Data analytics for Cyber security

-Future Directions in Data Analytics for Cybersecurity-

Vandana P. Janeja

Outline

Data Analytics in Cyberphysical Systems

- Cyberphysical Systems
- Internet-of-Things (IoT)

Multidomain Mining

- Integrating Multiple Heterogeneous Data
- Integrated Alerts from Multiple Sources

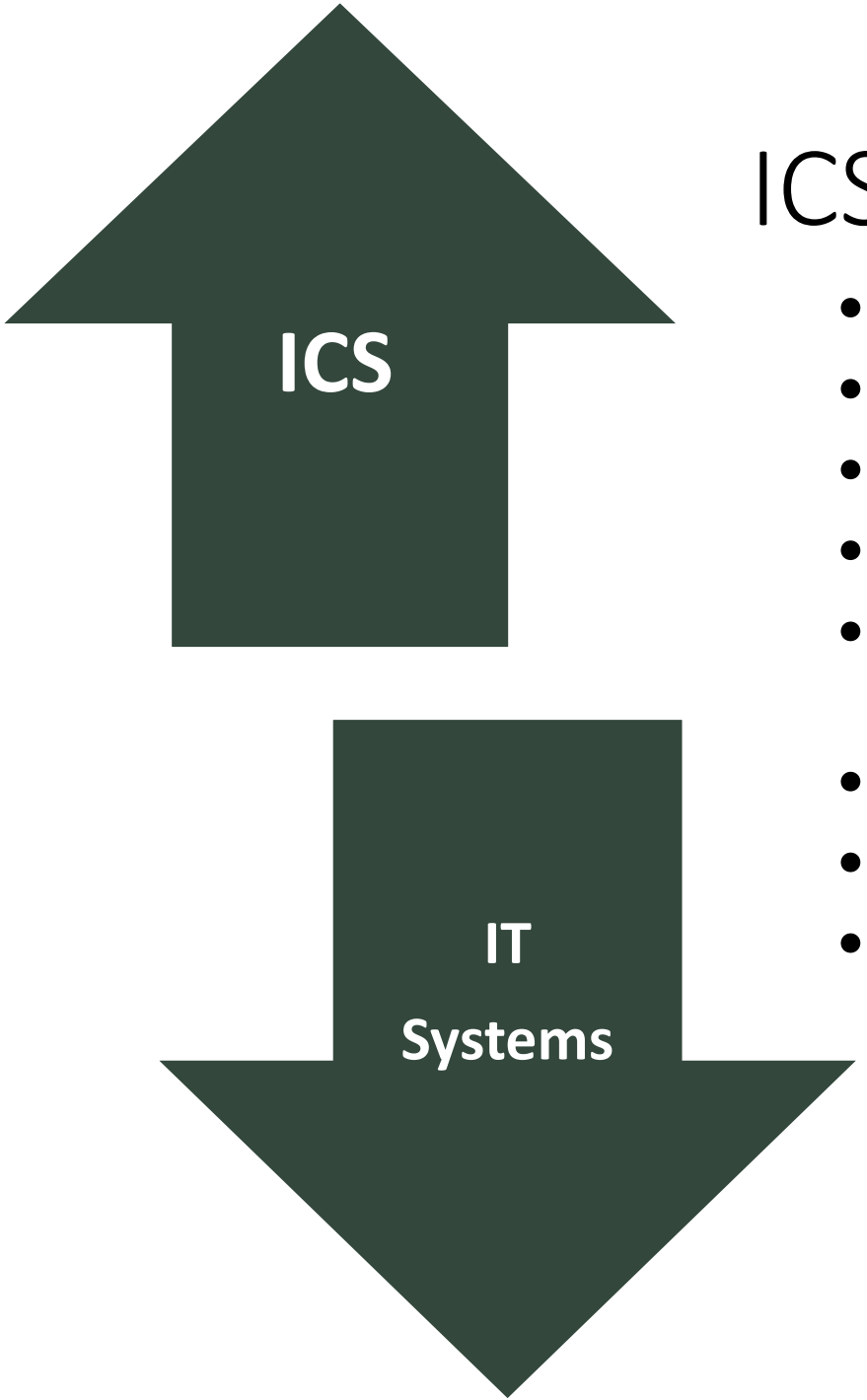
Advanced Machine Learning Models

- Deep Learning
- Generative Adversarial Networks
- Model Reuse

Ethical Thinking in the Data Analytics Process

Data Analytics in Cyberphysical Systems

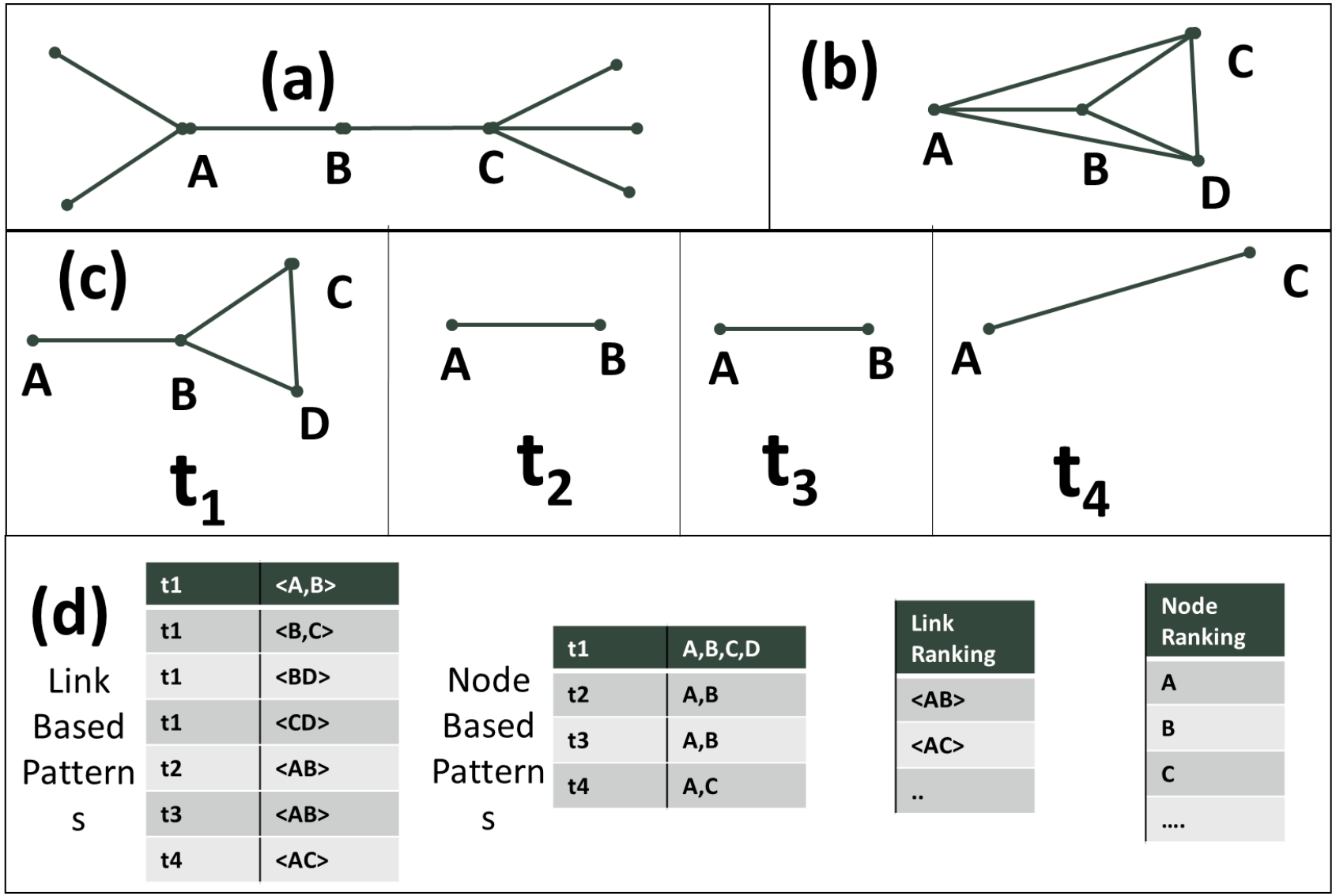
- Cyber Physical Systems are formed as a result of an integration and interaction of the cyber and physical systems. This introduces many interesting issues in managing, monitoring and analyzing these interactions and interfaces
- One major category of CPS is the Industrial Control Systems (ICS)
- Traditional ICS has comprised of Supervisory Control and Data acquisition (SCADA) systems, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC) found in the industrial sectors and critical infrastructures
- These are used for industries such as electrical, water, oil, gas and energy
- Traditionally ICS has been considered a much more physical process oriented space as compared to traditional information technology systems
- As a result cyber attack on an ICS will have much bigger impact on the health and safety of people, impact the economy
- These systems will also have a higher emphasis on reliability and accurate performance
- System integrity and availability have a much more emphasis as these systems cannot be offline for long periods
- There are redundancy requirements in events of failure
- All these are also brought into focus with the interactions with the physical domains
- One of the key vulnerability identified in the Guide to Industrial Control Systems (ICS) Security is stated as,”Lack of redundancy in critical components could provide single point of failure possibilities”
- The signals sent between the various sensors and the control units can be mapped similar to a network communication flow between IP addresses



ICS vs. IT Systems

