Intro

Problem & Solution

The Fuzzy Process

Phishing

Applying Fuzzy

Resources

Using Generative AI for Developer Enhancement & Software Factories

Raymond Garcia, Ph.D.
Co-Founder & Chief of Technology
PinnacleAi Platforms

PinnacleAi™ PLATFORMS

itag

TECH360°

Describe

Problem and solution (Phishing, Fuzzy Logic, and Generative AI)

Demonstrate

Apply Fuzzy to the web Web Phishing problem then use Generative AI to supplement the development

Conclude

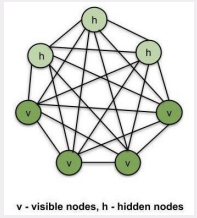
Discuss results, tools, and datasets

1990s
Boltzmann machines
(Early generative models)

2010's
Generative Adversarial Networks
(Synthetic Images)
Variational Autoencoders
(drug discovery via probability)

1

2



3

4

5

1980s
Early Foundations using ANNs and Backprogagation

Early 2000's
Early deep learning with stacked layers

Late 2010's
Audio Generation (WaveNet)
GPT, Large Language Models

PinnacleAi™ PLATFORMS

itag

TECH360°

PinnacleAi PLATFORMS ™ itag TECH360°

GPT

Large language model (LLM)

- Gives AI apps the ability to generate text
- One of the largest neural networks, with hundreds of billions of parameters

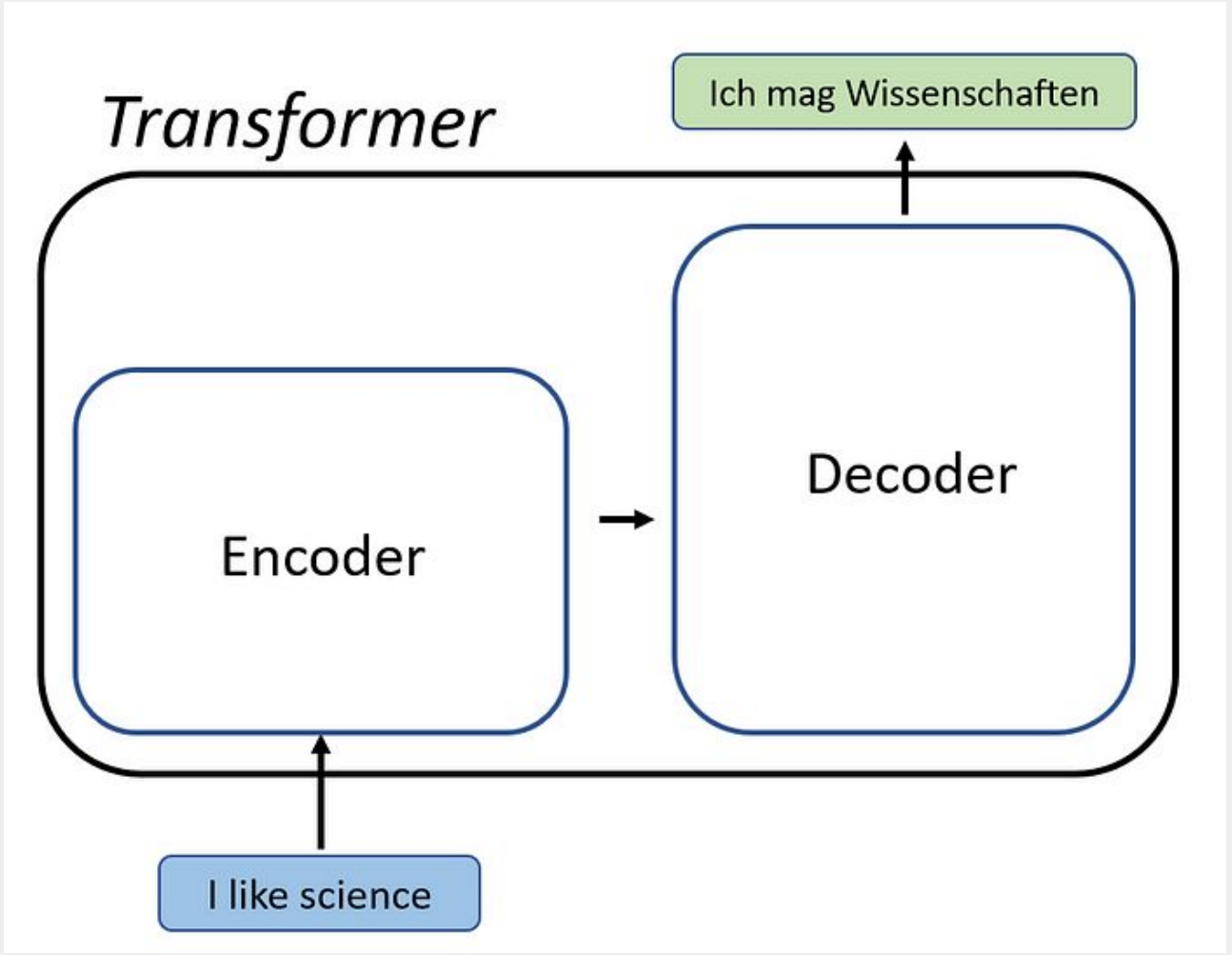
VS

ChatGPT

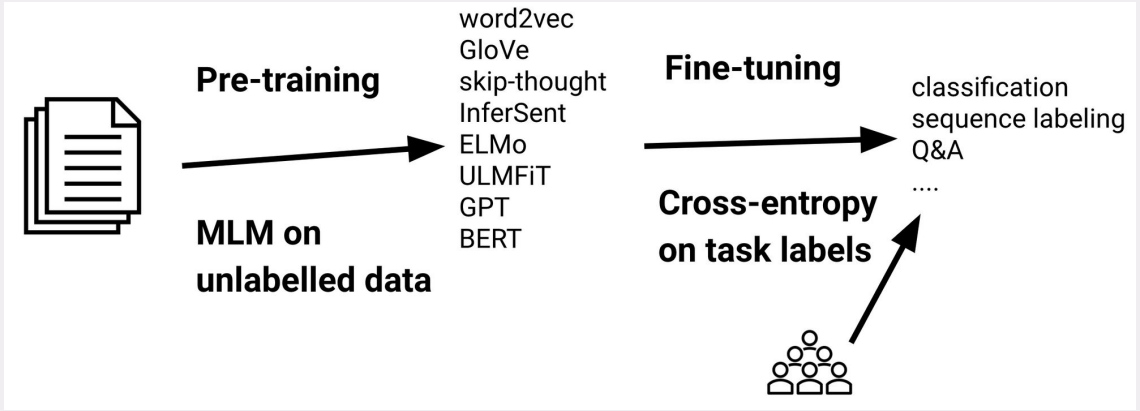
Chatbot app powered by GPT

- Relies on a set of GPT's parameters
- Optimized for dialogue
- Has content filters

_zapier



PinnacleAi ™
PLATFORMS
itag
TECH360°


Pre-training
MLM on
unlabelled data
word2vec
GloVe
skip-thought
InferSent
ELMo
ULMFiT
GPT
BERT
Fine-tuning
Cross-entropy
on task labels
classification
sequence labeling
Q&A
....

