IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 8, August 2021

DOI 10.17148/IJARCCE.2021.10804

QoS: Congestion and Queuing with Web Attack Detection

Sujay Singh[1], Vishesh S[2]

Student, BE, Department of CSE, Dr AIT, Bangalore, India [1]

BE, MBA[2]

Abstract: Quality of Service (QoS) refers to ability of a network to provide improved service to selected network traffic over various underlying technologies including Frame Relay, ATM, Ethernet and 802.1 networks, SONETS and IP-routed networks.The traffic through this network may include data types such as email, file sharing or web traffic. Other forms of traffic include voice and video. These are considered as sensitive forms of traffic. They often require guaranteed or regulated service. In this paper, we deal in detail with two factors affecting QoS: Congestion and Queuing. Identifying and rectifying the above problems to reduce packet loss, latency and jitter on the network is the errand for the day. Few of the Queuing Algorithms like First in First out (FIFO), Priority Queuing (PQ), Round Robin and Weighted Round Robin (WRR) are explained in brief pictorially. The internet is often vulnerable to attacks from possible hackers who try to compromise the system in order to illegally poach the resources of the system under question. These attacks are famously called web attacks and are a very common problem amongst the computer fraternity. Though there are several existing systems to counter the problem of attacks on the web, most of these systems have their own drawbacks, as in they do not provide classification on any other grounds except frequency, thus causing many web attacking http requests to fall out of the bracket. The objective of our project is to detect these web attacks from the http requests based on many parameters, and classify them as web attacks or not.

Keywords: Frame Relay, ATM, Ethernet and 802.1 networks, SONETS and IP-routed networks, Congestion and Queuing, First in First out (FIFO), Priority Queuing (PQ), web attacks, web attacking http requests.

I.INTRODUCTION

Quality of Service (QoS) of a network [1] is a vital parameter which measures the ability of the network to provide improved service to network traffic over Frame Relay, ATM, Ethernet and 802.1 Networks, SONETS and IP-routed networks.[2]

Tools which have been developed to enforce QoS are

- Classification

Classification is based on identifying traffic based on service requirements. The traffic is then marked so that traffic can be differentiated.

- Queuing

Queuing includes

i.First-In First-Out (FIFO)
ii.Priority Queuing(PQ)
iii.Custom Queuing(CQ)
iv.Round Robin
v.Weighted Round Robin(WRR)

II.CLASSIFICATION AND MARKING

Classification is the process of identifying and categorizing traffic into classes, typically based upon

- Incoming Interface.
- IP Precedence.
- DSCP.
- Source or Destination Address.
- Application.

Classification is the most fundamental QoS building block. Without classification all packets are treated the same.

Marking is carried out after classification and “colours” a packet (frame) so as to be identified and distinguished from other packets.Figure 1 shows classification and marking in the LAN with IEEE 802.1 Q.Figure 2 shows classification and marking in an Enterprise.

IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 8, August 2021

DOI 10.17148/IJARCCE.2021.10804

III. NETWORK SECURITY OBJECTIVE

Our objective is to detect whether the HTTP request is malicious or not, where word vector along with neural network is used with the hidden layers along with TF-IDF methodology. The word vector block and TF-IDF are combined together in order to determine whether a given request is a web attack or it is not a web attack. There are different categories of clusters which are considered in order to perform the category checks for the web attacks and the category includes the SQL, HTML and JavaScript.

IV. CONGESTION AND QUEUING

Congestion can occur in the network where there are points of speed mismatch or aggregation. Figure 3 shows Packets entering router and being forwarded by it. Network Congestion has been difficult to define quantitatively across the industry. For subscribers, it means choppy VoIP Communications, poor web browsing and frustrating online gaming performance. This is a major business threat for the Communication System Providers (CSPs). Speed mismatch are the most typical cause of congestion. Figure 4 shows the conditionof Speedmismatch possibly persistent when going from LAN to WAN. Figure 5 shows Aggregation, which is another reason for Congestion. Aggregation [3] is used to provide fastand transparent recovery in case individual links fail. But choke points are created as a result of Aggregation leading to Congestion.