- Health and safety of people, national economy
- Performance and reliability requirements
- System Integrity requirements
- Proprietary control protocols
- Difficulty in change and update to operating systems
- Availability Requirements
- Redundancy requirements
- Interactions with physical domains

Temporal evaluation of a sensor network



(d)

Link Based Patterns

t1	<A,B>
t1	<B,C>
t1	<BD>
t1	<CD>
t2	<AB>
t3	<AB>
t4	<AC>

Node Based Patterns

t1	A,B,C,D
t2	A,B
t3	A,B
t4	A,C

Link Ranking
<AB>
<AC>
..

Node Ranking
A
B
C
....

Data Analytics in Cyberphysical Systems

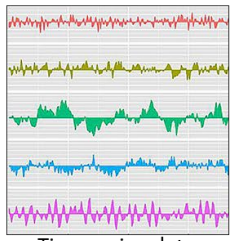
- Sensor networking and its applications can be adapted to Industrial Control Systems (ICS) and computer networks for supporting cybersecurity
- Let us consider a part of the sensor network where the nodes A, B, C, D
- We evaluate the nodes based on connections or number of links in (a)
- Here nodes A and C can be considered important as they are connecting hubs, where a large number of edges are incident, indicating a high degree of communication
- Similarly node B can be considered important because it is a connector between the two hubs
- However, in (b), we see a different scenario, where it is difficult to determine the clear importance based on links
- Thus, simply using metrics such as centrality, focusing on the number of edges incident on a node, may not be the best or even feasible
- Evaluating the critical nodes based on their behavior over time is much more useful here
- This behavior can be captured in terms of relationship based on edges between nodes, which could represent data transfers between nodes, such as in a computer network or an ICS network
- For example, in (c), the data transfers at time t1, t2, t3 for the network in (b) are shown
- These can now be used for link based patterns, or node based patterns to produce a ranking of links and nodes by importance, in terms of how many times they appear in the temporal windows as shown in (d)
- These can be mined in an association rule based method
- Certain time periods may be more important and thus, may be given more weight, which may be mined using quantitative association rule based methods