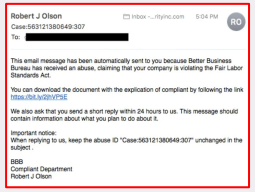
PinnacleAi PLATFORMS ™ itag TECH360°

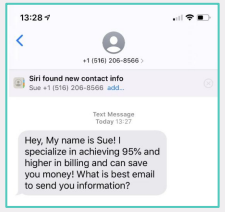
Smishing/Vishing

Smishing: Text or SMS,
Vishing: Voice->RDP

Angler Phishing

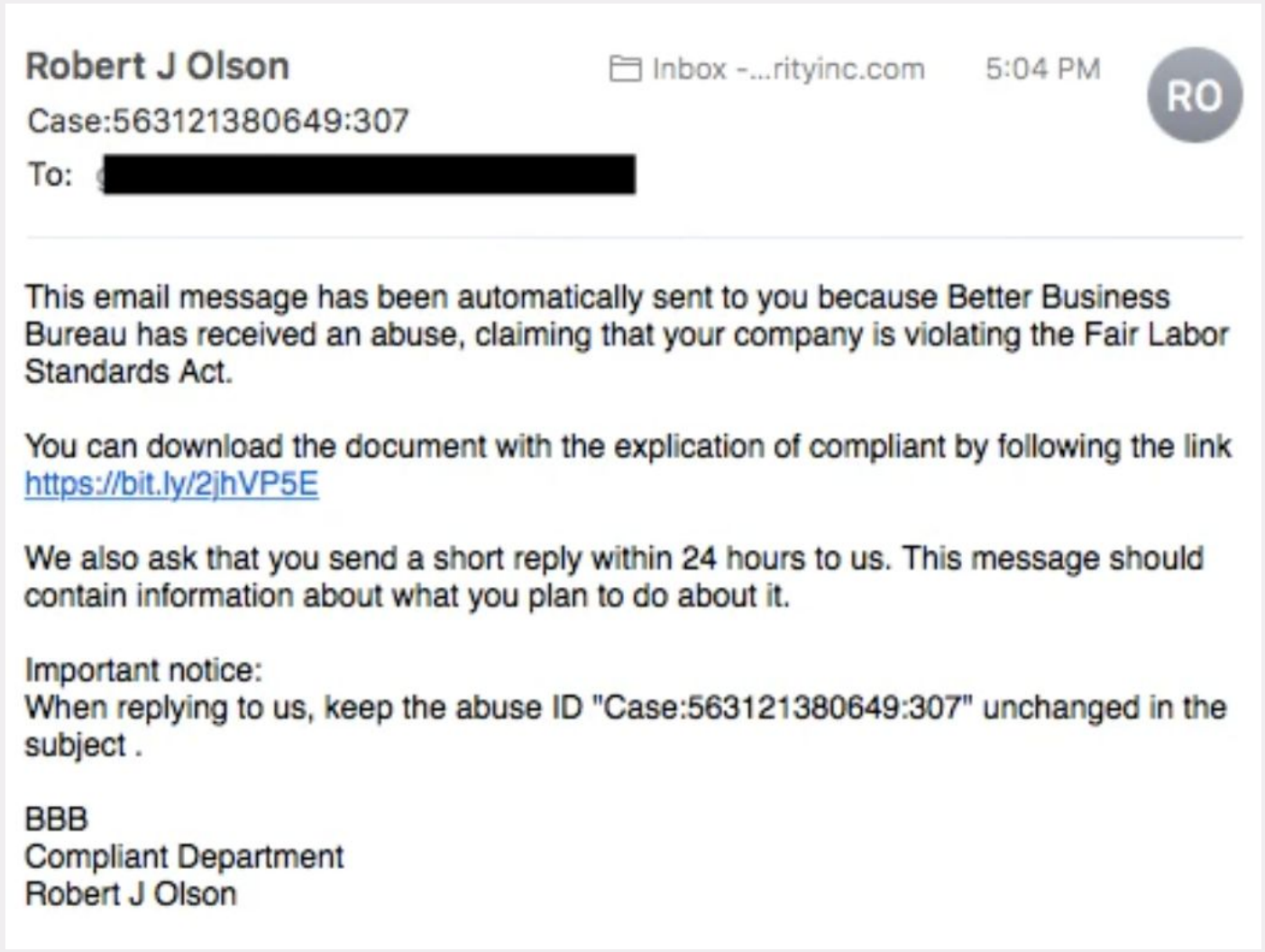
Hijacking responses inside social media





1. **Spear/Whaling**
   Targets a specific group (Spear: admins, etc., Whaling: C-Level)
2. **Smishing/Vishing**
   Smishing: Text or SMS, Vishing: Voice->RDP
3. **Email phishing**
   Email at-large and sextortion
4. **Angler Phishing**
   Hijacking responses inside social media
5. **Search Engine**
   SEO Poisoning

PinnacleAi PLATFORMS ™ itag TECH360°



Robert J Olson Inbox -...rityinc.com 5:04 PM RO

Case:563121380649:307

To: [redacted]

This email message has been automatically sent to you because Better Business Bureau has received an abuse, claiming that your company is violating the Fair Labor Standards Act.

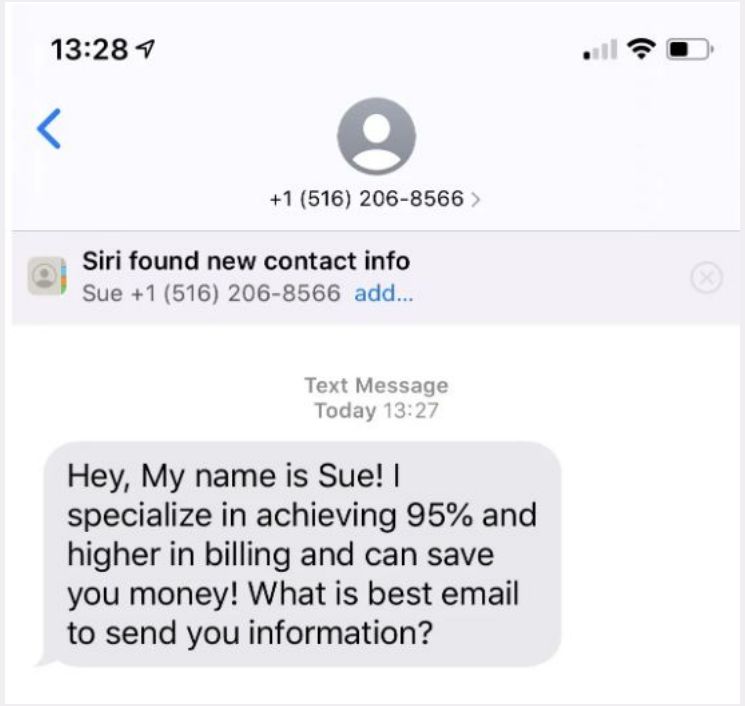
You can download the document with the explication of compliant by following the link https://bit.ly/2jhVP5E

We also ask that you send a short reply within 24 hours to us. This message should contain information about what you plan to do about it.

Important notice:
When replying to us, keep the abuse ID "Case:563121380649:307" unchanged in the subject .

