Synopsis/Research Proposal

IDS FOR HYBRID CLOUD

PRESENTED BY:

MUSHTAQ AHMAD DAR

M.TECH-3RD SEMESTER

UNDER GUIDANCE OF:

(DR. ZAHOOR AHMAD)

CONTENTS

- Abstract
- Introduction
- Literature survey
- Research method-detection method
- Data set
- Tools used
- Conclusion
- References

ABSTRACT:

Internet based applications and data storage services can be easily acquired by the end users by the permission of Cloud computing. Providing security to the cloud computing environment has become important issue with the increased demand of cloud computing. One of the needful components in terms of cloud security is Intrusion Detection System (IDS). To detect various attacks on cloud, Intrusion Detection System (IDS) is the most commonly used mechanism.

INTRODUCTION

An Intrusion detection system examines all internal and external network activities or attacks and identifies suspicious design that may point out the system attack or a network from someone attempting to break into the security or compromise a system .

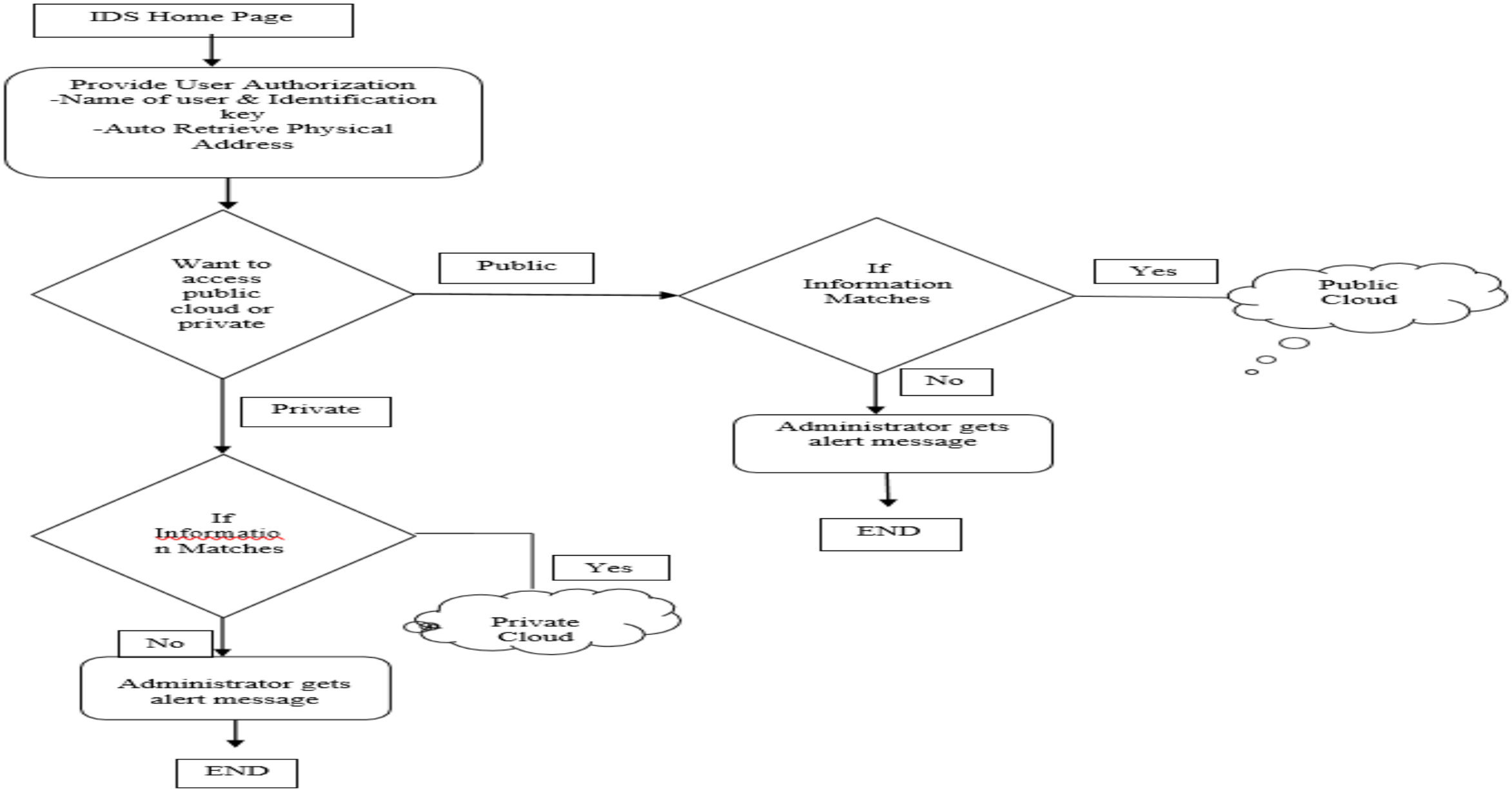
Due to the distributed nature of cloud computing, cloud computing environments are easy targets for invaders looking for possible susceptibility to exploit.