Internet-of-Things (IoT)

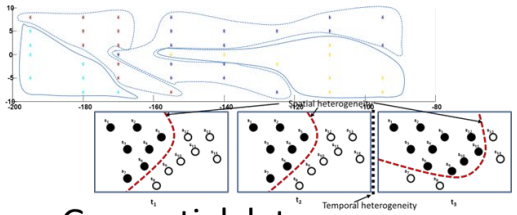
- Internet-Of-things (IoT) is interchangeably used and considered as complimentary to CPS in some studies
- Other studies have distinguished IoT as a class of CPS or seen it as intersecting with CPS
- IoT has indeed become a big share of the CPS space due to the explosion of the number of devices and advancements of smart devices and sensors
- Even though estimates vary, they are projected to grow anywhere from 18 billion to 50 billion devices worldwide by 2020
- This is a very large number of devices by any estimate and creates more security challenges given the highly unregulated and non-standard market for IoT devices
- One such space where smart devices have created this interesting intersection between cyber physical and Internet of Things is a smart car
- We are making our vehicles smart, fully connected with Internet to view real time traffic and weather, talk on the phone with Bluetooth, listen to the radio, watch video as well as getting real time status of automobile's mechanical functions
- However, this smart interface comes with a price, which is the vulnerability to threats as well as malfunctions to mechanical parts of the vehicle
- Other areas where IoT has taken a big role is in home security systems with fire alarms, CO monitors, door and garage sensors alarms, temperature control sensors

IoT examples: car and home sensors

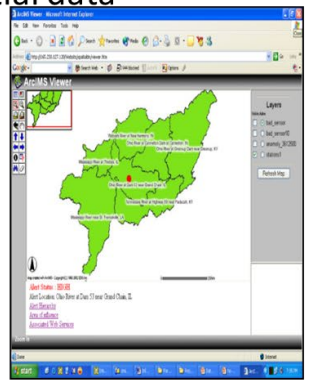
Smart Devices



Time series data



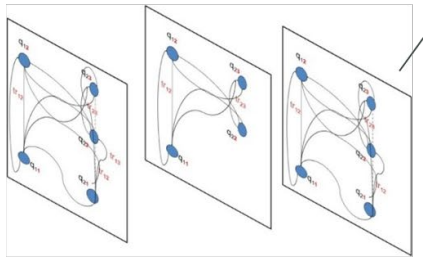
Geospatial data



Multiple Data Standards

- MQTT
- CoAP
- Lightweight M2M
- OMA NGSI-9/10

Analytics for IoT



Multi-dimensional views of data

Vehicle on board diagnostics data

IoT

- Let us consider a smart home with a series of devices measuring various phenomena around them
- In such a setting, depicted, several smart devices collect the information from a location with different levels of precision, collecting different data streams, perhaps using different standards
- We may want to evaluate behavioral aspects such as: How are we using our devices? Are there behavioral trends?
- We may also want to evaluate aspects of something anomalous in this complex space such as: Are there deviations from these trends? How do we discover threats and attacks?
- The data collected here is often of different modalities including spatial, temporal, image and text data
- The data can also be sliced in a multi-dimensional view over time
- The attack space is simply unmanageable
- Let us consider an example of a recent case study evaluating an incident at a university had close to 5000 systems making DNS lookups every 15 minutes
- In our current connected environments edge devices, vending machines, environmental systems, alarm systems, light bulbs and every other connected device on a university campus can lead to a massive attack space - This truly becomes a needle in the haystack problem
- Unlike companies and businesses where the responsibility of preventing and mitigating an attack is on the system administrators, where does this responsibility lie in an IoT scenario?
- It lies both with the device maker and the user
- This still creates difficult scenarios where IoT use is occurring in a public or shared space
- This landscape is one of the frontiers of cybersecurity and developing of novel data analytics solutions for such a space

Multi Domain Mining

- Data in real world is generated by multiple sources and is often heterogeneous in terms of the types of attributes in each dataset
- To be preemptive and provide actionable insights data from multiple sources need to be analyzed
- Such type of mining is referred to as multi-domain mining, where domain refers to distinct sources of data and these distinct sources may be completely disparately generated
- A Couple of examples are discussed to highlight the challenges and potential solutions to analyzing disparate data sources to provide actionable knowledge for events

Multi Domain Mining: Integrating multiple heterogeneous data

- In a computer network there are various mechanisms to allow for analyzing the network traffic data
- There may be scenarios where we want to expand the decision criteria especially when we may not have access to any traffic data, such as payload, but only header information
- In such a scenarios we can augment the header information with other types of data
- One such view point is that of a geospatial data which can enhance the knowledge of the IP session or even the IP reputation score itself

Multi Domain Mining: Integrating multiple heterogeneous data-IP Reputation scoring