BBB
Compliant Department
Robert J Olson

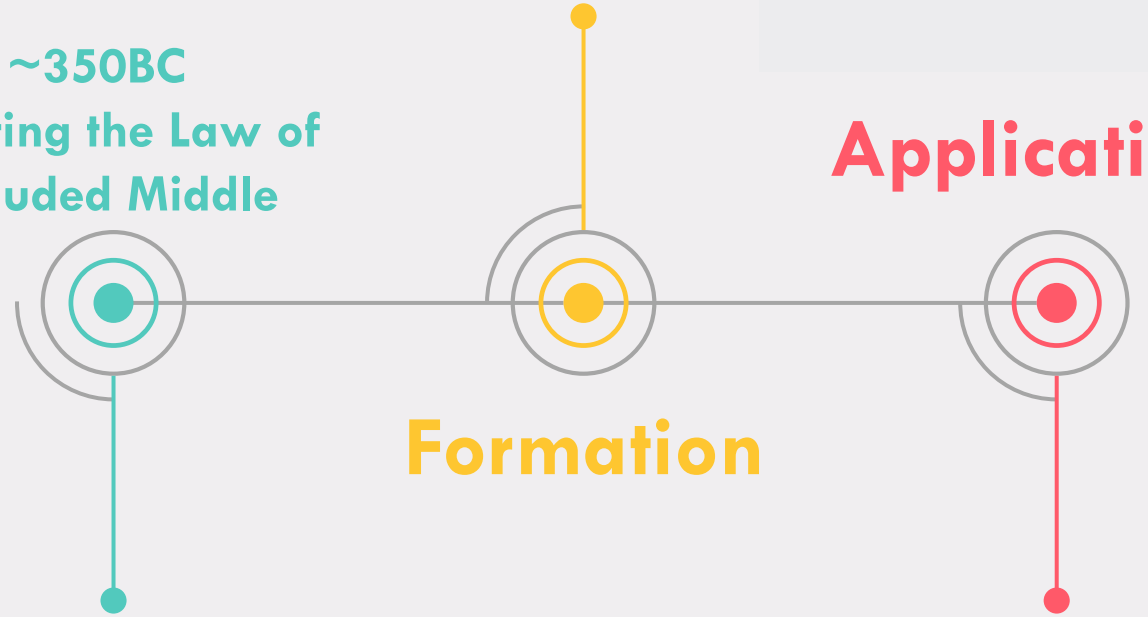
PinnacleAi PLATFORMS ™ itag TECH360°



PinnacleAi PLATFORMS ™ itag TECH360°

PinnacleAi PLATFORMS ™ itag TECH360°

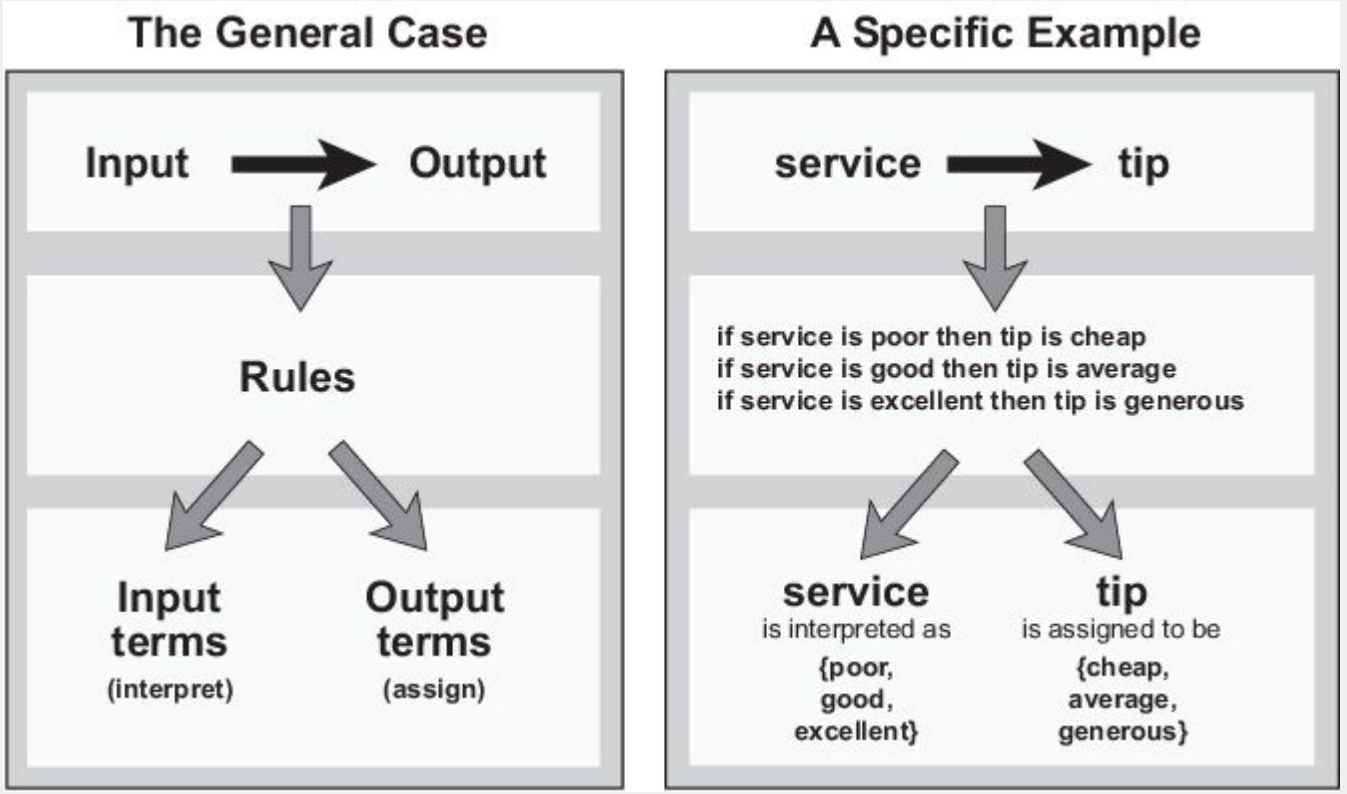
1854- Boolean Algebra (George Boole)
1965- Fuzzy Logic (Lotfi Zadeh)



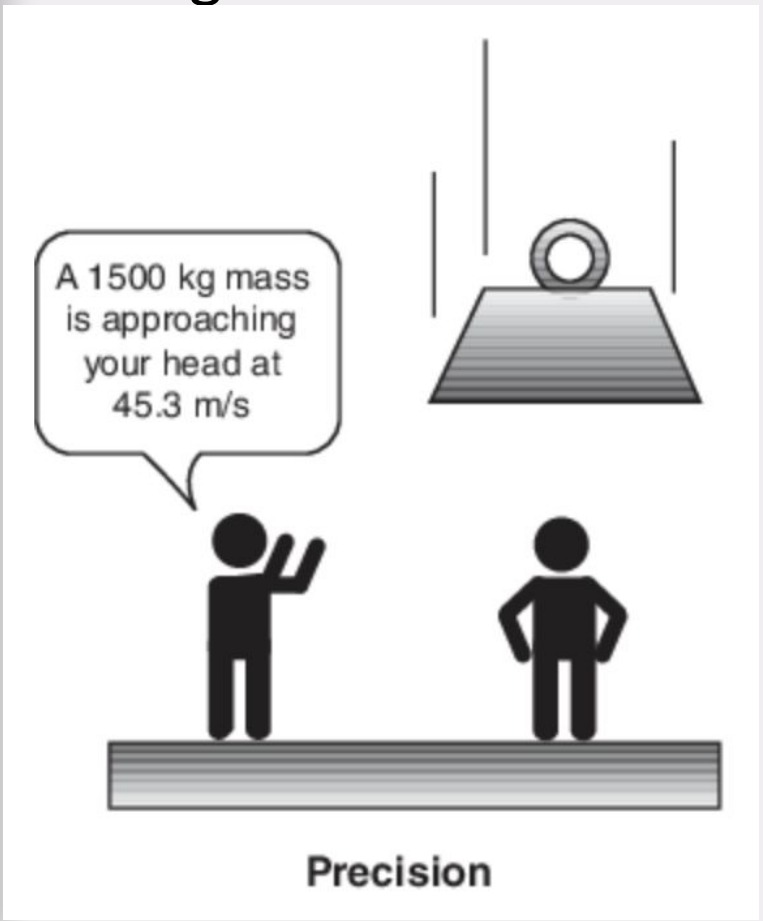
Either a proposition or its negation is true (Aristotle, 340BC),
Plato Rejected his pupil's notion

