dangerous activity in installing physical spaces.

Functionality:

Analyzes video data with the help of predictive algorithms.

They are used in identifying vices such as intrusion or movement that is out of the ordinary.

discharge notifications on the basis of physical security data assessment.

**User Behavior**

Description: Analyzes patterns in user behavior such as system usage, usage of files and interactions in order to identify potential insider threats which act as the model for user behavior.

Purpose: It aids in uncovering abnormality of user’s normal behavior that may be as a result of infiltrators.

Functionality:

Stores information on action performed by users and their overall activity.

In the proposed model, Random Forest model is used to identify normal and anomalous behaviors.

This notifies administrators of any suspicious actions of users in an organization.

**Network Traffic**

Description: Describes information that is a result of analysis of the network devices.

Purpose: Keeps track of the traffic flowing through the network and goes for threats like DDoS attacks in the process.

Functionality:

It includes network monitoring and analysis of relevant real time traffic issues.

Examines patterns which are peculiar based on the Machine Learning model such as the decision tree classifier and neural network.

Creates alarms for security threats when recognized in network traffic.

## **3.3 Performance requirements**

* 1. Response Time
* It should also be capable of identifying and analyzing threats to the organizational environment on-line as soon as possible.
* In order to prevent and eradicate threats within the organization, the system should be able to receive constant data feeds from end points, network traffic, human activity, physical security devices and systems and immediately produce alarms and analysis that it conveys without latency.
* Processing of data, detection of anomalies and generation of alert should preferably occur a few seconds after data has been entered.
  1. Scalability
* It must be able to scale up that means it must be capable of managing data processing from thousands of endpoints and devices.
* It should also be easy for the system to scale up as the organization generating the data becomes larger. This scalability guarantees that the access of logs, network traffic data, and video streams does not slow down the system.
* The system should be able to process and issue alerts in real-time and that should be possible as the number of endpoints and devices connected to it increases.
  1. Accuracy
* The desired performance of the machine learning models is high accuracy of insider and outside threats detection.
* The system should be trained with datasets from Kaggle as it is one of the most famous platforms for high quality and variety datasets. This guarantees that the models are refined and able to identify threats in different situations including new and unique kinds of attacks.

## **3.4. Design constraints**

**Default Credentials and Initial Login**

* Constraint: During the purchase of the platform, the vendor assigns a standard login and password for the first connection to the system.
* User Implementation:
  + Initial Login: In the first connection successfully made by SOC analysts to the system, they connect it using the vendor default credentials.
  + Password Change: The reader is logged in to the system from where he is directed to immediately change the default password for security’ This step is compulsory before the users can go further to using the system.
* Outcome: Strengthens security by guaranteeing that the initial access credentials are changed, so that an unauthorized person cannot use the system.

**System Access and Dashboard Navigation**

* Constraint: The default password needs to be changed and on the second time the users need to be transferred to the SOC Dashboard.
* User Implementation:
  + Accessing the Dashboard: After entering the account with "strong authentication,” SOC analysts are transferred to their dashboard where they have the following security components at their disposal.
  + Dashboard Components: The SOC Dashboard includes four main sections:
    - Network Traffic Analysis: Responsible for observing activity on the network in an attempt to detect something unusual or threatening.
    - Endpoint Analysis: Identifies security threats on an endpoint device after collecting data from the device in question.
    - Physical Security Analysis: Analyzes data from the physical security system, for instance CCTV to consider any suspicious activity.
    - Human Behavior Analysis: In this section, it is used to track user behavior in order to identify signs of an insider threat.
* Outcome: Facilitates access by analysts to all the fundamental security operations, in one workspace for efficient oversight.

**Analysis and Threat Detection**

* Constraint: The system should be able to accept input information more on human behavior analysis in order to identify insider threats.
* User Implementation:
  + Input Requirements: Now, users are required to feed information including the user activity profile, device access, activity and behavior metrics that will be utilized in the system.
  + Threat Detection: The system trains models for analyzing the profiles of user-deviations and if any threats are noticed then the SOC team is informed.