Literature survey:

SERVICES AND DEPLOYEMENT	IDS USED	PROFECIENCY/ACCURACY
AWS	HIDS	87%
GOOGLE DOCS	NIDS	95%
AZURE	HIDS	97%

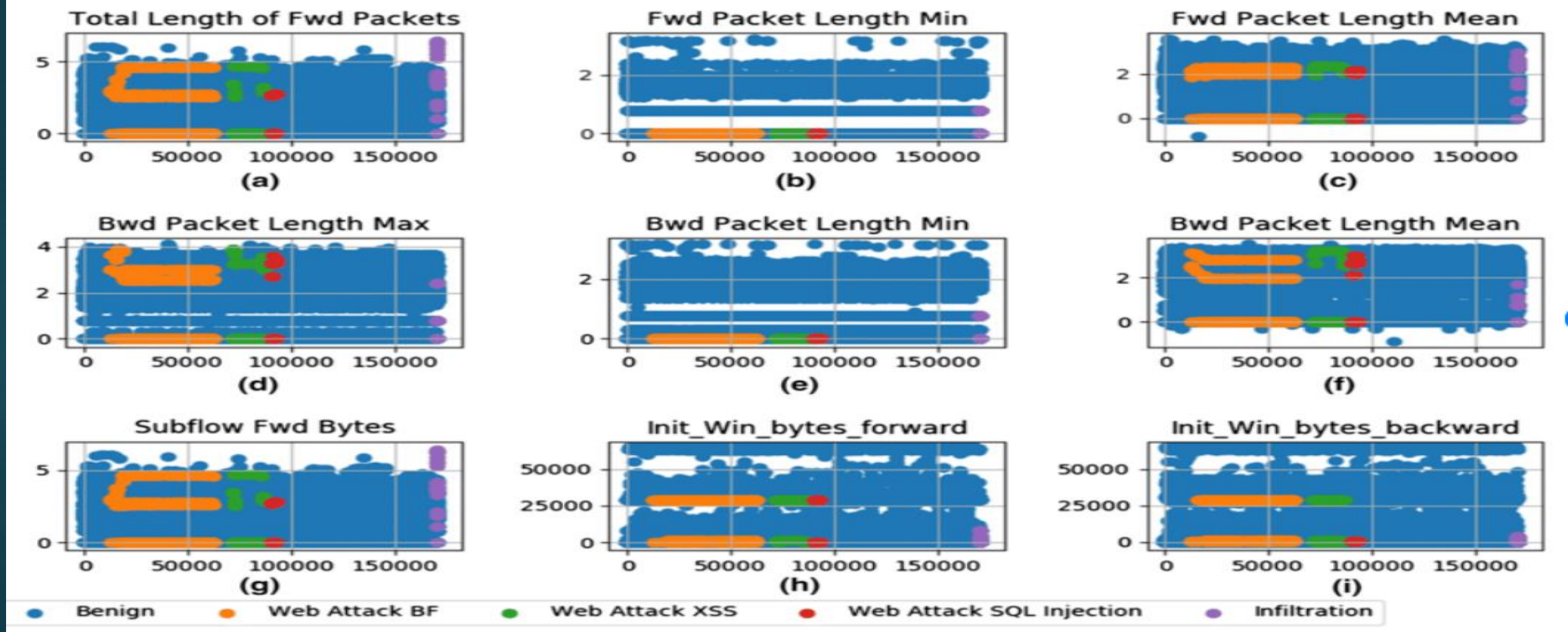
HYBRID INTRUSION DETECTION METHOD

Hybrid Intrusion Detection Method (HIDM) can be designed for hybrid cloud. HIDM has three phases: Registration stage, Signature analysis stage, Anomaly analysis stage stage.