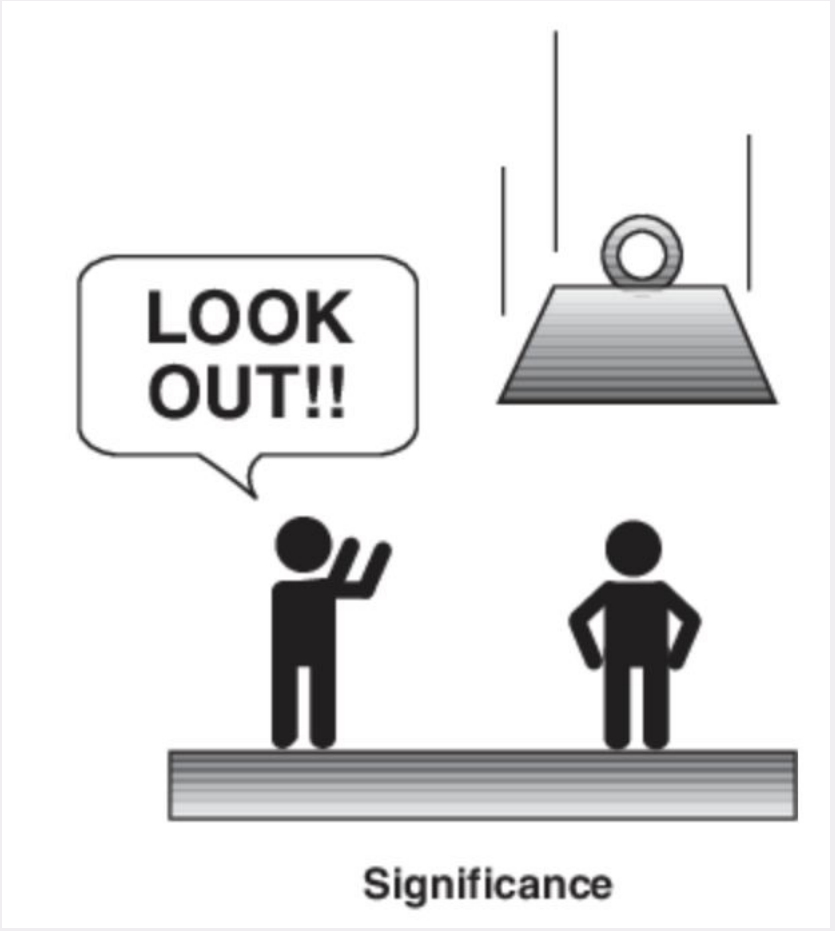
1990's – Risk, local monitoring, but mostly control,
2000's – Network Anomaly and Intrusion
2010's – Reputation, reliability, and trust,
2020's – Vehicular, iot, and resilience

PinnacleAi PLATFORMS ™ itag TECH360°

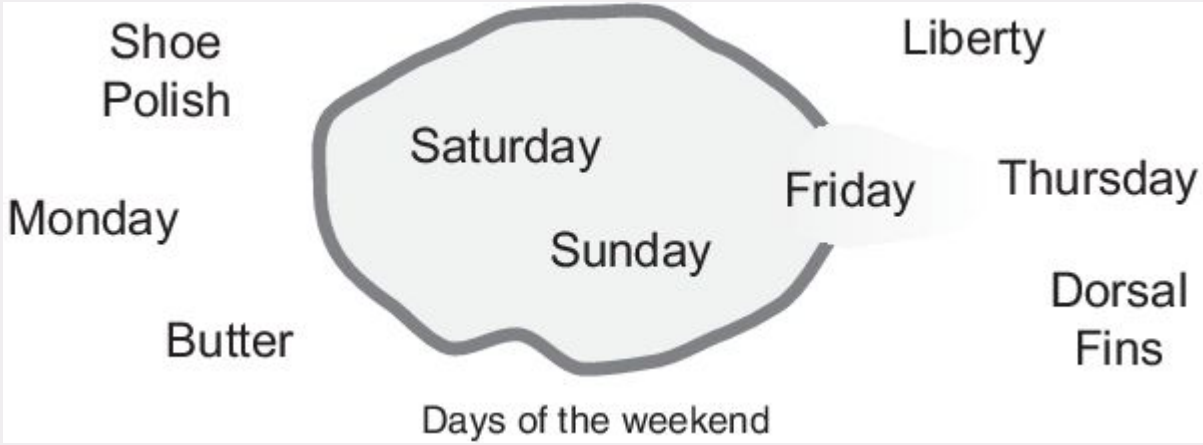


Fuzzy logic is all about the relative importance of precision:
How important is it to be exactly right when a rough answer will do?

