Not Original

SLIIT UNI

THE KNOWLEDGE UNIVERSITY

**IT4010 – Research Project - 2024**

**Topic Assessment Form**

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

1. Topic (12 words max)

| |
|---|
| DEEP LEARNING APPROACHES TO PROFILING ORGANIZATIONAL THREATS – NEXTGEN SOC |

2. Research group the project belongs to

| |
|---|
| **Computing Infrastructure and Security (CIS)** |

3. Research area the project belongs to

| |
|---|
| **Cyber Security (CS)** |

4. If a continuation of a previous project:

| | |
|---|---|
| Project ID | |
| Year | |

5. Brief description of the research problem including references (200 – 500 words max) – references not included in word count.

Organizational security is facing a huge challenge from the increasing complexity and sophistication of cyber attacks. As a result, Security Operations Centers (SOCs) have had to transform into NextGen SOCs, which use cutting-edge technology to improve threat detection, analysis, and mitigation. Despite the potential of deep learning to revolutionize cybersecurity practices, its application within organizational contexts, particularly in profiling threats across various dimensions including endpoint data, physical security systems, human behavior, and network traffic faces several multifaceted challenges.

- Integration and Interpretation of Heterogeneous Data Sources: One of the primary challenges is the integration of diverse data sources, such as endpoint logs, video surveillance footage, employee behavior data, and network traffic, into a cohesive deep learning framework. Each data type presents unique preprocessing, normalization, and interpretation challenges, complicating the development of unified models capable of leveraging this data to profile threats accurately [1].
- Dynamic Nature of Cyber Threats: The continuous evolution of cyber threats necessitates adaptive and evolving deep learning models. Traditional models may quickly become obsolete as new threat vectors emerge. Developing models that can learn from new data, adapt to changing patterns, and predict unknown threats remains a significant challenge [2].

- Scalability and Real-time Processing: Given the vast volumes of data generated by organizations, deep learning models must not only be accurate but also scalable and capable of processing data in real time or near-real time. Ensuring these models can operate efficiently without significant delays or resource overhead is crucial for their practical application in SOCs [3].
- Ethical and Privacy Considerations in Human Behavior Analysis: Applying deep learning to human behavior analysis for insider threat detection raises significant ethical and privacy concerns. Balancing the need for security with respect for individual privacy and ensuring models are free from bias and respect ethical guidelines is a complex challenge that must be addressed [4].
- Interoperability with Existing Security Infrastructure: Integrating deep learning-based threat profiling tools with existing security infrastructure without disrupting operational processes or requiring extensive overhauls poses logistical and technical challenges. Ensuring these new tools can communicate with and enhance existing systems is crucial for seamless adoption [5].
- Lack of Standardized Benchmarks and Evaluation Metrics: The absence of standardized benchmarks and evaluation metrics for deep learning models in the context of threat profiling makes it difficult to assess their effectiveness, compare them against traditional methods, or even evaluate their readiness for deployment in operational environments [5].

## References

[1] J. X. Gao, "Integrating Heterogeneous Datasets by Using Multimodal Deep Learning," 2020.