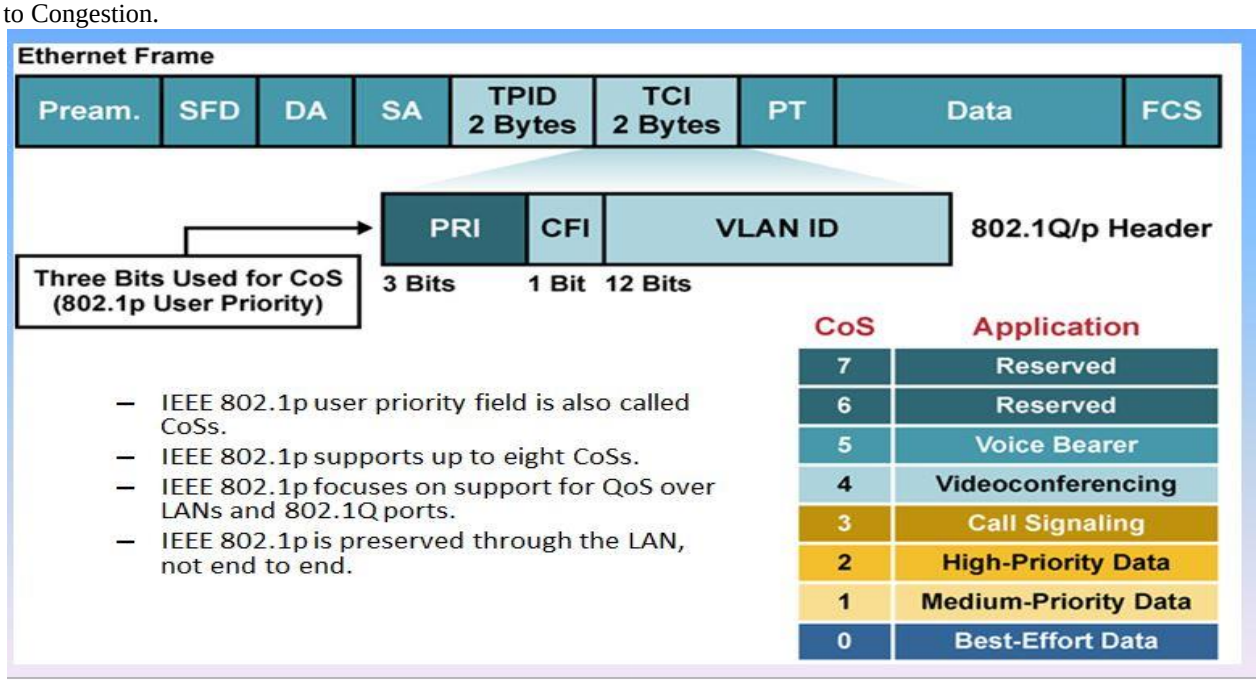

Figure 1 shows classification and marking in the LAN with IEEE 802.1 Q.