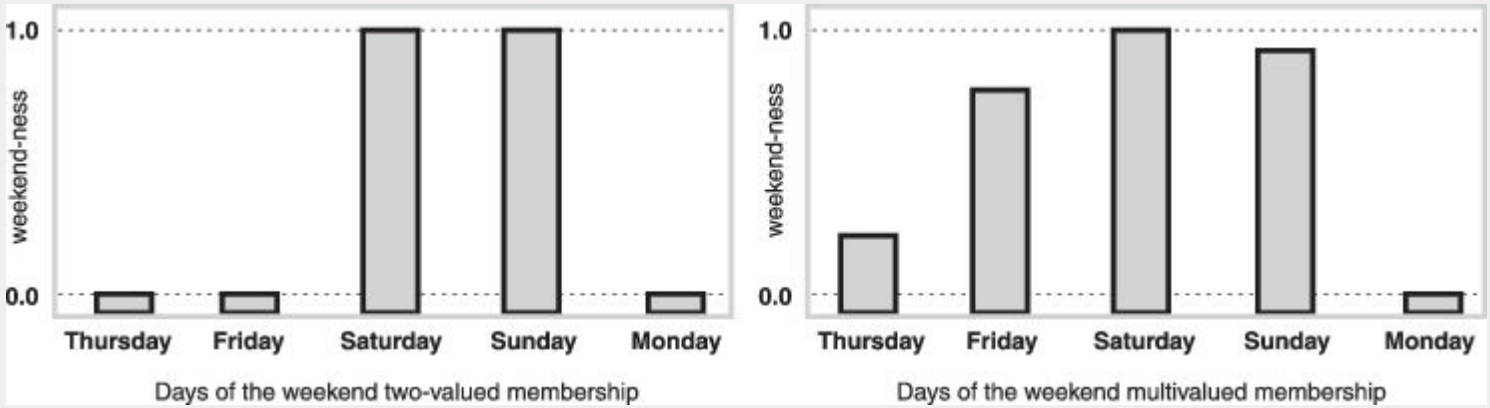


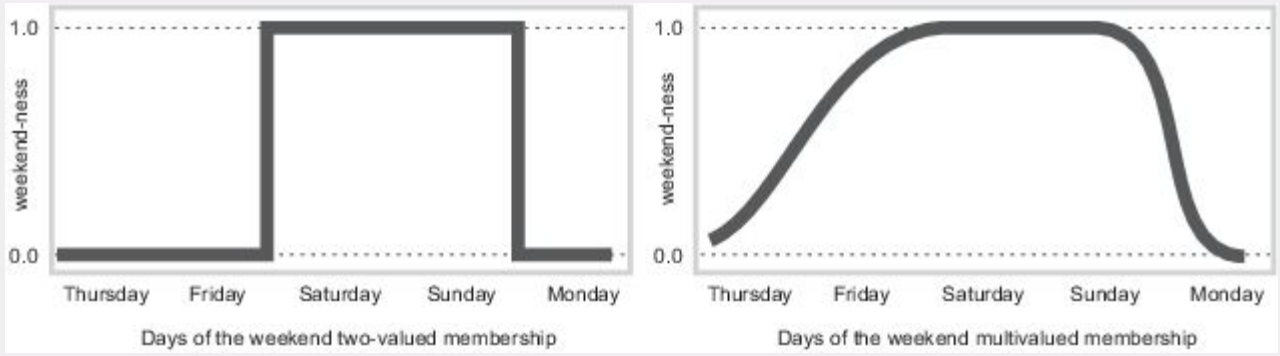


Fuzzy Sets

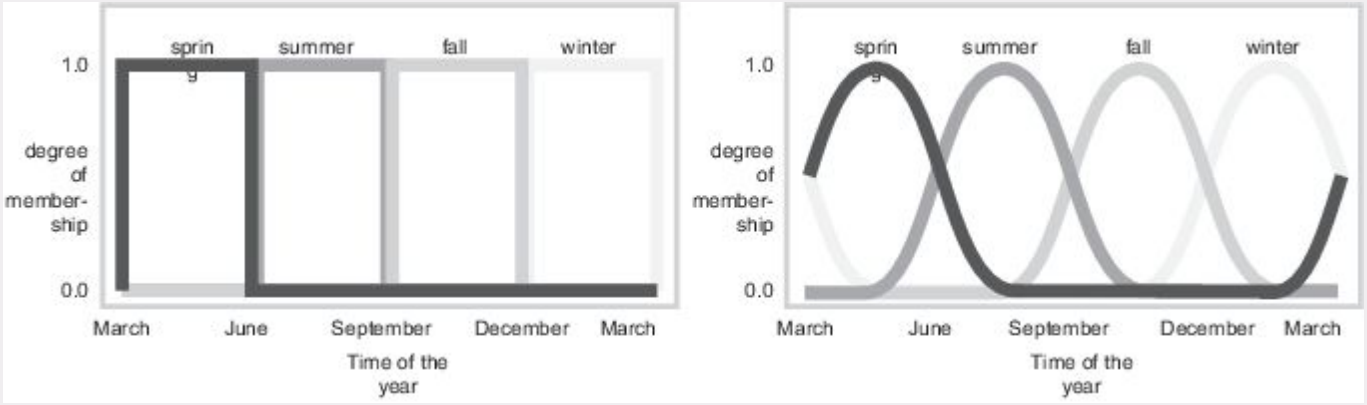

Shoe Polish
Liberty
Saturday
Friday
Thursday
Monday
Sunday
Dorsal Fins
Butter
Days of the weekend