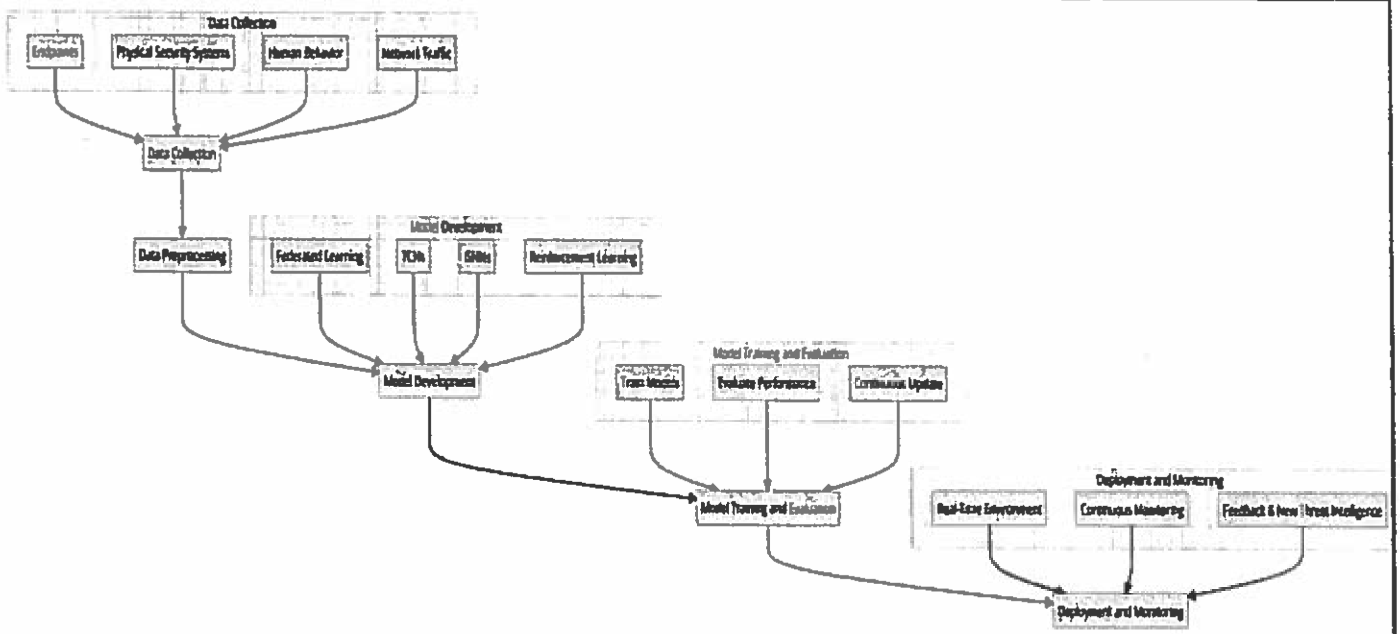
[2] N. V. V. M. T. Naresh Thaneeru, "Adaptive generative AI for dynamic cybersecurity threat detection in enterprises," 2024.

[3] "3 Main Challenges With ML Model Scalability," Deepchecks, 05 February 2024. [Online].

[4] G. T. M. M. Patrick Düssel, "Ethical Issues of User Behavioral Analysis through Machine Learning," 2017.

[5] X. W. Shuhan Yuan, "Deep Learning for Insider Threat Detection: Review, Challenges," 2020.

6. **Brief description of the nature of the solution including a conceptual diagram (250 words max)**




The following is a structure of a more complete framework of data-driven security systems. The process starts with Data Collection: endpoints, physical security systems, human behavior, network traffic, This collected data is preprocessed to make sure that it is clean and can be used for further analysis.

Federated Learning, Temporal Convolutional Networks (TCNs), Graph Neural Networks (GNNs), Reinforcement Learning, and more black-box model architectures in the Model Development phase. These methodologies serve different purposes in the realm of data analytics and prediction.

Then, the models go through the Model Training and Evaluation phase; they all are trained well tested for their performance. This then feeds into active model learning, which is a process of continuous updates that keeps the model working and adjusting to changing data patterns.

The models are then Operationalized and deployed as Real-Time Environment for monitoring live. This is an important stage as it includes the Continuous Monitoring and Feedback & New Threat Intelligence Integration to improve the model constantly.

The Deployment and Monitoring phase completes the life cycle by preserving the integrity of the built system and keeping it on alert to new threats to keep the environment secure through continuous vigilance and change.

This approach built with this structure means that the security system will not be just responsive & adaptive but also will be proactive through the use of advanced machine learning and real-time data monitoring to secure the threats in-place for optimal performance.

7. Brief description of specialized domain expertise, knowledge, and data requirements (300 words max)

**Endpoint Data:**

- **Expertise:** Design and implement adaptive neural networks that can change as soon as threats adapt or benign software updates. This calls for an intuitive comprehension of federated learning and self-supervised learning to tackle such issues and concerns about privacy and sensitivity of data.
- **Knowledge:** Development of novel few shot learning and transfer learning methods enabling models to generalize to new environments with very little data.
- **Data Requirements:** Aggregate endpoint data, including system logs, application behavior, and user interactions, and ensure data is anonymized and normalized for standardization.

**Physical Security Systems:**

- **Expertise:** Structure real-time deep learning-based analysis frameworks with edge processing to piece together systems like CCTV for prompt threat scanning. In practice, this means combining few-shot learning with Temporal Convolutional Networks (TCNs) for time-series video feed data treatment.
- **Knowledge:** Need to know to identify algorithms for image recognition and anomaly detection to make real-time predictions about whether behavior is normal or suspicious.
- **Data Requirements:** Real-time video footage and access logs from physical security systems, processed near the data source to enable faster alert times Data Specifications.

**Human Behavior Analysis:**

- **Expertise:** Prototype of privacy-preserving deep learning for identifying possible insider threats from anonymized aggregated behavior data It also presents differential privacy and graph neural networks (GNNs).
- **Knowledge:** Understanding workplace laws and concepts on AI exploiting human behavior, meeting standards and codes of ethics in the industry.
- **Data Requirements:** behavioral data that has been aggregated and anonymized, with controls in place to protect personal information, and is used to identify patterns that may point to insider threats.