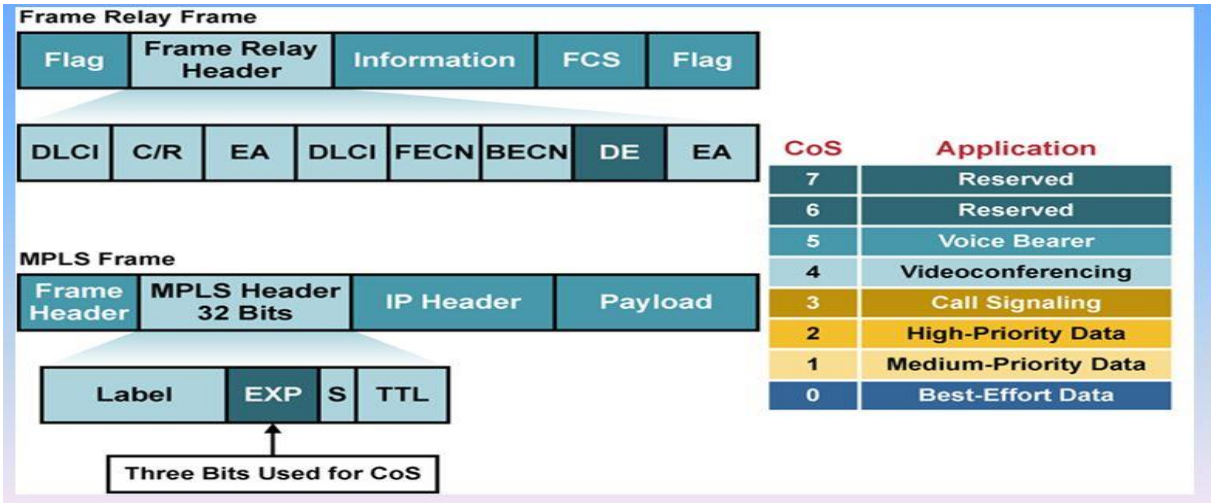

Figure 2 shows classification and marking in an Enterprise.

IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 8, August 2021

DOI 10.17148/IJARCCE.2021.10804

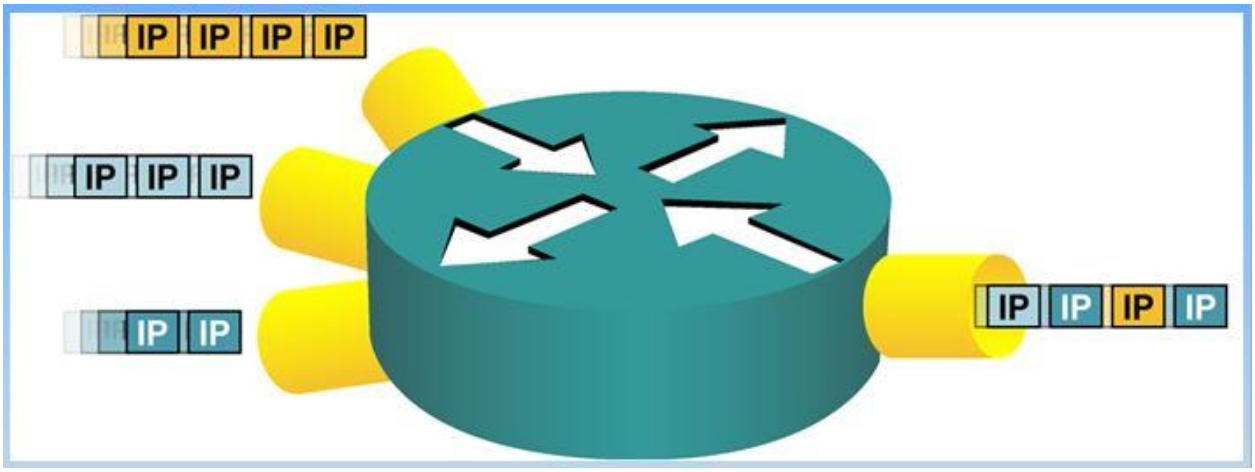

Figure 3 shows Packets entering router and being forwarded by it.