Weekend-ness Example

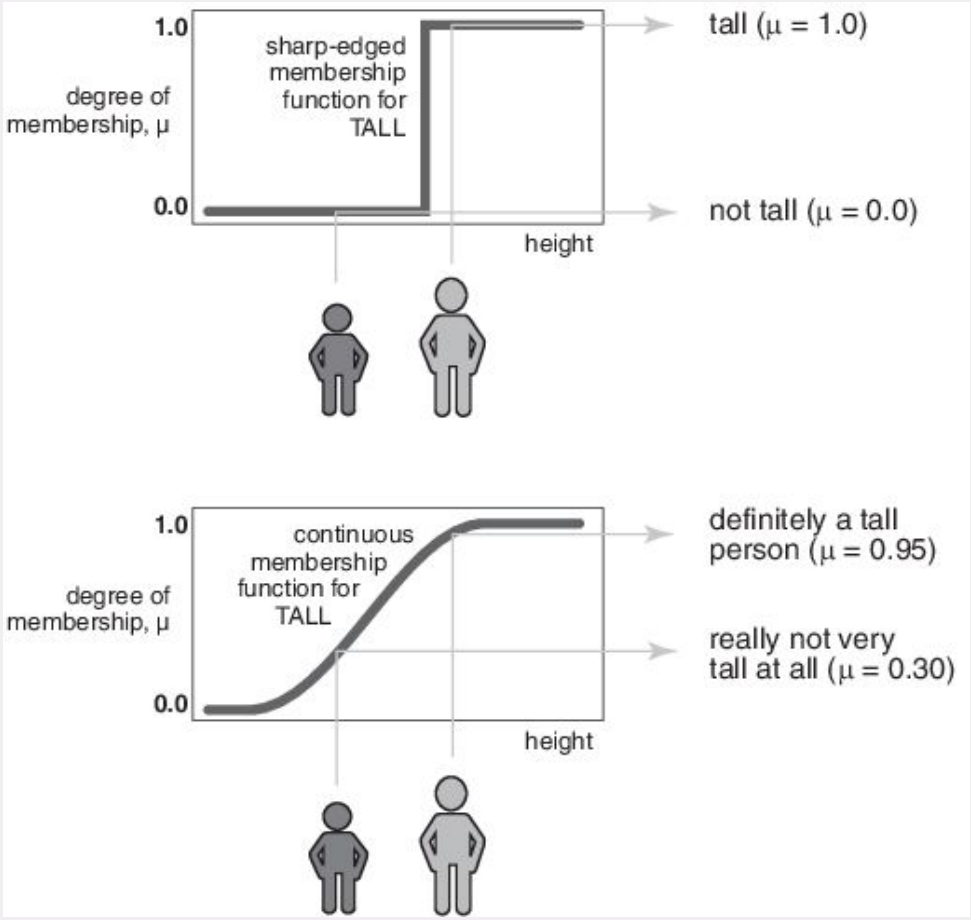




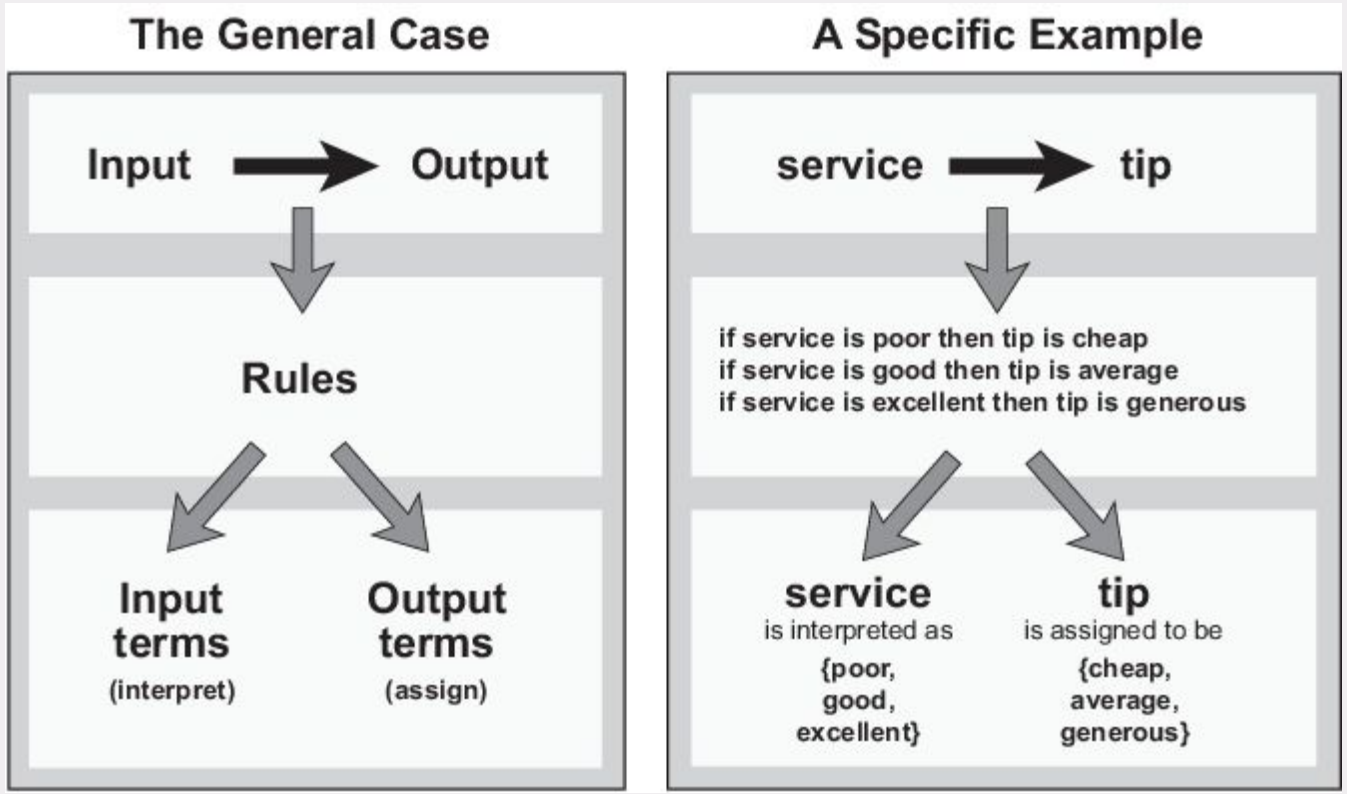
Fuzzy Membership Functions



Crisp vs Fuzzy Membership Functions



PinnacleAi PLATFORMS ™ itag TECH360°



PinnacleAi PLATFORMS ™ itag TECH360°

FCL - defined by the IEC 61131-7 standard. FCL scripts define the fuzzy system in terms of its variables (input, output), membership functions, and rule base.

```
FUNCTION_BLOCK FuzzyController

VAR_INPUT
   inputVariable1: REAL;
   inputVariable2: REAL;
   ...
END_VAR

VAR_OUTPUT
   outputVariable1: REAL;
   ...
END_VAR

FUZZIFY inputVariable1
   TERM Low: TRIANGLE (0, 25, 50);
   TERM Medium: TRIANGLE (25, 50, 75);
   TERM High: TRIANGLE (50, 75, 100);
END_FUZZIFY

FUZZIFY inputVariable2
   TERM TermName1: MF_TYPE (params);
   TERM TermName2: MF_TYPE (params);
   ...
END_FUZZIFY

DEFUZZIFY outputVariable1
   TERM LowValue: MF_TYPE (params);
   TERM MediumValue: MF_TYPE (params);
   TERM HighValue: MF_TYPE (params);
   METHOD: COG;  // Center of Gravity
   DEFAULT := 0;
END_DEFUZZIFY

RULEBLOCK RuleBlockName
   AND: MIN;  // AND method
   OR: MAX;   // OR method

   RULE 1: IF inputVariable1 IS Low AND inputVariable2 IS TermName1 THEN outputVariable1 IS LowValue;
   RULE 2: IF inputVariable1 IS Medium THEN outputVariable1 IS MediumValue;
   ...
END_RULEBLOCK

END_FUNCTION_BLOCK
```

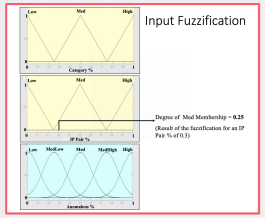
PinnacleAi PLATFORMS ™ itag TECH360°

Application

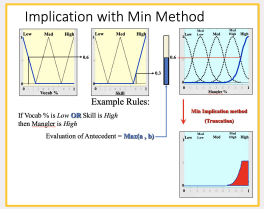
Application of the fuzzy operators for OR and AND

Aggregation

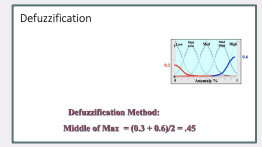
Aggregation Max used



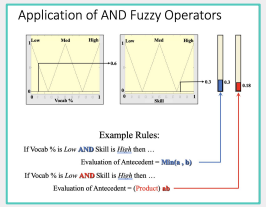
2



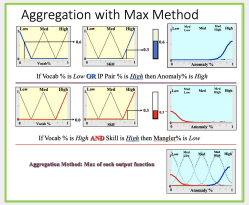
4



1



3



5

Fuzzification

Fuzzification of the input values to membership functions

Implication

If-then ruling

Defuzzification

Middle of Max used

Spear/Whaling
Targets a specific group (Spear: admins, etc., Whaling: C-Level)

