# Cognitive Automation with Machine Learning in Cyber Security

Rishi Kant
Independent Cyber Security Researcher, *RishiKant.in*

# AGENDA

**Cognitive Automation & Machine Learning**

Introduction, Their Processes, Learning Curve, Examples

**Cyber Security & It's challenges**

CS changing trend, Dealing of Challenges with ML

**Improvisation of Cyber Security Resilience**

Threat Analytics, Fraud Detection, Security In cident, Intrusion Detection

**Cyber Risk Management**

Cyber Risk Analytics, Evaluation of Risk

# Section Break

About Me

# Welcome!!

RISHI KANT

I am a Security professional with 11+ years of experience (independent or corporate) in the field of Cyber Security, Information Security, Digital Forensics, IT Administration, Secure Software Development, Training, and company operations. I worked in various industry verticals such as IT/ITES, E-Commerce, Government, BFSI and law-enforcement agencies

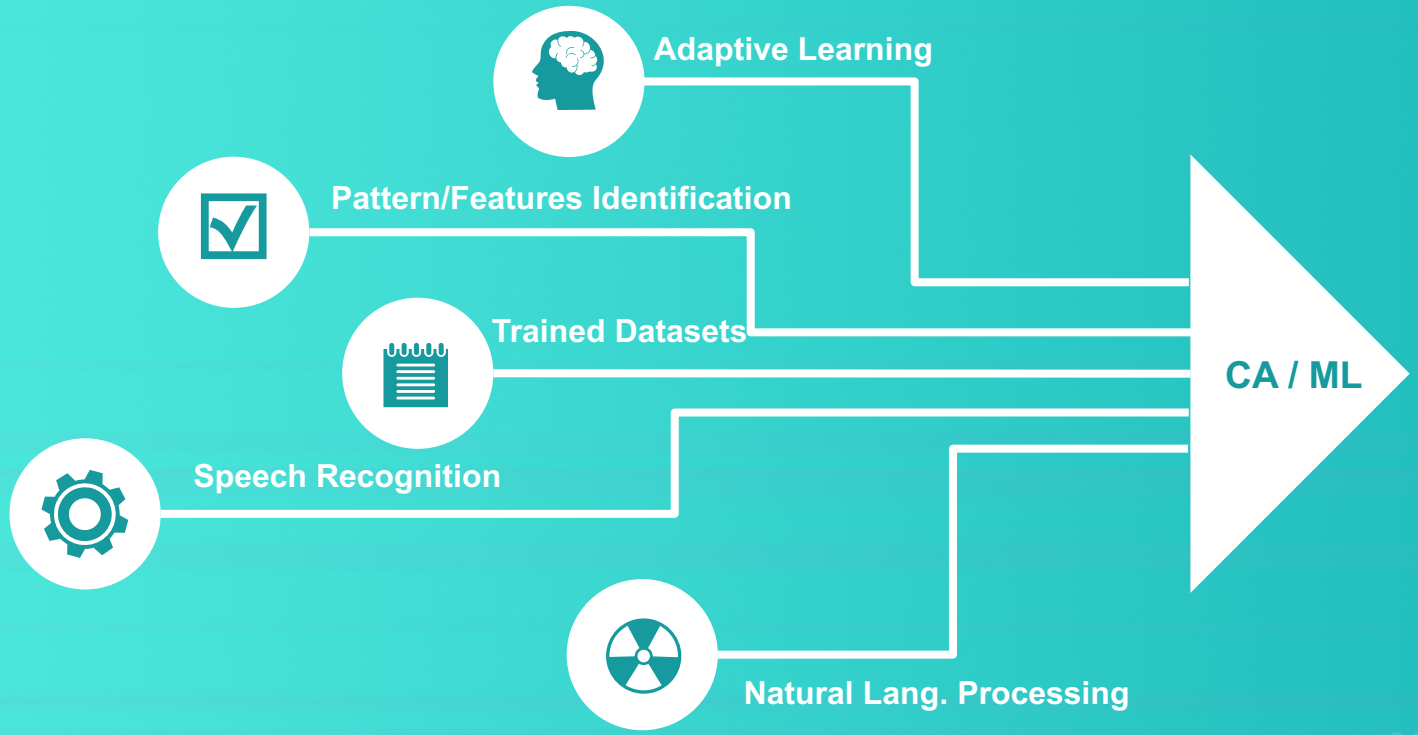
https://www.linkedin.com/in/hrishikant

# Section Break

Cognitive Automation & Machine Learning

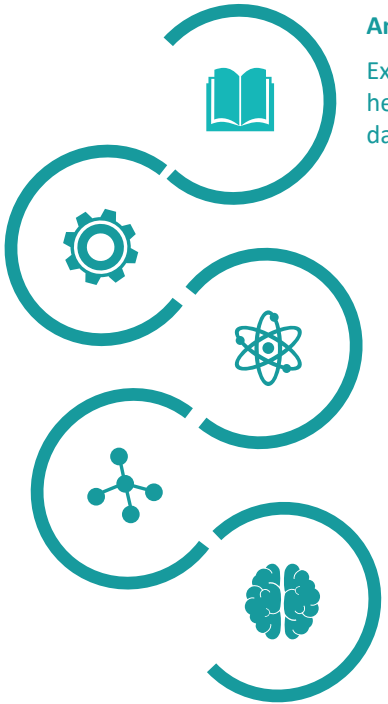
# Cognitive Automation & Machine Learn.

Major Elements



# Cognitive Automation & Machine Learn.

Simple Process flow



**Analysis of Data**

Examination of the all type of data for anomaly, healthy data, tamper data, unused data, critical data and others

**Extraction of features**

Extraction, clustering, grouping, classification of data on the basis of their criticality.

**Selection of unique features**

Anomalies action like malicious code, unusual transactions, unapproved tasks, net traffic, threat feeds

**Creating useful datasets**

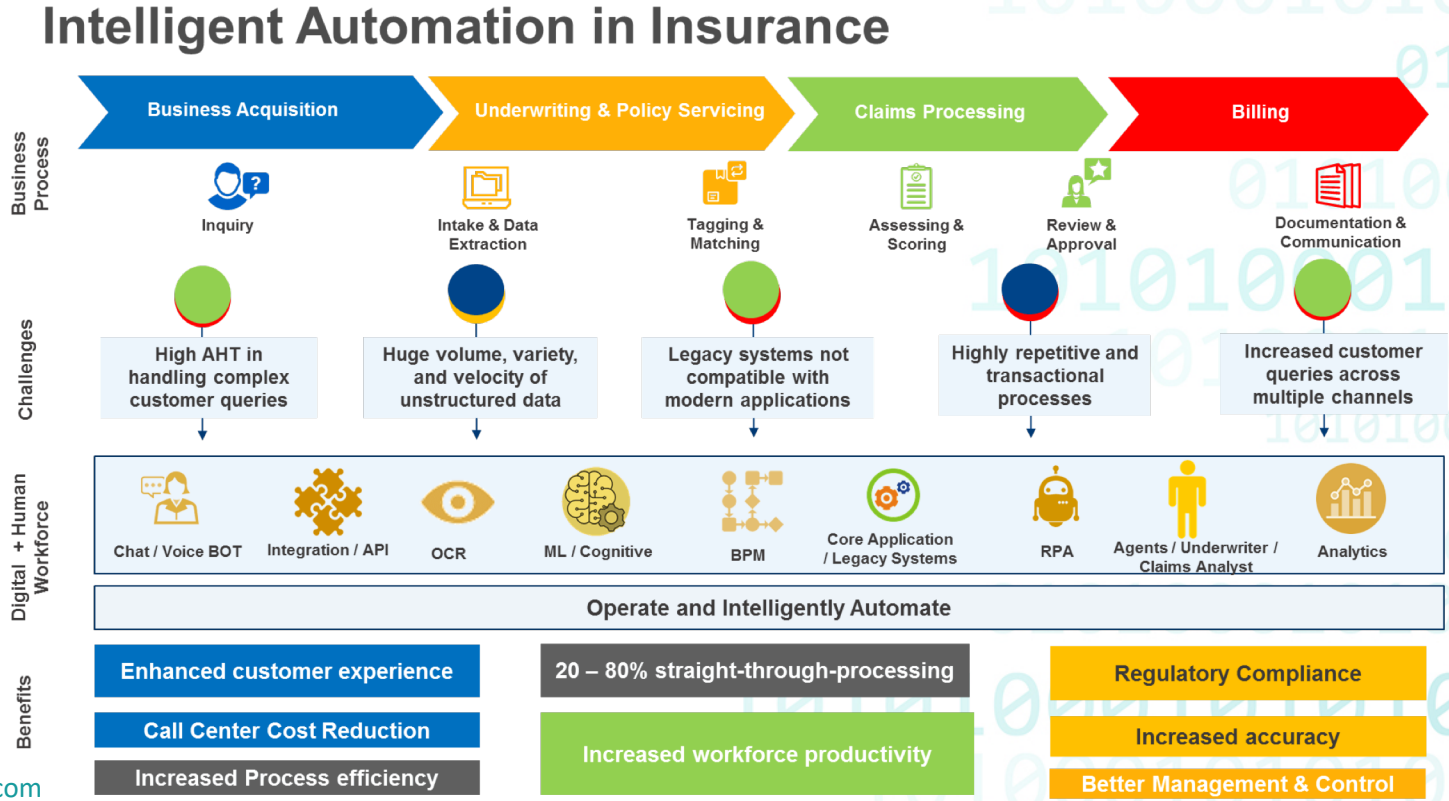
It's like trained machine, Creation of datasets on the basis of unique features.

