**Modular Intrusion Prevention System**

Rajendra Kumar Raghupatruni**,** Ravi Chandra Sadineni

Harshavardhan chowdary Ellanti, Nitish Garg**,** Anshul Anshul

Stony Brook University

## Abstract

Intrusion Prevention Systems are part of the defense-in-depth strategy of computing systems. One popular Intrusion Prevention System is called fail2ban. fail2ban monitors failed authentication attempts and temporarily blocks traffic from IP addresses that exceed a configurable number. E.g. fail2ban can block all traffic from IP address 1.2.3.4 if that IP address tried to log in more than 10 times in one minute. Our application is similar to fail2ban, monitors auth.log, errors.log etc., to identify the ip/hosts which tries to retry multiple times within a short span of time.

## Introduction

## Design and Implementation

## Evaluation

### Experimental Setup

## Results

## Conclusion

## Future Work

## References

* https://en.wikipedia.org/wiki/Fail2ban