Smishing/Vishing
Smishing: Text or SMS,
Vishing: Voice->RDP

Email phishing
Email at-large and sextortion

Angler Phishing
Hijacking responses

Search Engine
SEO Poisoning

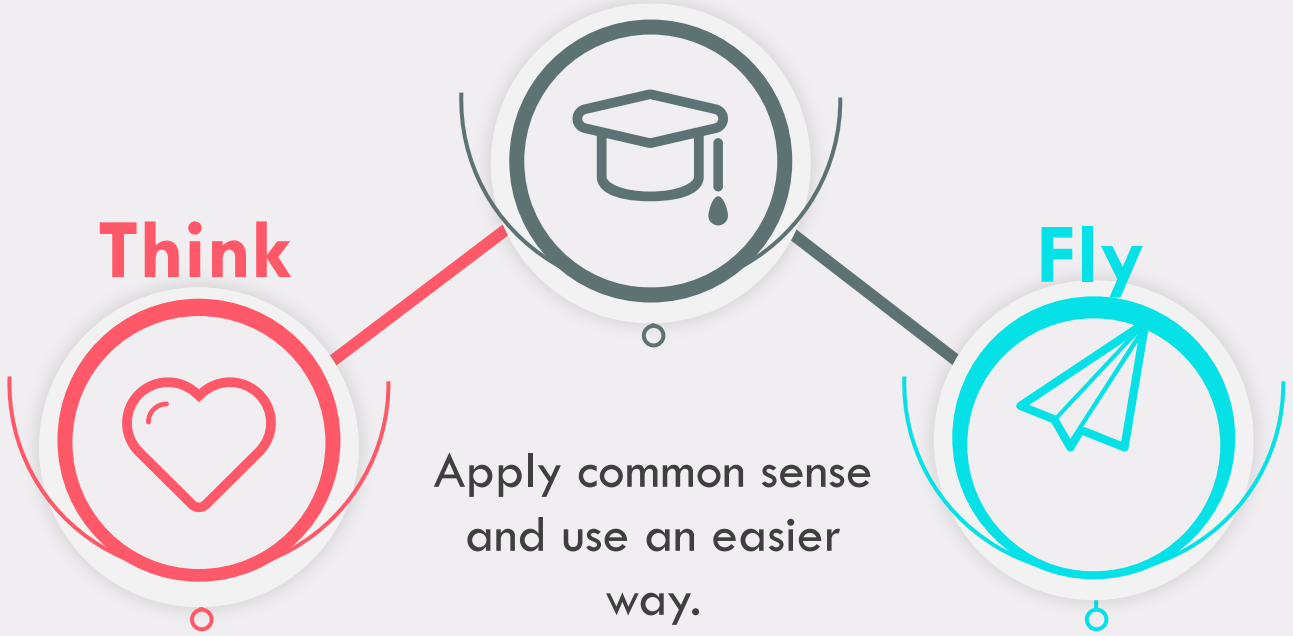
*https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html
https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack

PinnacleAi PLATFORMS

itag

TECH360°

Burdensome Test



Apply common sense and use an easier way.

Think about the process, flow, heuristic, rule set, etc.

When it makes sense, you may also see insights into other similar problems

PinnacleAi PLATFORMS

itag

TECH360°

Rule Based

Apply common sense and use an easier way.

Feature Rich

Think about the process, flow, heuristic, rule set, etc.

Eval Options

When it makes sense, you may also see insights into other similar problems

Problem Set up: Input

dataset_phishing.csv (3.66 MB)

Detail | Compact | Column — 10 of 89 columns

url	length_url	length_ho...	ip	nb_dots	nb_hyphens	nb_at
http://www.crestonwood.com/router.php	37	19	0	3	0	0
http://shadetreetechnology.com/V4/validation/a111aedc8ae390eabcfa130e041a10a4	77	23	1	1	0	0
https://support-appleld.com.secureupdate.duilawyeryork.com/ap/89e6a3b4b063b8d/?cmd=_update&dispatch=...	126	50	1	4	1	0
http://rgipt.ac.in	18	11	0	2	0	0

*DEMONSTRATING DIFFERENT PHISHING ATTACKS USING FUZZY LOGIC
Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018)
IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2

Problem Set up: Rules

a. Length of URL
Rule:IF
{URL length<54--->feature=Legitimate else if URL length>=54 and<=75--->feature=Suspicious Otherwise ---->feature=phished}
b.Using URL Shortening Services
Rule:IF
{TinyURL--->phished Otherwise---->Legitimate}
c. URL's having "@" Symbol
Rule: IF
{URL having @ symbol---->Phished Otherwise ---->Legitimate}
2. Domain based Features
a.Domain Age
Rule: IF
{Age of domain >=6 months---->Legitimate Otherwise ---->phishing
b. DNS Record
Rule:IF
{no DNS record for the domain---->Phishing Otherwise----> Legitimate}
c. Website Traffic
Rule:IF
{Website Rank<=100,000---->Legitimate Website Rank>100,000---->Suspicious Otherwise ----

d. PageRank
Rule:IF
{Pagerank<0.2---->Phishing Otherwise ---->Legitimate}
e. Google Index
Rule:IF
{Webpage indexed by google---->Legitimate Otherwise ---->Phishing}
3. HTML and JavaScript based Features
a.Status Bar Customization
Rule:IF
{onMouseOver changes Status Bar---->Phishing It doesn't change Status Bar---->Legitimate}
b.Disabling Right Click
Rule:IF
{Right click disabled---->Phishing Otherwise ---->Legitimate}
c.IFrame Redirection

*DEMONSTRATING DIFFERENT PHISHING ATTACKS USING FUZZY LOGIC
Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018)
IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2

Prompting for FCL (unrefined)

```
FUNCTION_BLOCK PhishingDetection

VAR_INPUT
   suspiciousLink: REAL; // [0, 1] - Degree of link suspiciousness
   emailSenderReputation: REAL; // [0, 1] –
Reputation of the email sender (0 being bad, 1 being good)
   urgencyLanguage: REAL; // [0, 1] - Degree of urgency in the email language
END_VAR

VAR_OUTPUT
   phishingRisk: REAL; // [0, 1] - Risk of the email being a phishing attack
END_VAR

FUZZIFY suspiciousLink
   TERM Low: TRIANGLE (0, 0.25, 0.5);
   TERM Medium: TRIANGLE (0.25, 0.5, 0.75);
   TERM High: TRIANGLE (0.5, 0.75, 1);
END_FUZZIFY

FUZZIFY emailSenderReputation
   TERM Bad: TRIANGLE (0, 0.25, 0.5);
   TERM Neutral: TRIANGLE (0.25, 0.5, 0.75);
   TERM Good: TRIANGLE (0.5, 0.75, 1);
END_FUZZIFY

FUZZIFY urgencyLanguage
   TERM Low: TRIANGLE (0, 0.25, 0.5);
   TERM Medium: TRIANGLE (0.25, 0.5, 0.75);
   TERM High: TRIANGLE (0.5, 0.75, 1);
END_FUZZIFY

DEFUZZIFY phishingRisk
   TERM Low: TRIANGLE (0, 0.25, 0.5);
   TERM Medium: TRIANGLE (0.25, 0.5, 0.75);
   TERM High: TRIANGLE (0.5, 0.75, 1);
   METHOD: COG; // Center of Gravity
   DEFAULT := 0;
END_DEFUZZIFY

RULEBLOCK PhishingRules
   AND: MIN;
   OR: MAX;

   RULE 1: IF suspiciousLink IS High AND
emailSenderReputation IS Bad THEN phishingRisk IS High;
   RULE 2: IF urgencyLanguage IS High AND
emailSenderReputation IS Neutral THEN phishingRisk IS
Medium;
   RULE 3: IF suspiciousLink IS Low AND
emailSenderReputation IS Good THEN phishingRisk IS Low;
   RULE 4: IF urgencyLanguage IS Medium AND
suspiciousLink IS Medium THEN phishingRisk IS Medium;
   // ... Additional rules can be added

END_RULEBLOCK

END_FUNCTION_BLOCK
```

Conclusions

URLs	Defuzzification methods		
	Mean of maximum principle	Weighted average method	Centroid method
http://facelook.shop.co/login.php	Phished	Highly phished	Highly phished
http://www.esmartstart.com	Highly phished	Phished	Phished
http://facebooook.axfree.com/	Suspicious	Legitimate	Suspicious
https://paytm.com/	Highly Legitimate	Legitimate	Highly Legitimate
https://www.amazon.in/	Legitimate	Highly Legitimate	Legitimate