- Current reputation systems pursue classification into a white and black list, i.e., binary categorization
- Separate lists for URLs and IP addresses are maintained
- Some tools that provide rudimentary reputation services include Cisco SenderBase (https://www.senderbase.org/), VirusTotal IP reputation (https://www.virustotal.com/) and Spam and Open Relay Blocking System (SORBS) (http://www.sorbs.net/)
- Most of these tools and lists are based on single dimensional features with no correlation among them
- Such shortcoming degrades a system's effectiveness for detecting sophisticated attacks and terminating malicious activities
- However, the set of attributes that the reputation scoring considers can be enriched, providing an expressive scoring system that enables an administrator to understand what is at stake, and increasing robustness by correlating the various pieces of information while factoring in the trustworthiness of their sources

Multi Domain Mining: Integrating multiple heterogeneous data-IP Reputation scoring

- IP reputation scoring model can be enriched using network session features and geo-contextual features such that the incoming session IP is labelled based on most similar IP addresses, both in terms of network features and geo-contextual features
- This can provide better threat assessment by considering not only the network features but also additional context, such as the geospatial context information collected from external sources
- Indeed in some countries, networks may encounter or even host large quantities of attacks as compared to others
- This may be due to shortage of cyber security expertise, level of development, the abundance of resources, corruption levels, or the computing culture in these countries (Mezzour 2015)
- Identifying these factors and quantifying them can provide insights into security policies and have a positive impact on the attack incidents
- These scenarios not only impact the countries facing such cybersecurity crises but also impact other countries and end users due to the level of connectivity in today's day and age
- Studies have also identified regions across the world which are prone to hosting certain types of attacks
- For example, studies have indicated that Trojans, worms and viruses are most prevalent in Sub-Saharan Africa (Mezzour 2015), some families of malware preferentially target Europe and US (Caballero 2011)
- Yet other studies (Wang 2009) have explained broad categories of worldwide systemic risks and country-specific risks where country specific risks include aspects of economy, technology, industry and international cooperation in enforcement of laws and policies

Sources of Geospatial data relevant to cybersecurity events with geopolitical aspects

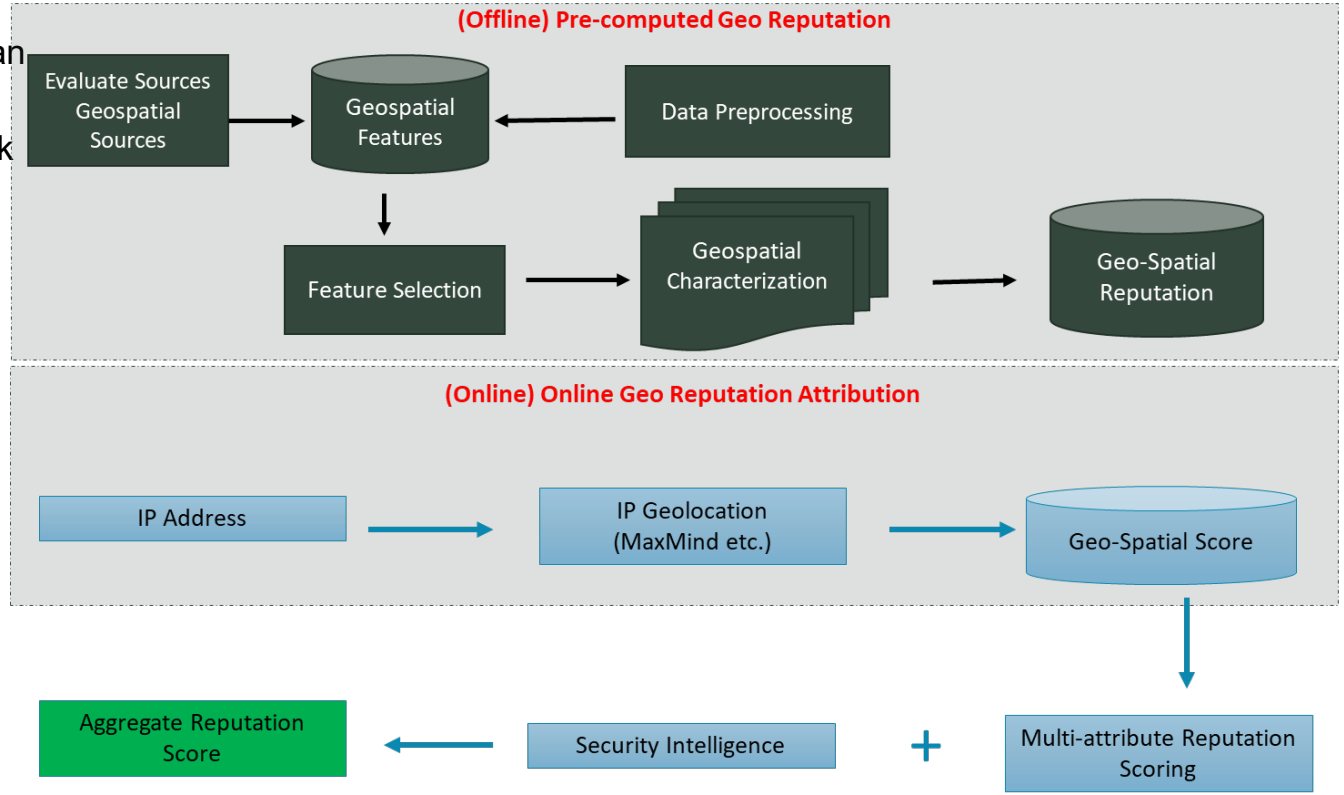
IP2Location	IPligence	U.S. National Geospatial-Intelligence Agency	MaxMind GeoIP	Neustar IP GeoPoint	Digital Element NetAcuity
Natural Earth Data	Capec MITRE	Diva GIS	UNEP Environment Data Explorer	Koordinates	MapCruzin
FAO GeoNetwork	European Environmental Agency	(Global Self-consistent, Hierarchical, High-resolution Geography Database) GSHHS	World Bank Open Data	Atlas of the biosphere	USAID Geoportal
US AID - Monitoring Country Progress (MCP) System	US AID - Health System Benchmarking Tool	ESPON Database Portal	Google Maps Gallery	History Database of the Global Environment	(Armed Conflict Location & Event Data Project) ACLED
Uppsala Conflict Data Programme (UCDP)	Global Terrorism Database (GTD)	Peace Research Institute Oslo (PRIO) PRIO-GRID	SEDAC - Gridded Population of the World (GPW)	SEDAC - Global Rural-Urban Mapping Project	Worldpop.org
Nordpil (Large Urban Areas 1950-2050)	Nelson WISC (Global Urban Extent)	GeoHive	US City Open Data Census	Stat Silk	United Nations Statistical Division (UNSD)