Alert Notifications: When the system identifies suspicious behavior that would suggest a security threat, then it produces real-time alarms that are sent to the SOC analysts.

* Outcome: Ensures that insider and outsider threats are detected accurately, allowing the SOC team to take timely action to mitigate risks.

## **3.5. Software system attributes**

### 3.5.1. Reliability

The system has to be reliable to meet necessary demands for its constant work in detecting and analyzing threats.

The system should be more available than traditional tools, which would ensure a consistently low-down time for real time threat analysis and mitigation. This much reliability ensures that a system is reliable, and it will successfully execute all its tasks in most circumstances.

### 3.5.2. Availability

The system should be online at all times to monitor and analyze the security of an organization.

The system should always enable the security teams to analyze, monitor and receive real-time threat data, alerts, or analytics.

### 3.5.3. Security

1.SOC Analyst Authentication Scenario

Explanation: The system should afford secure authentication for SOC analysts so that only those can access it.

Implementation:

* + Password Policies: The passwords have to meet the guidelines developed by NIST which include:
    - At least eight characters that include all the caps and lowercase letters, number, and symbol.
    - Periodic Password Updates and no usage of old password.
    - Brute force attacks countermeasures such as putting a temporary lock on the account after some incorrect log in attempts.
* Two-Factor Authentication (2FA): The system should support 2 FA in which a user is required to answer security questions or other forms of security checking before being granted access.

1. Input Field Validation

Explanation: All input elements that are used by a user should be checked to avoid such attacks as injections and correct input data.

Implementation:

* + SQL Injection Prevention: For there to be no possibilities of SQL injections, all input fields should apply querying parameters and prepared statements.
  + Cross-Site Scripting (XSS) Prevention: To address XSS attack by which attacker insert evil scripts in webpage, apply input anti summary and output obfuscation measures.
  + Validation Mechanisms: Implement non-standardized but reliable ready-to-use libraries or code of validation and filtering, employ strict varieties of coding for data entry and scanning in real-time.

1. Data Protection and GDPR Compliance

Explanation: The system has to safeguard the organizational data as prescribed by GDPR and avoid any unauthorized data leaks.

Implementation:

* + Access Controls: Restrict access by enforcing the usage of RBAC. This means that only those who are authorized should access certain data.
  + Data Minimization: The use of the system must be the only means for data collection and must also take precautions to avoid storing personal information.
  + Compliance Audits: Regular security audits and compliance checks to confirm that data handling practices meet GDPR requirements.
  + Incident Response: Data breach response plan will ensure prompt action in case of a breach, with procedures for notifying affected parties in accordance with GDPR rules.

### 3.5.4. Maintainability

The structures patterns should be integrated in such a system where individual segments can be modified regularly for enhancing the model, and other additional features like enhanced security threats.

The system should be designed in such a manner that inclusion of new detection models, incorporation of new data inputs and management of system parts and modules should not be a cumbersome task.

## **3.6. Other requirements**

To ensure the security of data, the given system has to conform to industry standards of security regulations and security practices.

Industry Standards: The security could be composed to meet the security standards needed, that includes:

* Information security management according to ISO/IEC 27001.
* Management Of cybersecurity risks with help of NIST Cybersecurity Framework.
* GDPR (General Data Protection Regulation**)** for data protection and privacy of individuals within the EU.
* Regular Audits: Some specific recommendations for the systematic compliance of the system include the following: Standing the compliance audit point for the system so that it can reflect on the requirements standardly herein and revised from time to time depending on the emerging regulations.
* Documentation and Reporting: Keep records of the compliance filed data handling processes and security measures to support audits and reporting systems.

# **References**

A. Manoharan and M. Sarker, “REVOLUTIONIZING CYBERSECURITY: UNLEASHING THE POWER OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR NEXT- GENERATION THREAT DETECTION,” *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, pp. 2151–2164, Apr. 2022.

