**SUPPLY CHAIN VULNERABILITY ANALYSIS AND PREDICTION**

**Team Members**:

Team Member 01

Name : Varshini M

SRN : PES1UG22CS678

Email id : [varshu1102225@gmail.com](mailto:varshu1102225@gmail.com)

Team Member 02

Name : Srishti Mathur

SRN : PES1UG22CS614

Email id : [srishmath123@gmail.com](mailto:srishmath123@gmail.com)

**Abstract:**

Supply chain attacks pose significant risks to organizations, particularly impacting cloud environments indirectly. This research paper explores the intricate relationship between supply chain attacks and their ramifications on cloud services.

Firstly, it discusses how vulnerabilities introduced through compromised suppliers can propagate into cloud infrastructures, affecting the confidentiality, integrity, and availability of data and services. Historical data analysis of supply chain attacks reveals patterns and trends, emphasizing the increasing sophistication and frequency of such incidents targeting third-party applications used by cloud customers. Understanding these historical trends helps in identifying evolving attack vectors and enhancing pre-emptive security measures. The vulnerabilities are categorized according to various elements of cloud infrastructures, accompanied by in-depth examinations of particular vulnerabilities within each element, thus improving comprehension of specific areas of vulnerability.

Additionally, the research includes the analysis of any possible vulnerabilities present in the package.json files associated with Node.js projects, providing corresponding visualizations to help in a broader understanding and effective mitigation. Through these analyses and predictive insights, organizations can strengthen their defences against supply chain vulnerabilities, safeguarding their cloud infrastructures, and maintaining trust among users and stakeholders.

Furthermore, this paper proposes a predictive model using Support Vector Classification (SVC) to assess the severity of supply chain attacks. By leveraging machine learning algorithms, the model evaluates attack attributes and contextual factors to predict the severity of the attack, aiding proactive risk management strategies.

**Novelty:**

1. Detailed Exploration of Supply Chain Attacks:

Comprehensive analysis of how vulnerabilities from compromised suppliers impact cloud infrastructures, focusing on the confidentiality, integrity, and availability of data and services.

1. Historical Data Analysis:

Identification of trends and patterns in supply chain attacks through historical data, highlighting the increasing sophistication and frequency of these incidents.

1. Classification of Vulnerabilities:

Classification of vulnerabilities based on different components of cloud infrastructures, with detailed discussions on specific vulnerabilities in each component, enhancing the understanding of specific areas of risk.

1. Node.js Package Vulnerability Analysis:

Analysis of vulnerabilities present in the package.json files associated with Node.js projects. This includes providing visualizations that facilitate a broader understanding of the vulnerabilities.

1. Predictive Modelling:

Introduction of a predictive model using Support Vector Classification (SVC) to evaluate the severity of supply chain attacks based on attack attributes and contextual factors. This model aids in proactive risk management and enhances pre-emptive security measures.

1. Mitigation Techniques:

Provision of mitigation techniques based on the predictions from the SVC model. This ensures that organizations not only understand potential vulnerabilities but also have actionable steps to address them.

Tools:

* Support Vector Classification (Machine Learning Model)
* Pandas
* Matplotlib
* HTML
* CSS
* Flask