Multi Domain Mining: Integrating multiple heterogeneous data

- Geospatial data not only provides additional context but provides a framework to accommodate additional geo-political information which often plays a big role in hactivism or politically inspired attacks
- The figure provides a set of rich sources to access geospatial data for countries and in some cases even at a granular level of cities
- Some of these sources such as Ip2location provide a way to identify a user location based on IP address in a non-intrusive manner
- Several other data sources such as Worldbank open data (https://data.worldbank.org/), PIOR-GRID (http://grid.prio.org/#/), ACLED (https://www.acleddata.com/) data provide socio-political and geo political conflict data

Multi Domain Mining: Integrating multiple heterogeneous data

- Such data can be used to create Geospatial characterization of regions (for example using methods proposed by Janeja et. al. 2010)
- When an IP address is encountered it can be geolocated using the IP location databases such as Ip2location or Maxmind
- Based on its geolocation the location score from the characterization can be attributed to it
- The geospatial attributes for this region can be appended to the network attributes for this IP (Sainani 2018)
- Any additional security intelligence can be appended to provide an aggregate reputation score to this IP
- The data heterogeneity in terms of types of attributes, namely categorical vs. continuous can be addressed using methods which are capable of handling mixed attribute datasets (such as Misal 2016)

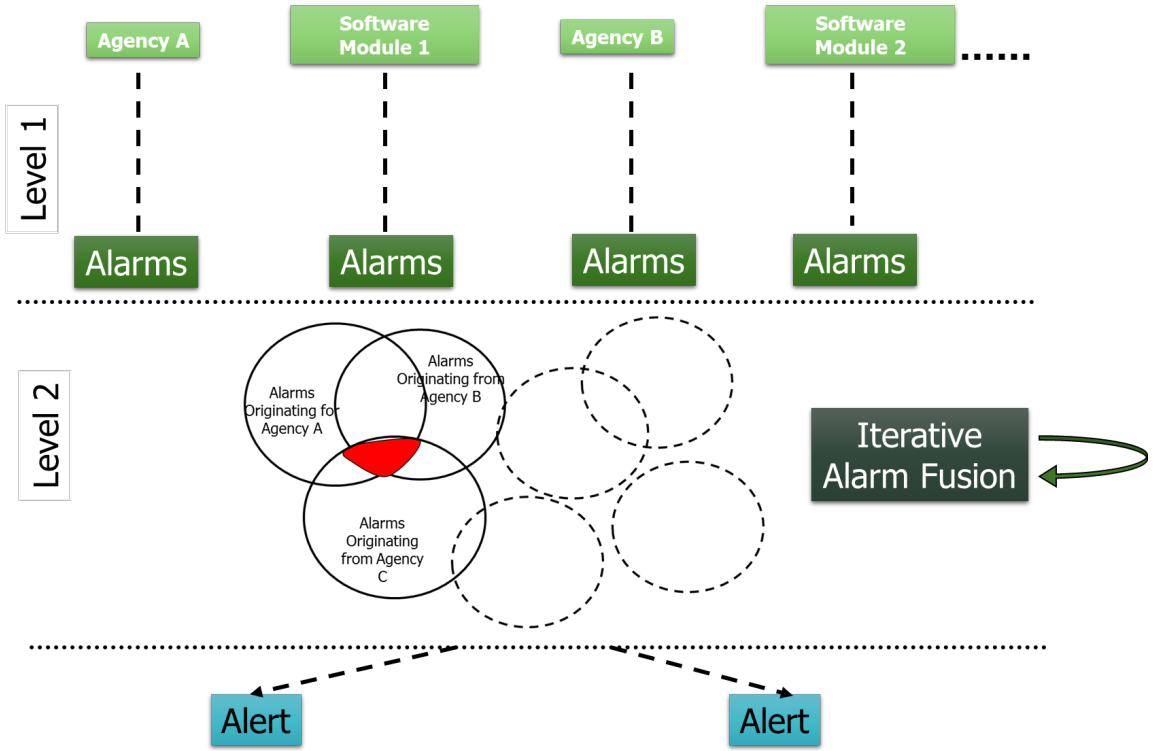


Integrated alerts from multiple sources

- Computer networks are increasingly facing the threat of unauthorized access
- Other networks such as sensor networks, industrial control systems also face similar threats
- Intrusion detection aims at identifying such threats using signatures of unauthorized access or attacks
- There are very few systems which address the issue of ‘zero day’ attacks where the attack signature is not known before-hand
- Let us consider a scenario where the threat is two pronged first there is an attack on the organization and second there is an attack on a partner which shares key resources
- In the first part of the attack intruders take advantage of vulnerabilities in public-facing web servers
- In addition hackers secretively scout the network from compromised workstations which have already been targeted beforehand as part of a coordinated prolonged attack
- The second part of the attack starts with spear-phishing
- Instead of casting out thousands of e-mails randomly, spear phishers target select groups of people with something in common such as common employer, similar banking or financial institution, same college, etc.
- The e-mails are deceptive since they appear to be from organizations from which victims are expecting emails
- Potentially a second group of hackers institutes a spear-phishing attack on the organization’s major business partners, with which it shares network resources
- The hackers are able to obtain a privileged account and compromise a root domain controller that is shared by the organization and its partner
- When the intruders try to recreate and assign privileges, it triggers an alarm

Integrated alerts from multiple sources

- In this scenario where the attack is distributed, it may be difficult to integrate these alarms to identify if this is a single malicious attack or the attack may be spread out over time
- This requires the discovery of an integrated alert from alarms generated from disparate sources across a prolonged period of time as shown in the figure.
- Each alarm generated has a set of attributes such as the source and destination of the data, port, length of data packet, etc.
- Each source generating the alarm is also described through a set of attributes such as type, port frequently used, etc.
- The series of alarms received in such a complex application domain is composed of the raw messages received from multiple sources and an alert is the processed and aggregated output generated from these alarms
- Such an approach for the alarm data fusion would include alarm source characterization and alarm clustering using source characterization and temporal lag determination
- The alarms could be generated from a single source as a series of bursts, or from multiple sources such as multiple agencies or multiple software modules as shown in figure
- Another scenario (Janeja 2014) is when the alarms are being generated from multiple Intrusion Detection systems (IDS)
- We can perform clustering of the IDS log data after preprocessing
- The data is in the form of parsed IDS alarms where each alarm is a data point with a priority level, high, medium or low
- This data is being collected from multiple IDS sources
- In this case the premise is that a low priority alarm may not really be a low priority alarm when seen in conjunction with some of the other alarms from different IDSs
- Since we are looking at all alarms from multiple IDSs we have the opportunity to study the similarity between alarms and then judge whether an alarm is truly a low priority or could be potentially high priority
- The end goal is that multiple low priority similar alarms could potentially indicate cyber-attacks
- To distinguish whether these alarms are true alerts we would need to examine if the sources have similar characteristics. A source characterization based on the features associated with sources can be performed