R. Kaur, D. Gabrijelčič, and T. Klobučar, “Artificial intelligence for cybersecurity: Literature review and future research directions,” *Information Fusion*, vol. 97, p. 101804, 2023, doi: https://doi.org/10.1016/j.inffus.2023.101804.

E. Sodiya, A. Atadoga, U. Umoga, and O. Amoo, “A comprehensive review of machine learning’s role in enhancing network security and threat detection,” *World Journal of Advanced Research and Reviews*, vol. 21. Apr. 2024. doi: 10.30574/wjarr.2024.21.2.0501.

J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, “Cyber-physical systems security: Limitations, issues and future trends,” *Microprocess Microsyst*, vol. 77, Sep. 2020, doi: 10.1016/j.micpro.2020.103201.

H.-T. Duong, V.-T. Le, and V. T. Hoang, “Deep Learning-Based Anomaly Detection in Video Surveillance: A Survey,” *Sensors*, vol. 23, no. 11, 2023, doi: 10.3390/s23115024.

B. Bin Sarhan and N. Altwaijry, “Insider Threat Detection Using Machine Learning Approach,” *Applied Sciences*, vol. 13, no. 1, 2023, doi: 10.3390/app13010259.

A. Kumar, “Cybersecurity Threat Detection using Machine Learning and Network Analysis,” *Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023*, vol. 1, pp. 38–46, Apr. 2024, doi: 10.60087/jaigs.v1i1.p46.

A. Papanikolaou, A. Alevizopoulos, C. Ilioudis, K. Demertzis, and K. Rantos, “A Blockchained AutoML Network Traffic Analyzer to Industrial Cyber Defense and Protection,” *Electronics (Basel)*, vol. 12, no. 6, 2023, doi: 10.3390/electronics12061484.

A. Alraizza and A. Algarni, “Ransomware Detection Using Machine Learning: A Survey,” *Big Data and Cognitive Computing*, vol. 7, no. 3, 2023, doi: 10.3390/bdcc7030143.

M. Atti and M. Yogi, “Application of Deep Reinforcement Learning (DRL) for Malware Detection,” *International Journal of Information technology and Computer Engineering*, vol. 4, pp. 23–35, Apr. 2024, doi: 10.55529/ijitc.43.23.35.

H.-M. Chuang and L.-J. Ye, “Applying Transfer Learning Approaches for Intrusion Detection in Software-Defined Networking,” *Sustainability*, vol. 15, p. 9395, Apr. 2023, doi: 10.3390/su15129395.

V. Ravi *et al.*, “Deep Learning for Cyber Security Applications: A Comprehensive Survey.” Apr. 2021. doi: 10.36227/techrxiv.16748161.

L. Frank, “Edge AI: Deploying models directly on edge devices for real-time processing,” *Artif Intell*, Apr. 2024.

L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, “Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review,” *Sensors*, vol. 23, no. 3, 2023, doi: 10.3390/s23031151.

S. Z. El Mestari, G. Lenzini, and H. Demirci, “Preserving data privacy in machine learning systems,” *Comput Secur*, vol. 137, p. 103605, 2024, doi: https://doi.org/10.1016/j.cose.2023.103605.

T. Mazhar *et al.*, “Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods,” *Future Internet*, vol. 15, no. 2, 2023, doi: 10.3390/fi15020083.

P. Tam, S. Ros, I. Song, S. Kang, and S. Kim, “A Survey of Intelligent End-to-End Networking Solutions: Integrating Graph Neural Networks and Deep Reinforcement Learning Approaches,” *Electronics (Basel)*, vol. 13, no. 5, 2024, doi: 10.3390/electronics13050994.

N. Jahan, G. Bajwa, and T. Akilan, “Federated Learning-assisted Self-supervised CNN for Monkeypox Diagnosis,” in *2023 IEEE Western New York Image and Signal Processing Workshop (WNYISPW)*, 2023, pp. 1–5. doi: 10.1109/WNYISPW60588.2023.10349384.