**Network Traffic Analysis:**

- **Expertise:** Usage of graph neural networks (GNNs). and Deep Reinforcement Learning techniques to perform real-time network traffic analytics. Creating and training these neural nets requires an understanding of how components interact in network environments.
- **Knowledge:** Reinforcement learning and Generative Adversarial Networks (GAN) to autonomously adjust to new network attack vectors and test unique attack strategies.
- **Data Requirements:** Network traffic data, analyzed in real-time so that the solution can properly identify and react to growing cyber threats quickly.

8. Objectives and Novelty

| Main Objective |
|---|
| The primary goal of this project is to develop and implement novel deep learning models that protect privacy for holistic threat dissemination in Security Operations Centers (SOCs). These models will be used to analyze network traffic, endpoint data, physical security systems, and human behavior to improve overall organization security while adhering to ethical and privacy standards. The development of flexible and scalable models is prioritized in order to address the complex and evolving trends of cyberthreats, guarantee seamless integration with the current security infrastructure, and others. |

| Member Name | Sub Objective | Tasks | Novelty |
|---|---|---|---|
| Ashra M.F.F. | Threat Profiling with Endpoint Data | **Data Collection and Preprocessing:**<br>• Log Access points e.g., system logs, application behavior, user interactions.<br>• Protect User Privacy through Anonymized Data.<br>• Cleaning and separating data (Removing irrelevant features & normalizing inputs) | **Federated Learning System:**<br>• permits endpoint devices to cooperatively learn a common detection model.<br>• To handle privacy issues and data sensitivity, all training data is kept on the device.<br><br>**Self-Supervised Learning** |

| | | | |
|---|---|---|---|
| | | **Model Development:**<br><br>• Train a decentralized model — (Federate learning without raw data exchange)<br>• Mandate self-supervised learning algorithms: make labels out of data.<br><br>**Model Training and Evaluation:**<br><br>• Train model on subset dataset across endpoints.<br>• Train and evaluate model over validation set using accuracy, precision, recall, and F1 score.<br>• Need to refresh the model with new data to ensure the model is up-to-date and understand the most recent threats.<br><br>**Deployment and Monitoring:**<br><br>• The model can be deployed to various endpoints now that it has been saved and trained.<br>• Indicators should be | **Mechanisms:**<br><br>• Enables the model to gain knowledge from the data's inherent structure.<br>• Makes it possible for the model to identify new risks without requiring large amounts of labeled datasets. |

| | | | |
|---|---|---|---|
| | | tracked over time and thresholds adjusted to maximize sensitivity and specificity.<br>• Create a feedback loop for ongoing tuning of the model to achieve success, and additional threat intel. | |
| Gunawardhana K.P.A.T. | Threat Profiling with Physical Security Systems | **Video Data Collection and Preprocessing:**<br>• Import CCTV footages from dataset and extract frames from videos.<br>• Use a pre-trained CNN model (e.g., VGG16, ResNet) to extract features from each frame.<br>**Model Development:**<br>• Create a model with few-shot learning integrated for quick response to new threats.<br>• Sequences of video frames can be analyzed using Temporal Convolutional Networks (TCNs) to identify suspicious activity over time. | **Few-Shot Learning:**<br>• Allows models to be quickly adjusted to new security risks with few instances.<br>• Especially appropriate for CCTV footage analysis in cases when specific threat situations are uncommon.<br>**Temporal Convolutional Networks (TCNs):**<br>• Excel is a powerful tool for handling time-series data, such as sequential video feed frames. |

| | | | |
|---|---|---|---|
| | | **Training and Real-time Analysis:**<br>• Use the annotated dataset to train the model.<br>• Apply the real-time video feed analysis methodology into practice.<br>• To reduce latency, process data on-site using edge computing.<br>**Evaluation and Iteration:**<br>• Using measures for detection latency, recall, and precision, evaluate the model's efficacy in real-time threat identification.<br>• Iterate the model in response to feedback on performance and new security requirements. | • Over time, improve the identification of suspicious activity, which will support strong real-time threat detection. |
| Senevirathna D.H. | Threat Profiling through Human Behavior Analysis | **Data Collection with Privacy Preservation:**<br>• Collect aggregated and anonymized data about the | **Differential Privacy:**<br>• Ensures the protection of personal privacy for |