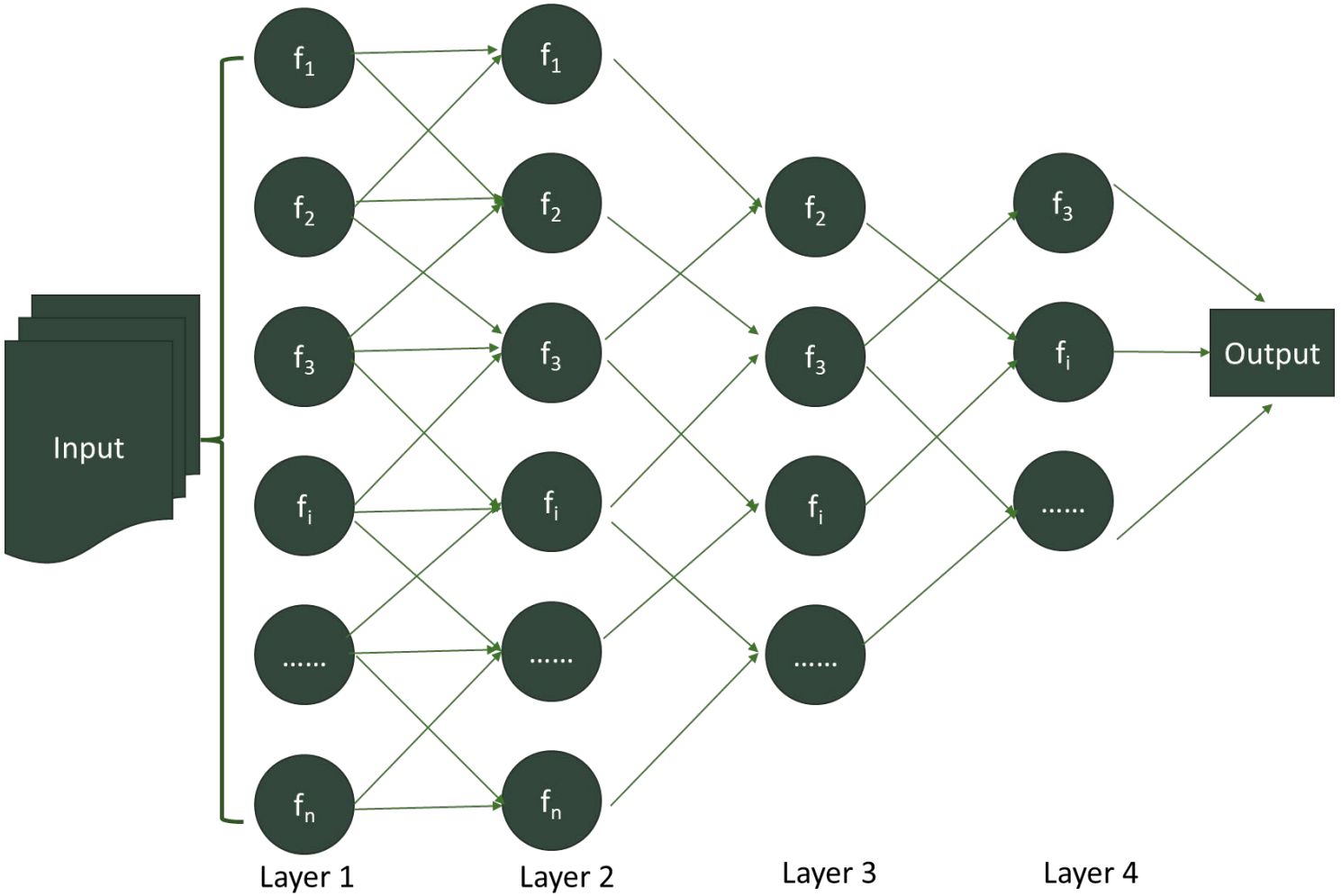
Integrated alerts from multiple sources

- Clusters of alarms based on attributes can be generated
- For each cluster the set of sources associated with each cluster and the alarm cardinality of each cluster, which is the number of alarms in a cluster are identified
    - If only one source is generating alarms in a cluster then source is flagged for investigation
    - If alarm cardinality of a cluster is greater than a preset threshold and if all of the alarms in the cluster are from one source then this can lead to raising an alert
    - Next for every source in a particular characterization such that this source is not equal to the source in the cluster, if the source s is in not in any other cluster it implies that potentially the other sources in the characterization as well are not generating alarms
    - This cluster can be flagged as possible false positive for further investigation
    - This really means that if a source is part of a cluster but the other sources from this characterization are not in any of the clusters then this source may be a false positive
- After removing the clusters representing the false positive, among the remaining clusters of alarms, two cases may occur: a) A cluster comprises of a significant number of alarms but these alarms do not belong to one single source in a characterization and b) No single cluster has a significant number of alarms
    - In case of the first scenario, an aggregated alert can be generated if there is any cluster which has alarms greater than a preset threshold
    - In case of the second scenario, we can identify the overlap between the clusters to find *mutually related alarms* to generate an aggregated alert
    - It is clear that higher the overlap more strongly related are the alarms
    - *Entropy overlap can be utilized* for identifying the overlap of the clusters
    - Entropy essentially measures the quality of the clustering in terms of how the elements in the cluster have been allocated
    - The aim is to identify the overlap one would need to identify the clusters with the highest entropy
    - Essentially, this will allow eliminating the alarms that are not mutually related, thereby leading to the filtering of the alarms