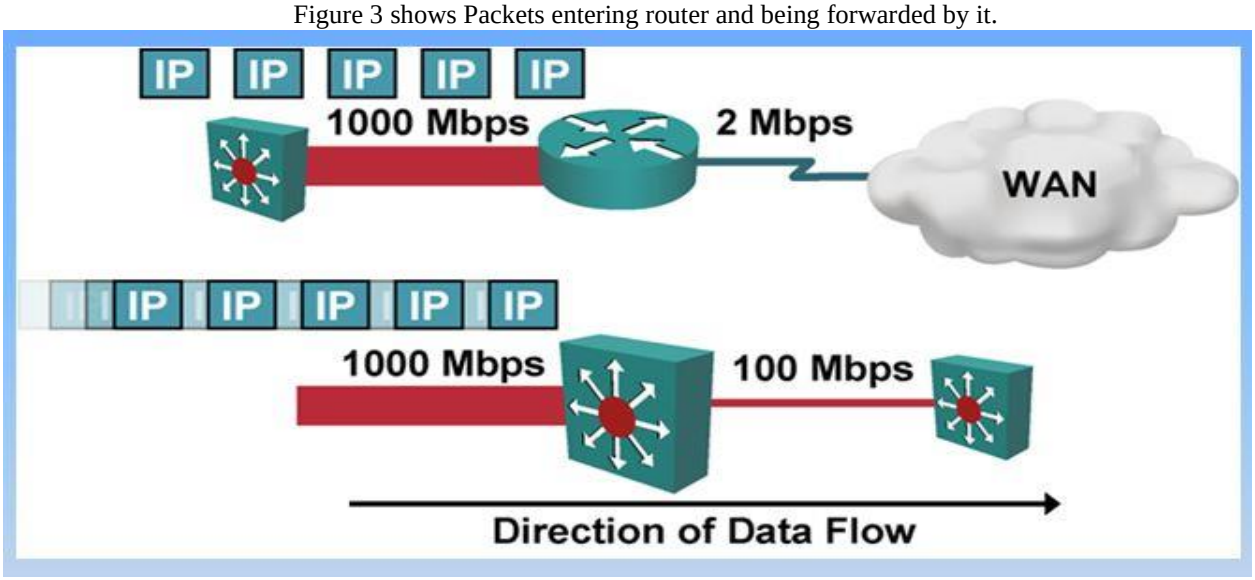

Figure 4 shows the condition of Speed mismatch possibly persistent when going from LAN to WAN.

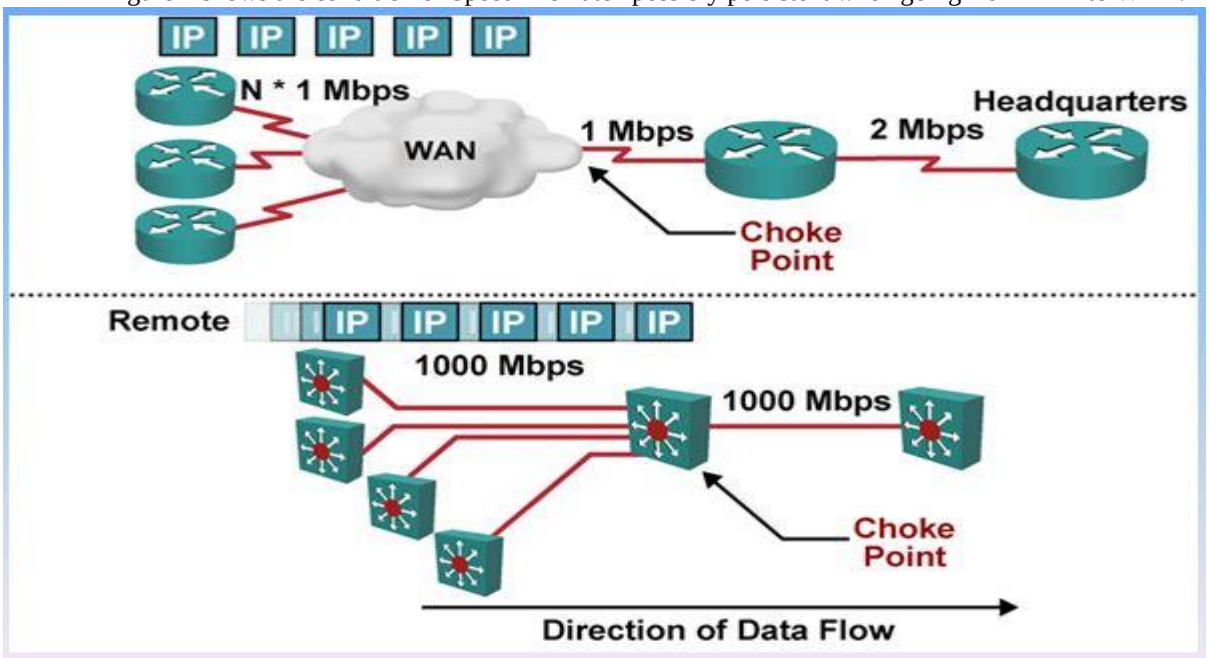

Figure 5 shows aggregation

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 8, August 2021

DOI 10.17148/IJARCCE.2021.10804

V.QUEUING

Queuing is designed to accommodate temporary congestion on an interface of a network device by storing excess packets in buffers until the bandwidth becomes available. Queuing is a Congestion-management mechanism that controls Congestion on interfaces.

