**Author:**

Jabez, J.Muthukumar, B. -2015

**Problems:**

To analyze and monitor each data packet minutely so that no malware can be transferred , although IDS is capable of doing that but signature detection of IDS is not found much efficient

**Tools:**

Outlier Detection Approach ( using Neighborhood Outlier Factor (NOF) )

**Result:**

As a result of using Layered technology for anomalous behaviour , it has been found out from no. of experiments that it success rate is much greater than other machine learning algorithms because it takes less CPU resources and detect affected data packets at a faster than any other

**RISK MANAGEMENT:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Probability** (P) 1 = low  5 = high | **Severity (S)** 1 = low  5 = high | **Risk Score**  (P x S) | **Mitigation** |
| Zero – day Vulnerability | 3 | 4 | 12 | User should keep updating the application as a security measure |
| False Positives | 3 | 3 | 9 | There should be rules and policy made for the application to highlighting false alarm issue |
| Data Integrity of end user | 2 | 5 | 10 | Data should be made backup at all the time to ensure integrity of data |
| Encrypted Packets | 2 | 5 | 10 | Firewalls should me made stronger ensuring the stoppage of encrypted and affected packets |

**Summary:**

In this research paper, it has been proposed the idea of making intrusion detection system more efficient . However, IDS are made to detect any intrusion that can impact the data integrity of the end users and monitor each and every data packet that came into their network , but smart intruders know ways to bypass both firewall and IDS by different means and that’s a big risk . It has been seen that different machine learning algorithms are considered to be effective to train IDS with different large datasets but this process considered as much time consuming with less successful detection where as there is a better one i.e.; Anomalous detection approach using layered technology . this idea has been presented throughout this report . By using this technique , IDS become efficient by detecting affected packets at a very less time because it had been trained not only with big data sets at distributed environments but also with KDD data sets , which are usually collected from all over the world , making IDS to execute in a less time with accuracy , thus decreasing the chances of false positives

**Significance:**

**Society having different issues doesnot prosper at all , especially when it comes to mental health issues . Mental illness like depression and anxiety most severe one which spread disorder in the society , thus government should start some campaign**