    - If the entropy is greater than the entropy threshold we flag the cluster overlap and raise an alert
- Once an alert is generated sources can be associated with it
- The set of sources of the alarms are the sources of the alarms in the cluster or in the other scenario, the sources of the alarms in the overlap
- These sources can be aggregated by aggregating the feature vectors of all the sources thus generating a composite feature vector of the source of the alert

Deep Learning

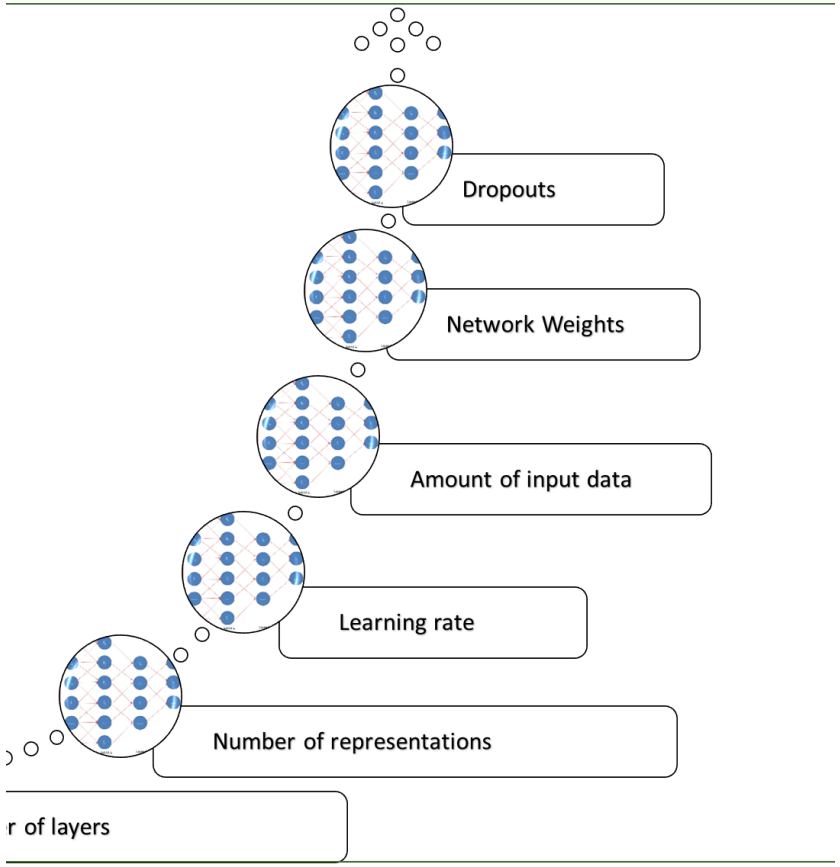
- Deep learning is a type of machine learning that learns the features through multiple layers of abstractions
- For example, if the task is learning to recognize a picture of an individual, the deep learning model may start with various levels of abstractions, starting with the most basic pixels in an image, to an abstraction of an outline of the nose to the outline of the facial structure
- Deep learning algorithms compute the representations of one layer by tuning the parameters from the previous layers (Le Cun 2015)
- As the amount of data increases performance of most machine learning algorithms plateaus. However, performance of deep learning algorithms increases as the amount of input data increases
- An example deep learning model is shown in figure where the input is translated into several features or representations in layer 1
- Some of these representations can be dropped in subsequent layers, throughout the layers the representations are weighted based on the reduction in a loss function until the model converges to the output which is the prediction task
- Deep learning has found a major application in computer vision where images can be labelled based on their most basic of features and abstracting to the higher level composition of the images
- Deep learning has also found applications in anomaly detection (Naseer 2018).
- Deep Learning emulates how human brain learns through connections of neurons
- The most fundamental level of learning comes from neural networks which were in vogue in the early 1960's and have now had a renewed interest due to the deep learning algorithms
- The difference is now we have the availability of massive amounts of data and computing capacity which has resulted in stronger models and learning algorithms