The Queuing Algorithms used are:

- *First-In First-Out (FIFO)*

In this mechanism, the first packet coming in will be the first packet going out. It is the simplest of all algorithms. It consists of only one queue. All individual queues are FIFO. Figure 6 shows FIFO and packets flowing in one direction.

- *Priority Queuing(PQ)*

Unlike FIFO, Priority Queuing uses multiple queues. It allows prioritization. Always the first queue is emptied before going to the next queue.Figure 7 shows PQ process.

Steps involved

i.Empty Queue No 1.
ii.If queue No 1 is empty, then dispatch one packet from queue No 2.
iii.If both queue No 1 and queue No 2 are empty then dispatch one packet from queue No 3.

- *Round Robin and Weighted Round Robin*

Round Robin uses multiple queues. There is no prioritization. Dispatches one packet from each queue in each round. Weighted Round Robin (WRR) uses prioritization and a certain weight is assigned to each queue. Dispatch packets from each queue proportionately to an assigned weight as shown in figure 8.

i.Dispatch up to four from queue 1.
ii.Dispatch up to two from queue 2.
iii.Dispatch one from queue 3.
iv.Go back to queue number 1.

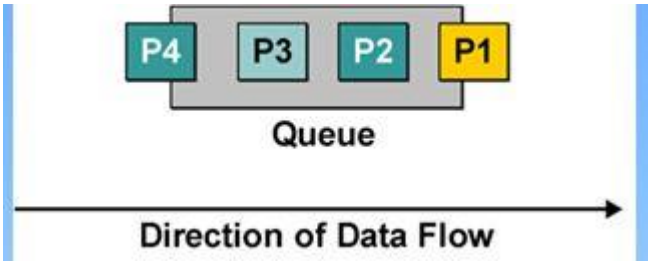

Figure 6 shows FIFO and packets flowing in one direction.

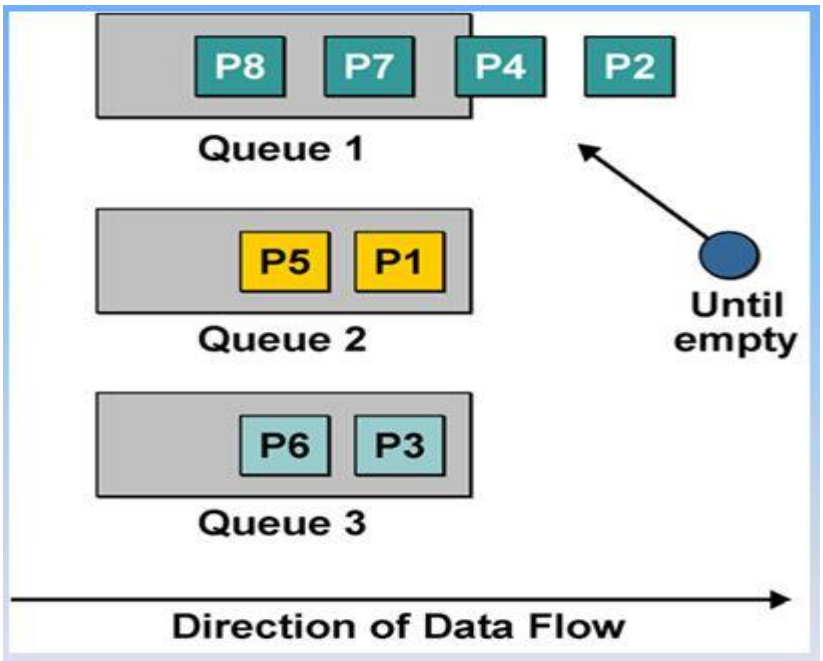

Figure 7 shows PQ process.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 8, August 2021