**Selection of unique features**

Evaluation of real data on the basis of trained datasets for anomalies detection on the basis of confidence coefficient.

# Cognitive Automation & Machine Learn.

Example in Insurance




InSource: hexaware.com

# Section Break

Cyber Security & It’s Challenges

# IS Controls timeline

## Traditional

### Mathematical Model

Deals problems were aided by mathematical models like cryptography (analog basis or digital basis).

We can easily predict by past experience of attacks (before 2000).

Some of attacks:
(1980-1990)
The 414s, Bank of Chicago, Catch the wave
(1990-2000)
Operation SunDevil, Citibank, Level Seven, The Media are Liars

## Modern

### Strategic Model

Deals with abstract threats which cannot be solved only by using mathematical models. Ex: Intrusion detection, Data leakage, SPAM mitigation

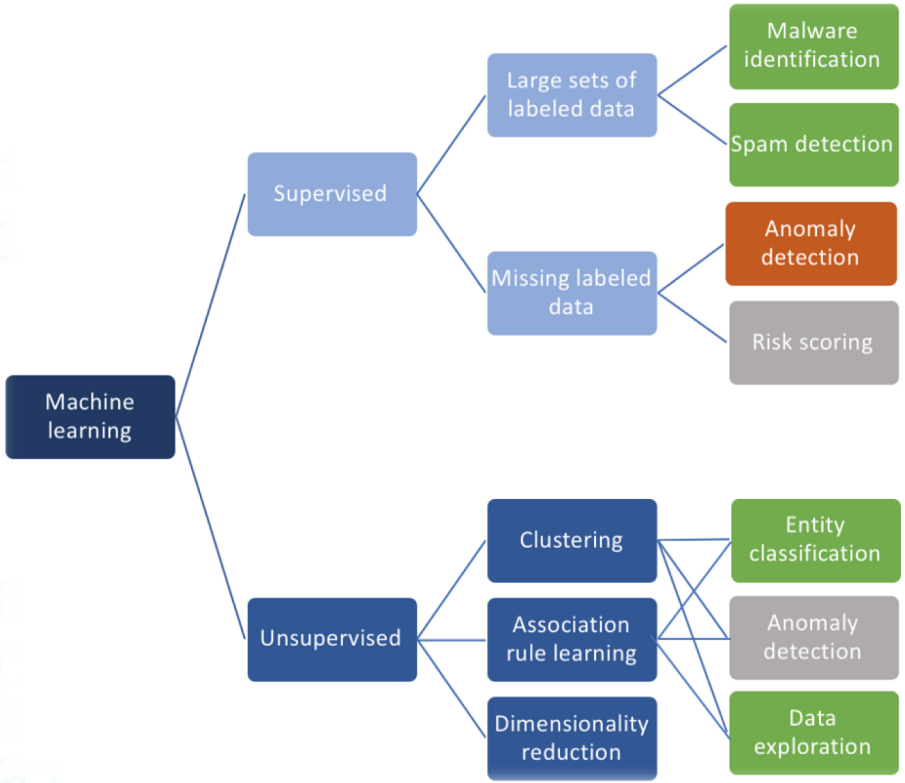
We can eaily predict by past experince of attacks.

Some of attacks:
(2000-2009)
I Love You Bug, Nasa No-Go, Zombie King,
(2010-2020)
Stuxnet Worm, PlayStation, Year of the Tiger, WHMCS

** Machine learning add the value as it will work on the basis of prediction and adaptive learning while cognitive add the value in process optimization, staff reduction and get away from redundant work*

# Cyber Security & It's Challenges

Utilization of machine learning in Some of Cyber Security practices




## Some Others

Spam Mitigation
Malware Detection
Mitigation the Denial of Service Attacks
User Identification
Detecting Identity Theft
Information Leakage Detection & Prevention
Detecting Advanced Persisted Threats
Detecting Hidden Channels

