Can AI and Big Data really help in Cyber Security

DEEP seas

Bringing calm to the cyber seas for our clients

Why am I here – Pop quiz ?

a. I have no idea

b. I am intimidated

c. A little out of place

d. I am crazy

e. Because we have a huge Big Data Use Case in Cyber Security that needs Math

f. All of the above

What do I mean by Big Data in Cyber?

Customer example 3 year view.

- Their growth is 5%.
- Their log volume growth is 40%.
- Their Log size is 250%.

Story Through a Timeline

Nuclear Engineer

Mont An

Early AI Winter

AQ Technology

mate y

Patent 11301467 B2

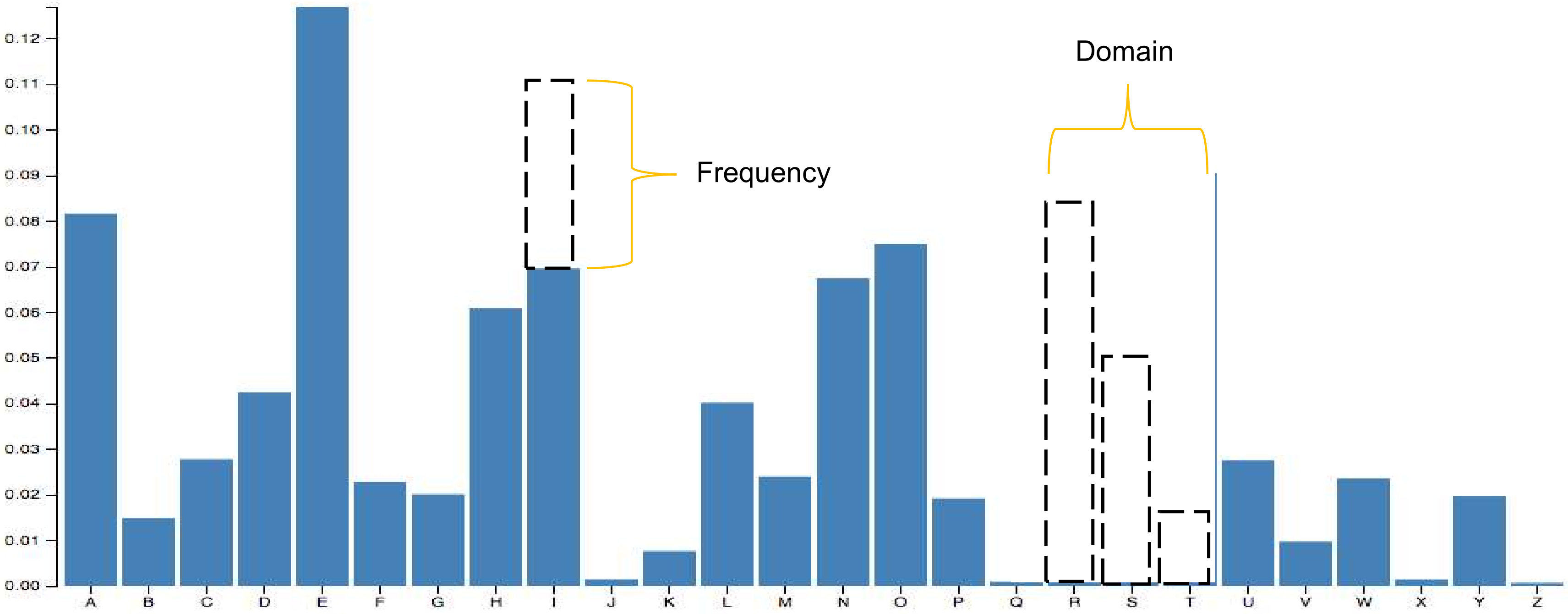
The Patent

Domain: set of values for which metrics are generated or grouped from a given query

E.g. Examine gaps in x-axis

Frequency: numeric result of a mathematical function for a given domain

E.g. Examine gaps in y-axis



Rough Set DB Performance

- Testing Criteria
  - Industry Benchmark Cost Comparison was made using the Top Performing TPC System
  - DeepSeas's Database size was 2.5X the benchmark testbed data set

- Testing Summary – AQ Technology is
  - 10% of the hardware cost
  - Over 10X better cost per query
  - 5X faster query performance

Category	TPC- Industry Benchmark Cost Comparison (Top Performing TPC System)	AQ Technology
Cost	$472,069	$42,152
Queries/Hour	1,009,065	1,110,650
Price/Performance	$0.47/ Query	$0.037/Query
Database Size	1000 GB	2500 GB
Average Query Time	5.2 seconds	1.08 seconds

The Maths – Volumetric

Features (11)	Total Possible Values	Total Combinations Possible (From 11 Data Sources) That Require Analysis
Source IP	4,228,250,625	7,412,123,345,625
Destination IP	4,228,250,625	31,340,315,168,716,000,000,000
Destination Port	65,656	2,057,679,732,717,220,000,000,000,000
Protocol	50	102,883,986,635,861,000,000,000,000,000
Direction	10	1,028,839,866,358,610,000,000,000,000,000
Disposition	6	6,173,039,198,151,650,000,000,000,000,000
Source Country	240	1,481,529,407,556,400,000,000,000,000,000,000
Destination Country	240	355,567,057,813,535,000,000,000,000,000,000,000
Subject user	1,000	355,567,057,813,535,000,000,000,000,000,000,000,000
Target user	1,000	355,567,057,813,535,000,000,000,000,000,000,000,000,000
Vendor Event ID	56,000	19,911,755,237,558,000,000,000,000,000,000,000,000,000,000,000

We are client obsessed

We believe in the power of diverse perspectives

We stand in solidarity with our teammates

We solve hard problems at the speed of cyber

We prioritize personal health and wellness

Joel Holland
Joel.Holland@deepseas.com

Thank You