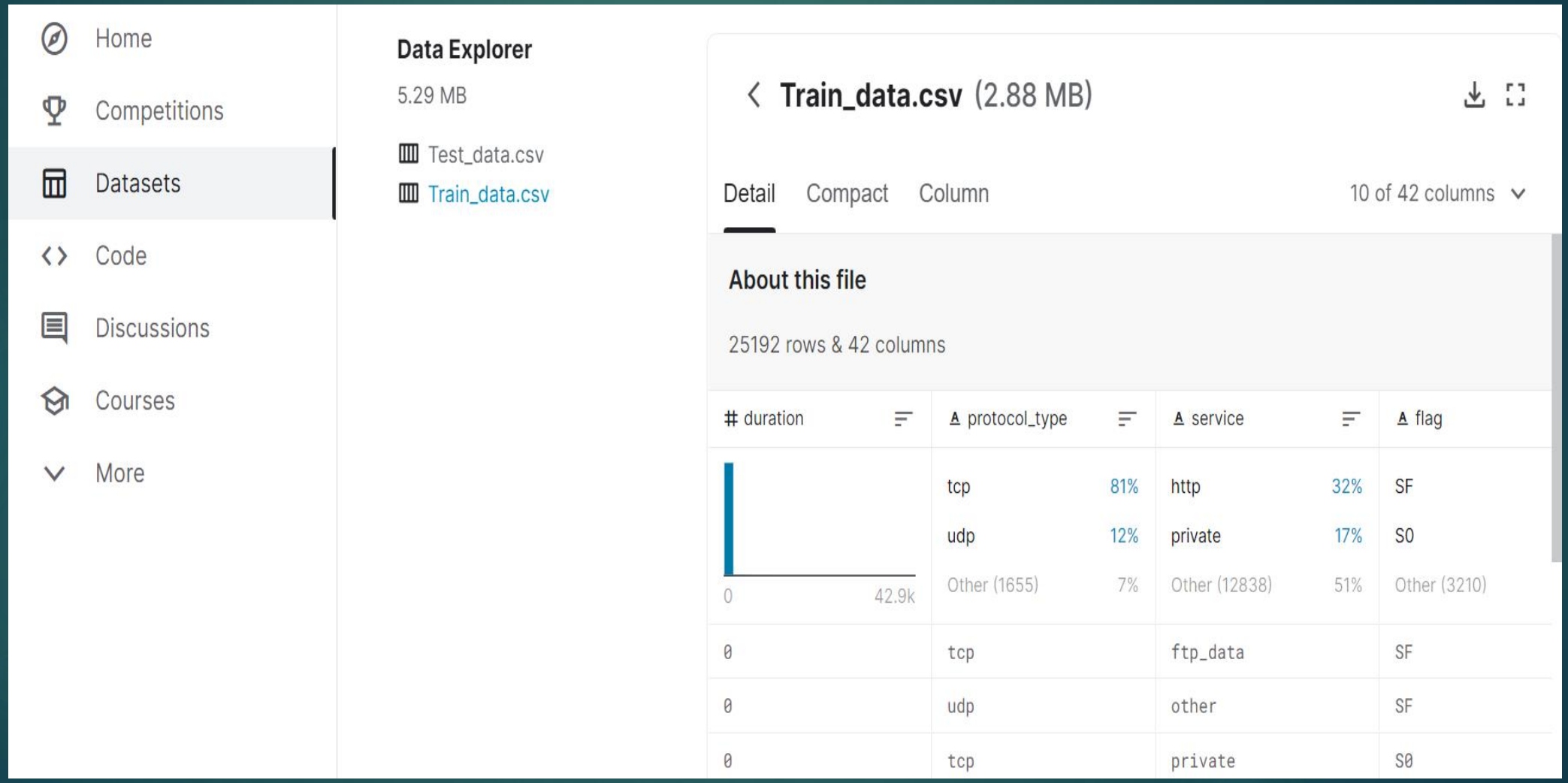
HYBRID INTRUSION DETECTION METHOD

DATA SET



Attack instances distribution in CICIDS 2017 dataset

DATA SET


Home
Competitions
Datasets
Code
Discussions
Courses
More
Data Explorer
5.29 MB
Test_data.csv
Train_data.csv
Train_data.csv (2.88 MB)
Detail
Compact
Column
10 of 42 columns
About this file
25192 rows & 42 columns
duration
protocol_type
service
flag
tcp 81%
udp 12%
Other (1655) 7%
http 32%
private 17%
Other (12838) 51%
SF
S0
Other (3210)
0
42.9k
0 tcp ftp_data SF
0 udp other SF
0 tcp private S0

❖ Algorithm USED

The most common Shallow Learning algorithms used for IDS are **Decision Tree**, K-Nearest Neighbor (KNN), Artificial Neural Network (ANN), Support Vector Machine (SVM), K-Mean Clustering, Fast Learning Network, and Ensemble Methods

TOOLS USED

- Snort 3
- SURICATA
- Implementing PGPA

CONCLUSION

By joining much more principle the effectiveness of the method can be enhanced to discover an Intrusion in a network.

By improving the values based upon the limitation of time the implementation of the method can be enhanced. If the counting of users gets enlarged, the performance of the proposed method will hold well.

References

1. *M.M.M.Hassan," Current Studies on Intrusion Detection System, Genetic Algorithm and Fuzzy Logic", International Journal of Distributed and Parallel Systems, Vol.4, No.2, pp.35-47.*
2. *Ms. Parag K Shelke, Ms. Sneha Sontakke and Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research,Vol.1,ISSN 2277-8616, 2012.*
3. *Hassen Mohammed Alsafi, Wafaa Mustafa Abduallah and Al-Sakib khan Pathan,"IDPS: An integrated Intrusion Handling Model for Cloud Computing Environment, International Journal of Computing and Information Technology (IJCIT), 2012.*
4. *Ms. Parag K Shelke, Ms. Sneha Sontakke and Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research,Vol.1,ISSN 2277-8616, 2012.*

Thank you