**A picture containing text

Description automatically generated**

Concordia Institute for Information System

Engineering (CIISE)

INSE 6610

Cybercrime Investigation (Summer 2023)

**Project Proposal on**

Log analysis for intrusion detection/investigation. Techniques using machine learning.

**Submitted to:**

**Prof. Ivan Pustogarov**

Team Members

|  |  |
| --- | --- |
| Student Name | Student ID |
| Yaswanth Kalyanam | 40194341 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Introduction**

Security is an important challenge which that needs to be handled by organisations these days as number of cybercrimes are on the rise. Advancements in the field of computer science has certainly opened up new attack surfaces for outsiders to perform well planned cyber-attack to gain unauthorised information. Measures such as installing firewalls, Intrusion Detection Systems(IDS), Intrusion Prevention Systems(IPS), Next Generation Firewalls, having policies, anti-virus will certainly help in preventing cyber-attacks. However, this could generate large amounts of log details on daily basis that could be very difficult for the security analysts to process and identify which is legitimate request and which is an attack. This could be a problem as large amounts of information could be overwhelming that could cause many attacks to go undetected.

To counter this issue, we need an approach like Machine Learning that is faster and more effective in terms of identifying attacks through log data. Machine Learning is a subset of Artificial Intelligence(AI) that basically uses algorithms and data to imitate how a human would perform a similar action. With more data and data and training the accuracy of the machine improves giving us better results. In this paper, we are going to review Log analysis for intrusion detection/investigation which basically is an attack detection process done using log files as primary sources combined with machine learning and compare this with some of the other techniques that are currently in use for intrusion detection.

**References:**

G. Tsakalidis and K. Vergidis, "A Systematic Approach Toward Description and Classification of Cybercrime Incidents," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 4, pp. 710-729, April 2019, doi: 10.1109/TSMC.2017.2700495.