DOI 10.17148/IJARCCE.2021.10804

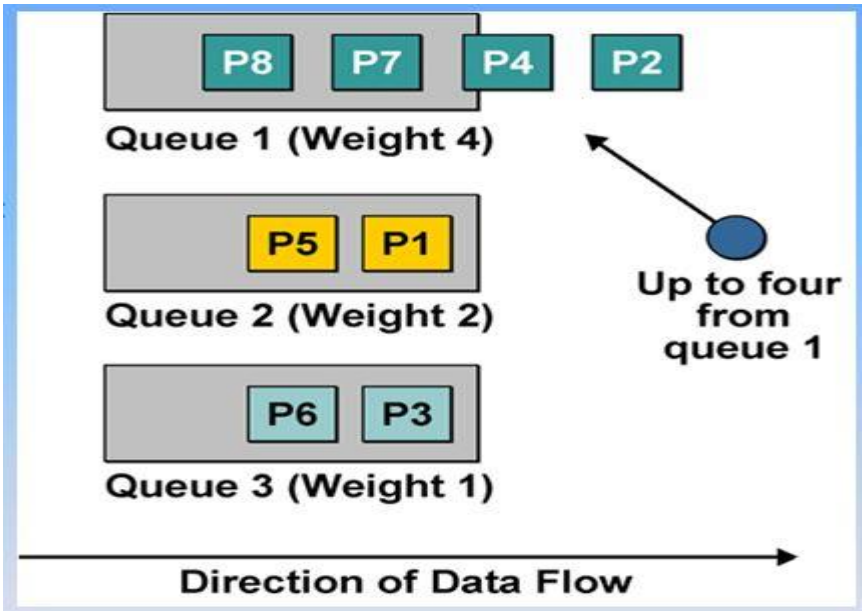

Figure 8 shows mechanism of Weighted Round Robin.

VI. MODEL FOR WEB ATTACK DETECTION

Algorithm: K-means Clustering:

- Purpose: Classification of HTTP request into anomaly or not.
- Input: The classified words related to various categories along with the total FV score for each category specific to dataset. [5][6][7]
- Output: HTTP request is classified as anomaly and non-anomaly, and then based on the total FV score, anomaly is further classified into html, JavaScript and SQL.
- Different words related to various kinds of web attacks are obtained from the training vectors.
- Unique data ids are found by making use of TF-IDF matrix.
- The count of various web attack category words is obtained.
- The total feature vector for each of the data set based on the word and TF-IDF values is found.
- Compute the distance between the feature vector and the trained vectors.
- Find the minimum distance.
- The class label corresponding to the minimum distance is assigned a class respectively

VII. CONCLUSIONS

Delivering Quality of Service to network traffic is of great importance for critical applications and sensitive traffic like video and voice. Congestion affects QoS due to speed mismatch and aggregation. Queueing is designed to accommodate temporary congestion on an interface of a network device. Various queueing algorithms are designed to solve the problem of congestion, storing extra packets in buffers for proper bandwidth accomodation. These algorithms are explained pictorially. Classification of data is done by using K-means algorithm. We have detected web attacks from the http requests based on many parameters, and classify them as web attacks or not. We also have classified the attacks as HTML, JavaScript or SQL attacks, thus providing a novelty. Thus, the system solves the problem of undetected web attacks through http requests and thus increases the security of the system.

REFERENCES

[1] Quality of Service Overview – Cisco-
https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/.../guide/fqos.../qcfintro.pdf
[2]Layer 2 Local Switching – Cisco-
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/wan.../wan-l2-lcl-swng.pdf
[3] Individual QoSversus Aggregate QoS - IEEE Computer Society-
https://www.computer.org/csdl/trans/nt/2005/02/01424045.pdf
[4] Efficient fair queuing algorithms for packet-switched networks-IEEE- DOI-10.1109/90.664266
[5] J. Saxe, and K. Berlin, "Deep neural network based malware detection using two dimensional binary program features," in International Conference on Malicious and Unwanted Software (MALWARE), IEEE, 2015.
[6] R. M. Pandurang and D. C. Karia, "A mapping-based podel for preventing Cross site scripting and sql injection attacks on web application and its impact analysis," 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2015, pp. 414-418, doi:

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 8, August 2021

DOI 10.17148/IJARCCE.2021.10804

10.1109/NGCT.2015.7375152.
[7] T. Rashid, I. Agrafiotis, and J. RC Nurse, "A new take on detecting insider threats: exploring the use of hidden markov models," in Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, ACM, 2016.