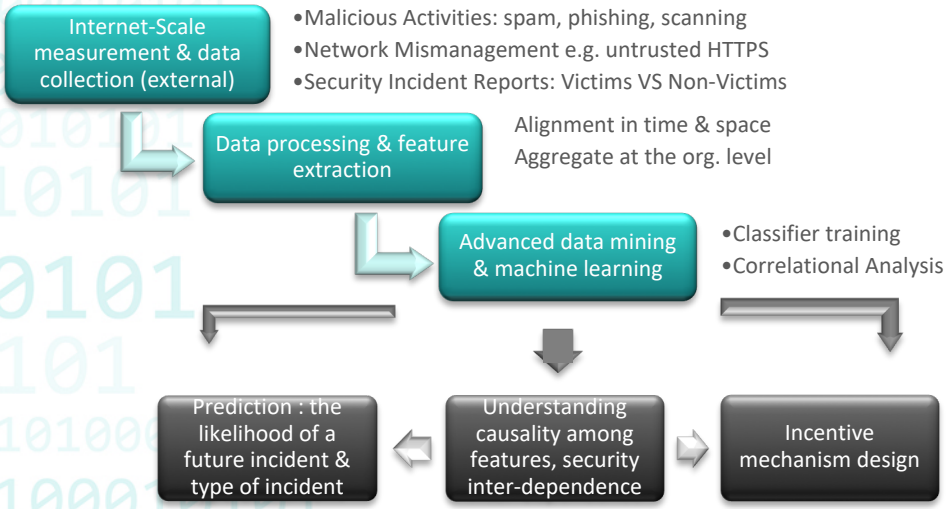
# Section Break

Improvisation of Cyber Security Resilience

# Improvisation of Cyber Security Resilience

Different flows

## Security Incident



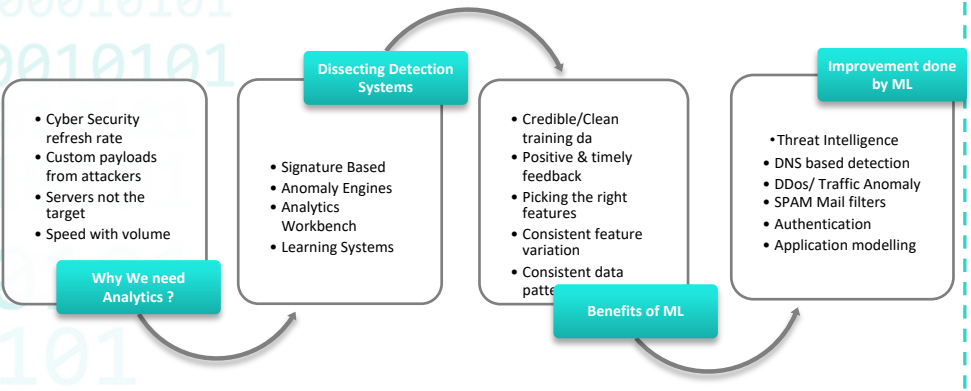

## Fraud Detection

| | Method | Human Involvement | Speed | Accuracy |
|---|---|---|---|---|
| Traditional Detection | • Rely on pattern matching against recognised past fraud types. Transactions then assessed based on general **rules**, such as whether the customer is buying abroad.<br>• Humans to identify trends and manually update their models to account for changes in fraudulent activity. | • **High**<br>• Requires significant manual analysis and review, with regular updates to fraud systems. | • **Medium**<br>• More human involvement, often using audit trails to identify fraud.<br>• Less computing power. | • **Medium**<br>• Often corrective over preventive with limited use of data, meaning lower detection success rates. |
| Machine Learning | • Algorithms analyse historical transaction data for each customer to understand their individual spending patterns. **They can therefore spot subtle anomalies that indicate fraud.**<br>• Algorithms self-learn, meaning they quickly adapt to new means of fraud, and can stay ahead of fraudsters. | • **Low**<br>• Automatic - humans to maintain the algorithmic models. | • **High**<br>• Real-time, automatic reviews of transactions using vast amounts of data from multiple sources. | • **High**<br>• Preventive over corrective, meaning higher rates of fraud detection and fewer false alarms. |