| | | | |
|---|---|---|---|
| | | interactions and activities of employees.<br>• To protect individual privacy, use differential privacy approaches.<br><br>**Graph Model Development:**<br><br>• Model complex connections and interactions in the data by using Graph Neural Networks (GNNs).<br>• Identify trends that point to insider threats.<br><br>**Model Training and Validation:**<br><br>• Use the dataset with privacy protected to train the GNN model.<br>• Verify performance against known cases of harmless behavior and insider threats.<br><br>**Deployment and Continuous Learning:**<br><br>• Use the model to do | deep learning algorithms that analyze employee behavior data.<br>• Allows combining findings without compromising the privacy of specific personal information.<br><br>**Graph Neural Networks (GNNs):**<br><br>• The intricate relationships and interactions between models inside organizational networks.<br>• Enhances the detection of insider threats by offering a greater understanding of behavioral patterns. |

| | | | |
|---|---|---|---|
| | | continuing analysis.<br>• Provide procedures for continual learning and adjustment in response to novel behaviors and identifying risks while upholding privacy standards. | |
| Gunasekara W.M.M. | Threat Profiling with Network Traffic Analysis | **Network Data Collection and Simulation:**<br>• Collect data about network traffic.<br>• Train new cyber threat patterns using Generative Adversarial Networks (GANs).<br>**Reinforcement Learning Model Development:**<br>• Create a model for reinforcement learning that communicates with the network environment.<br>• By offering rewards based on timely and accurate threat detection, organizations may show workers to see threats. | **Reinforcement Learning:**<br>• Allows dynamic adjustment in response to changing network risks by means of ongoing communication with the network environment.<br>• Allows the model to gradually learn the best practices for detecting and mitigating threats.<br>**Generative Adversarial Networks (GANs):**<br>• Improves the model's detection |

| | | | |
|---|---|---|---|
| | | **Model Training and Evaluation:**<br><br>• Real-world network data and threat simulations are used to train the model.<br>• Determine performance by comparing the response time, false positive rate, and detection rate.<br><br>**Operational Integration and Feedback Loop:**<br><br>• Include the model in the network analysis tools provided by the SOC.<br>• Track performance in real-time.<br>• Modify the model in response to feedback from threats and false positives identified. | capability of complex cyberthreats by simulating new attack tactics during training.<br>• provides more realistic and various adversarial examples, which enhances adaptation to newly threats. |

| IT4010 – Research Project - 2024 |
|---|
| Topic Assessment Form |

9. Supervisor checklist

a) Does the chosen research topic possess a comprehensive scope suitable for a final-year project?

| Yes | ✓ | No | |
|---|---|---|---|

b) Does the proposed topic exhibit novelty?

| Yes | ✓ | No | |
|---|---|---|---|

c) Do you believe they have the capability to successfully execute the proposed project?

| Yes | ✓ | No | |
|---|---|---|---|

d) Do the proposed sub-objectives reflect the students' areas of specialization?

| Yes | ✓ | No | |
|---|---|---|---|

e) Supervisor's Evaluation and Recommendation for the Research topic:

GOOD.

10. Supervisor details

| | Title | First Name | Last Name | Signature |
|---|---|---|---|---|
| Supervisor | DR. | HARINDA | FERNANDO | |
| Co-Supervisor | Mr. | Kavinga | Yapa | |
| External Supervisor | | | | |
| Summary of external supervisor's (if any) experience and expertise | | | | |

THE KNOWLEDGE UNIVERSITY

**IT4010 – Research Project - 2024**

**Topic Assessment Form**

**This part is to be filled by the Topic Screening Panel members.**

**Acceptable:** Mark/Select as necessary

| | |
|---|---|
| Topic Assessment Accepted | |
| Topic Assessment Accepted with minor changes (should be followed up by the supervisor)* | ✓ |
| Topic Assessment to be Resubmitted with major changes* | |
| Topic Assessment Rejected. Topic must be changed | |

* Detailed comments given below

**Comments**

Component 1 plan how FL is going to be used within your component.

Component 2 ensure the dataset ~~th~~ has the features expected from the research. Proposed novelty is not clear.

OK.

**The Review Panel Details**

| Member's Name | Signature |
|---|---|
| Mr. Kavinga Yapa | |
| Mr. Kanishka Yapa | |
| Ms. Chethana Liyanapathirana | |
| | |
| | |
| | |

***Important:**

1. According to the comments given by the panel, make the necessary modifications and get the approval by the **Supervisor** or the **Same Panel.**
2. If the project topic is rejected, identify a new topic, and follow the same procedure until the topic is approved by the assessment panel.