A SYNOPSIS ON

AI Powered Cyber Threat Detection System

Submitted in partial fulfilment of the requirement for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE & ENGINEERING

Submitted By:

Sandarbh Singhal	**2119108**	**Sec-J**
Ujjwal Bisht	**2119108**	**Sec-E**
Ujjawal Singh Tolia	**2119355**	**Sec-J**
Saurabh Painuly	**2119144**	**Sec-J**

Under the Guidance of

Mr. Saksham Mittal

Department of Computer Science and Engineering

Graphic Era Hill University

Dehradun, Uttarakhand

September 2024

Graphic Era
HILL UNIVERSITY
Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)
University under section 2(f) of UGC Act, 1956

CANDIDATE'S DECLARATION

We hereby certify that the work which is being presented in the Synopsis entitled "**AI Powered Cyber Threat Detection System**" in partial fulfilment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science and Engineering in the Department of Computer Science and Engineering of the Graphic Era Hill University, Dehradun shall be carried out by the undersigned under the supervision of

Mr. Saksham Mittal, Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun.

Sandarbh Singhal	**Graphic Era Hill University**	**2119108**	**Sec-J**
Ujjwal Bisht	**Graphic Era Hill University**	**2119357**	**Sec-E**
Ujjawal Singh Tolia	**Graphic Era Hill University**	**2119355**	**Sec-J**
Saurabh Painuly	**Graphic Era Hill University**	**2119144**	**Sec-J**

The above mentioned students shall be working under the supervision of the undersigned on the "**AI Powered Cyber Threat Detection System**"

SAKSHAM MITTAL

Supervisor **Head of the Department**

Chapter 1

Introduction and Problem Statement

Cybersecurity threats are growing in complexity, frequency, and scale. As organizations expand their digital footprints, traditional manual threat detection methods have become inefficient and insufficient to keep up with the evolving landscape of cyberattacks. These threats, including data breaches, malware, and unauthorized access, often go undetected until significant damage is done. To address this challenge, the **AI Powered Cyber Threat Detection System** aims to detect anomalous network traffic or security breaches in real-time using machine learning models. By leveraging AI, the system provides rapid identification of potential threats, reducing the response time and mitigating the risk of damage.

This solution is designed to scale with growing data volumes, providing enhanced visibility and control over network security.
The system will serve as a proactive defence mechanism, reducing reliance on manual detection while improving response time and efficiency in mitigating cybersecurity risks.

Chapter 2

Background/ Literature Survey

The rise of cyber threats has led to significant research in AI-driven cybersecurity solutions. Several anomaly detection techniques, ranging from simple statistical methods to advanced machine learning algorithms, have been explored in recent years. Neural networks, reinforcement learning, and unsupervised learning models have shown promise in identifying patterns that deviate from normal network behaviour. Traditional cybersecurity solutions focus on predefined threat signatures, which often fail to detect novel or evolving attacks. Machine learning models offer an advantage by learning from historical network data, allowing for the detection of unknown or previously unseen threats.

Studies have shown that unsupervised learning methods, like clustering or autoencoders, can detect zero-day attacks, while supervised learning approaches, such as neural networks, have been employed for specific threat types. Research also points to the need for real-time analysis, given the high-speed nature of modern cyberattacks.

Key research papers in the field:

1. "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges" by García-Teodoro et al. (2009).
2. "A Survey on Machine Learning for Cybersecurity: Algorithms, Datasets, and Practices" by Apruzzese et al. (2020).
3. "Deep Learning Models for Cybersecurity: A Survey and Critical Review" by A. Roy et al. (2021).

Chapter 3

Objectives

1. **Real-Time Detection**: Build a system that can analyse network traffic in real-time and flag anomalous activities indicating potential security breaches.
2. **Scalability**: Design the system to scale with large datasets, ensuring performance remains consistent as network traffic grows.
3. **AI Integration**: Leverage unsupervised learning algorithms to detect unknown, zero-day threats without relying on predefined signatures.
4. **User-Friendly Interface**: Develop a React.js-based dashboard that provides network administrators with real-time alerts, detailed threat reports, and visualization tools.
5. **Efficient Threat Mitigation**: Ensure the system provides actionable insights that allow for swift threat resolution, minimizing potential damage.

Chapter 4

Hardware and Software Requirements

Hardware Requirements:

1. **Processor**: Minimum Intel i5 or AMD equivalent for local deployment; multi-core processors recommended for large datasets.
2. **RAM**: 8 GB minimum for development; 16 GB or higher recommended for deployment.
3. **Storage**: SSD with 100 GB minimum for data logs and system logs; scalable cloud storage recommended for large datasets.
4. **Network**: High-speed Ethernet or Wi-Fi for seamless data transfer and real-time monitoring.

Software Requirements:

1. **Frontend**:
    - React.js for developing the user interface.
    - Axios for API integration.
2. **Backend**:
    - Python for machine learning model development.
    - Flask/Django for building APIs to integrate models with the frontend.
3. **Database**:
    - MongoDB or PostgreSQL for storing network logs, threat reports, and user data.
4. **Machine Learning Libraries**:
    - TensorFlow or PyTorch for neural networks.
    - Scikit-learn for anomaly detection models.
5. **Operating System**: Linux (Ubuntu) for backend; cross-platform compatibility for the frontend.
6. **Version Control**: Git for source code management.

Chapter 5

Possible Approach/ Algorithms

The AI Powered Cyber Threat Detection System will employ machine learning algorithms tailored for detecting anomalies in network traffic. The following approaches will be explored:

1. **Unsupervised Learning**:
    - **Autoencoders**: These will be used to reconstruct normal network traffic patterns. Any significant deviation from the normal reconstruction is flagged as an anomaly.
    - **K-Means Clustering**: This method will cluster similar traffic patterns together, flagging outliers as potential threats.
    - **Isolation Forest**: This algorithm isolates anomalies rather than profiles normal behaviour, making it useful for real-time anomaly detection in network traffic.

2. **Supervised Learning** (for specific threat types):
    - **Convolutional Neural Networks (CNNs)**: Used for detecting patterns in time-series data, such as network packet sequences, to identify common attack vectors.
    - **Reinforcement Learning**: Can be applied to adaptively monitor network environments and respond to emerging threats based on reward feedback mechanisms.

3. **Hybrid Approach**:
    - A combination of both unsupervised and supervised learning models will be integrated for enhanced detection accuracy. The unsupervised models will detect previously unseen attacks, while supervised models will identify known patterns based on labelled data.

References

1. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). "Anomaly-based network intrusion detection: Techniques, systems and challenges". *Computers & Security*, 28(1-2), 18-28.

2. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2020). "A Survey on Machine Learning for Cybersecurity: Algorithms, Datasets, and Practices". *Computers & Security*, 96, 101916.

3. Roy, A., Cheema, P., & Namuduri, K. (2021). "Deep Learning Models for Cybersecurity: A Survey and Critical Review". *IEEE Access*, 9, 99190-99226.