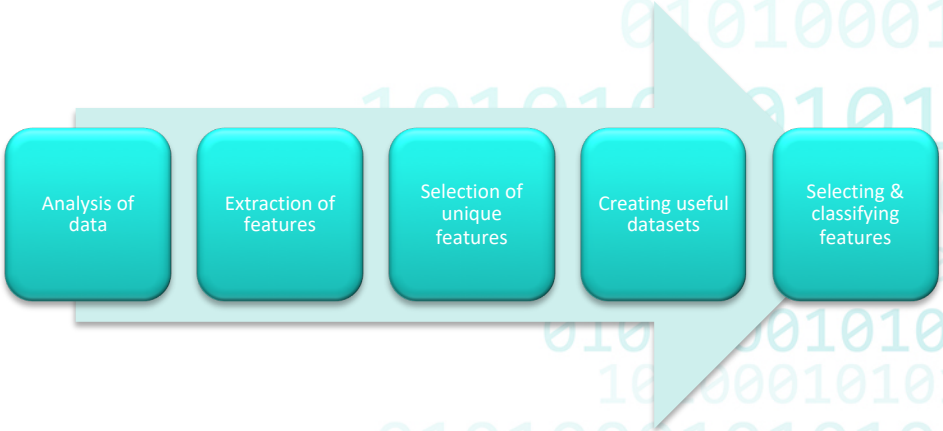
# Improvisation of Cyber Security Resilience

Different flows

## Intrusion Detection




## Threat Analytics

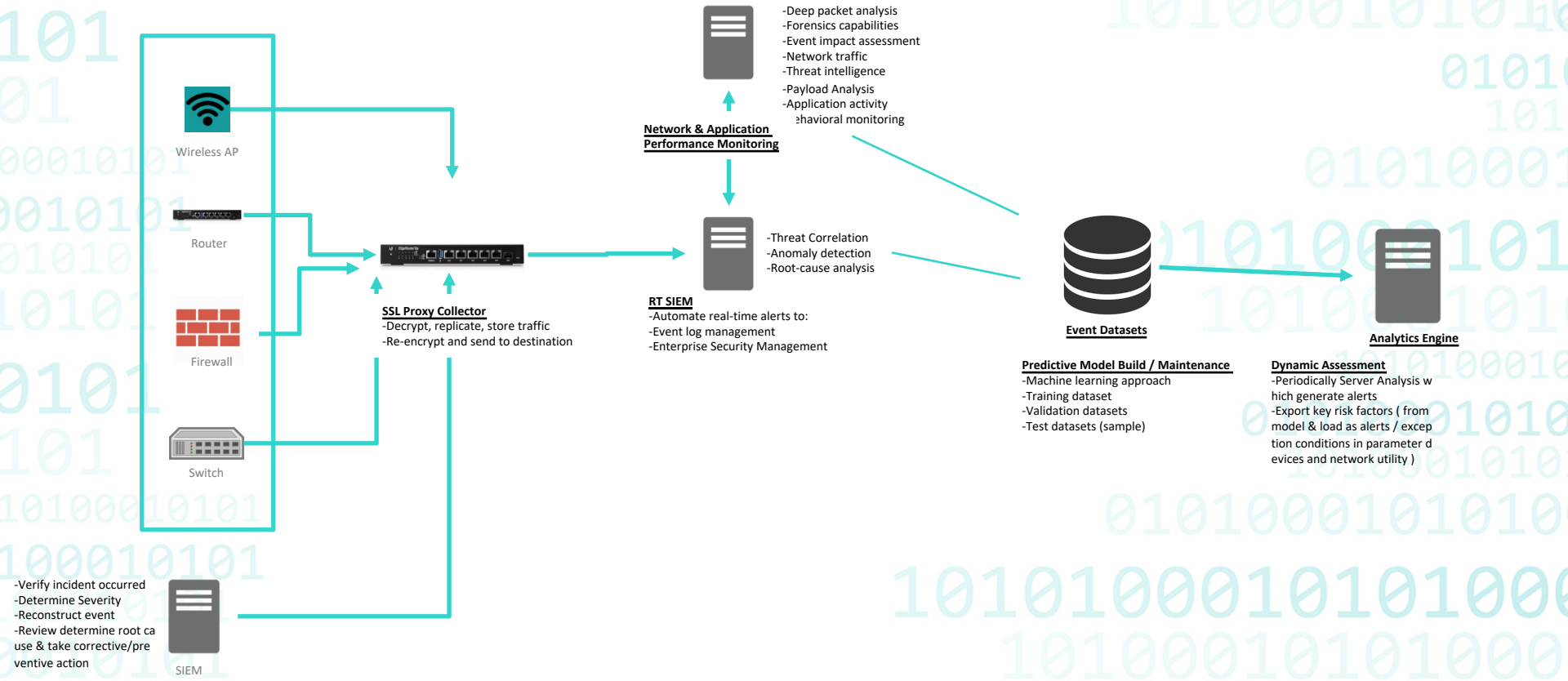


# Section Break

Cyber Risk Management

# Cyber Risk Management

## Cyber Risk Analytics



# Thank you

It’s pleasure to share my experience with you guys!

Please ask your questions or mail me: Rishi-kant@live.in