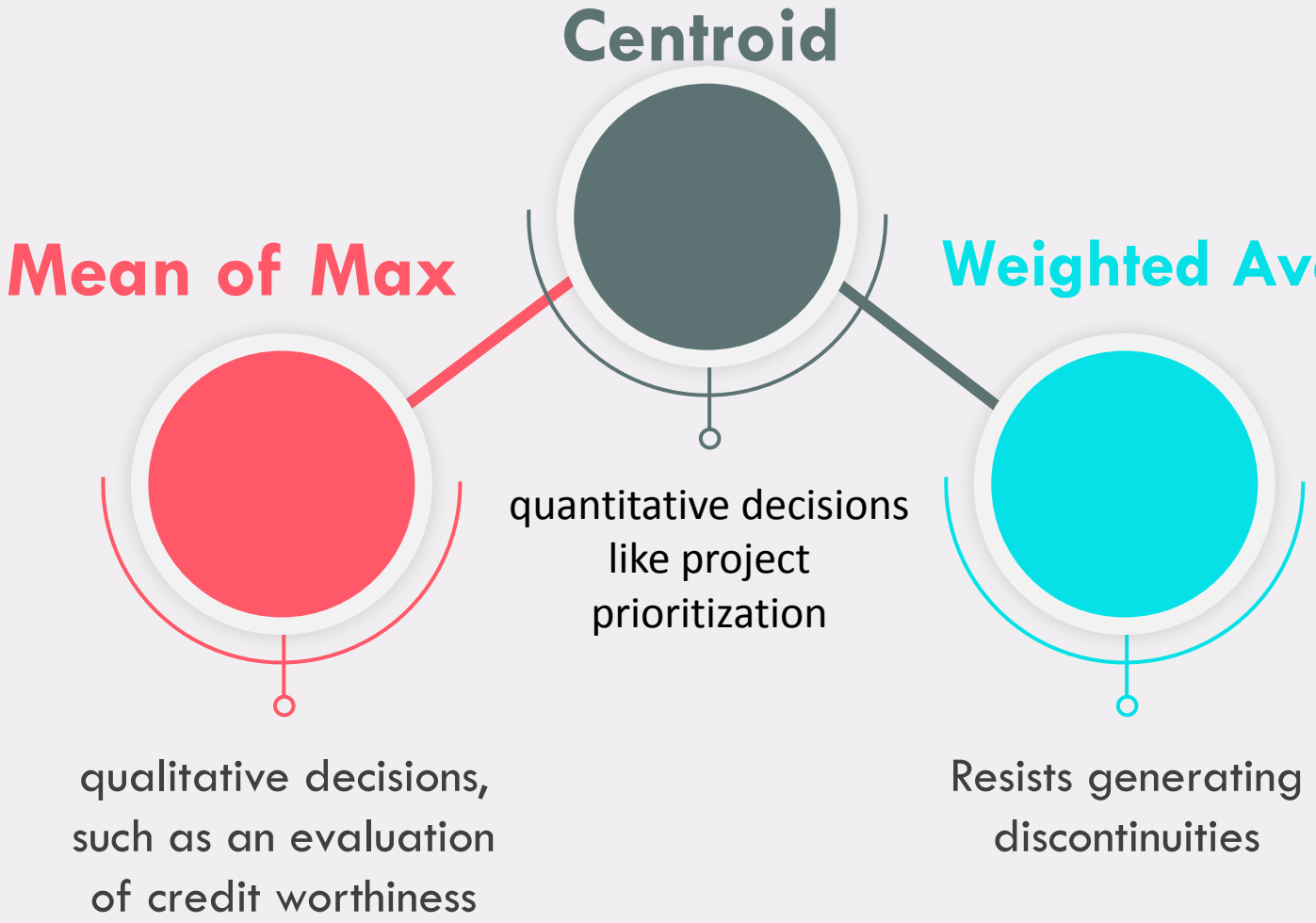
An important aspect of a defuzzification method is the continuity of the output.

*DEMONSTRATING DIFFERENT PHISHING ATTACKS USING FUZZY LOGIC
Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018)
IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2

PinnacleAi PLATFORMS

itag

TECH360°



PinnacleAi PLATFORMS

itag

TECH360°

Code

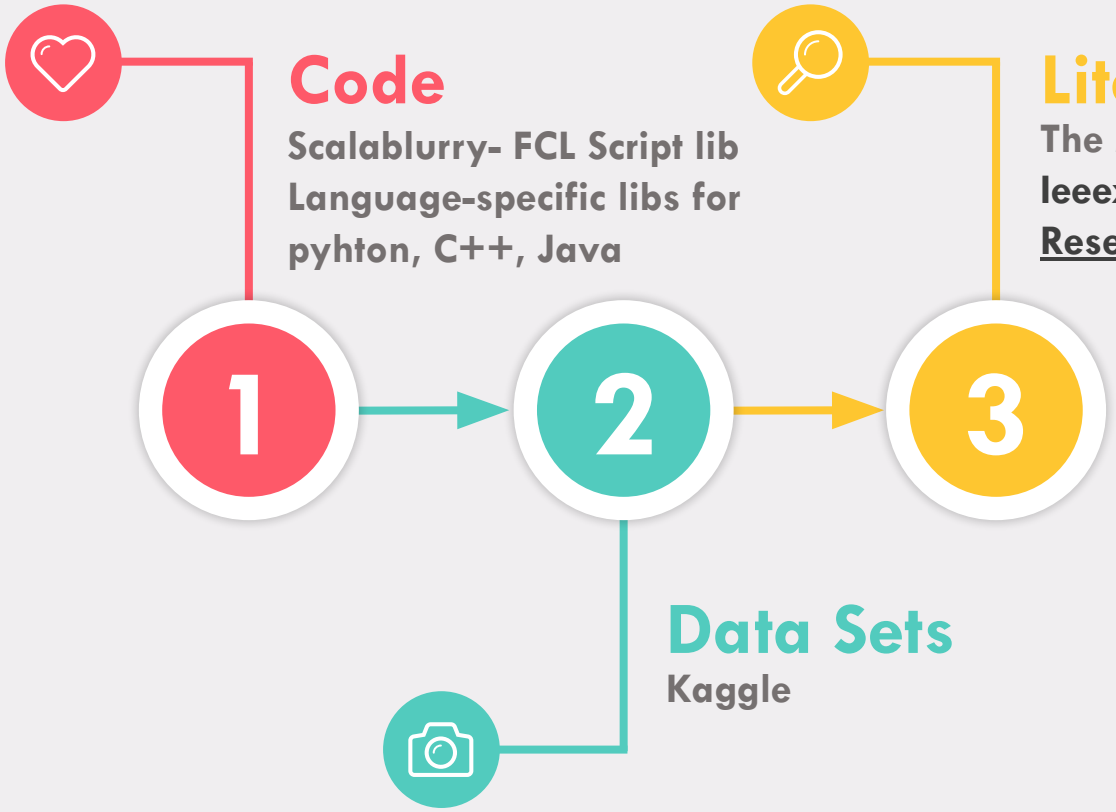
Scalablurry- FCL Script lib
Language-specific libs for
pyhton, C++, Java

Literature

The Mathworks,
Ieeexplore, ACM,
Research Gate

Data Sets

Kaggle



Thank You!

PinnacleAi PLATFORMS

Raymond Garcia, Ph.D.

Co-Founder & Chief of Technology

ray@1pinnacleai.com

LinkedIn

YouTube rgvidworld

raygarcia