Deep Learning



Deep Learning: Challenges

- Deep learning models have several hyper parameters that need to be predetermined and tuned including number of layers, number of nodes in each layer, network weights, and dropouts in each layer
- Some of these factors are also interdependent and can also impact the learning rate of the model
- If the input data is not large the model cannot be trained well
- The true strength of deep learning is possible in massive datasets and requires heavy parameter tuning
- The challenge also comes in with explainability, of how these parameters are impacting the outputs and the interpretation of the final outcomes



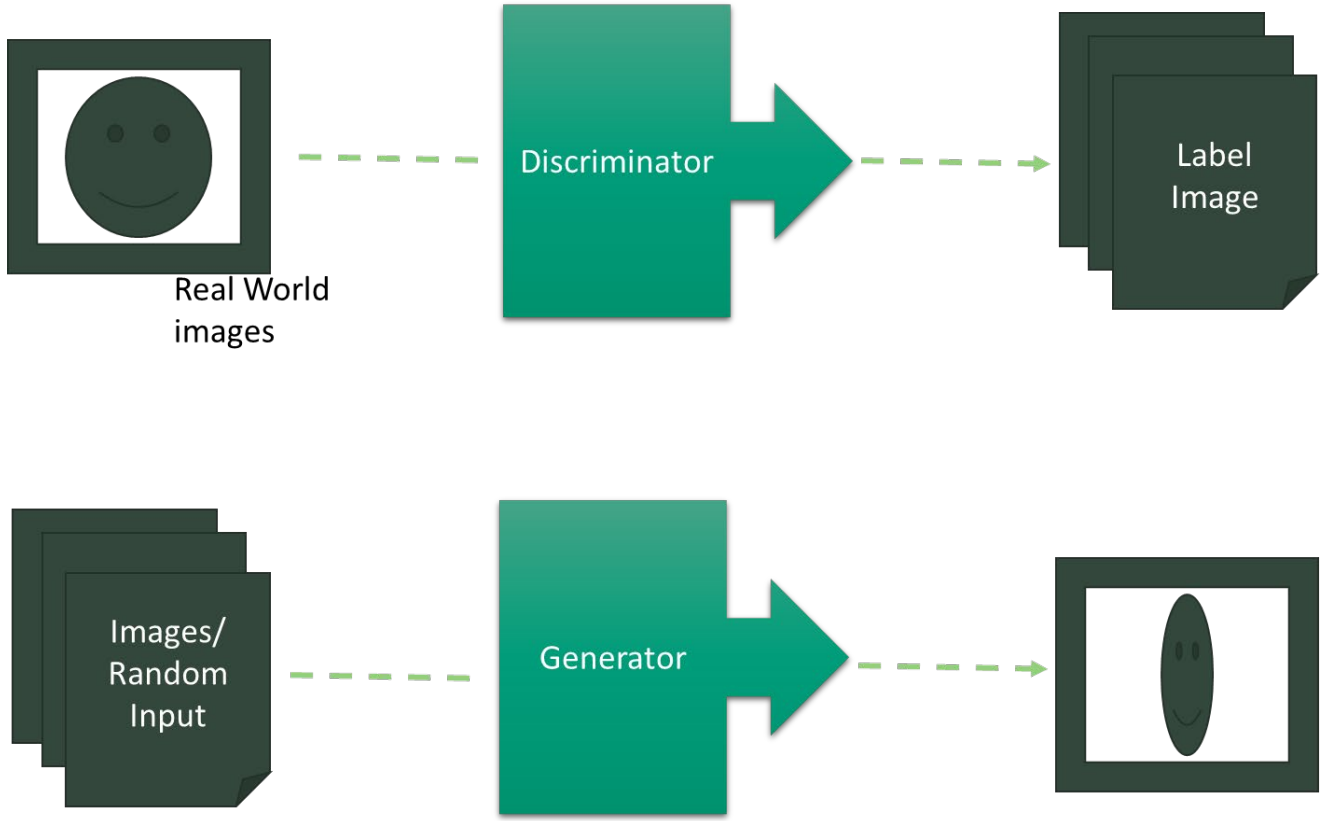
Generative Adversarial Networks (GAN)

- Generative models have been explored with pioneering work in 1996 (Hinton et. al 1996) where an expectation maximization algorithm was used to identify the model that generated an image of a handwritten digit
- This approach not only labelled the data but also explained the model generating it.
- Recent work (Goodfellow 2014) formalized the idea of Generative Adversarial Network (GAN) as a model comprising of two components, a generative model and a discriminative model

Generative Adversarial Networks (GAN)

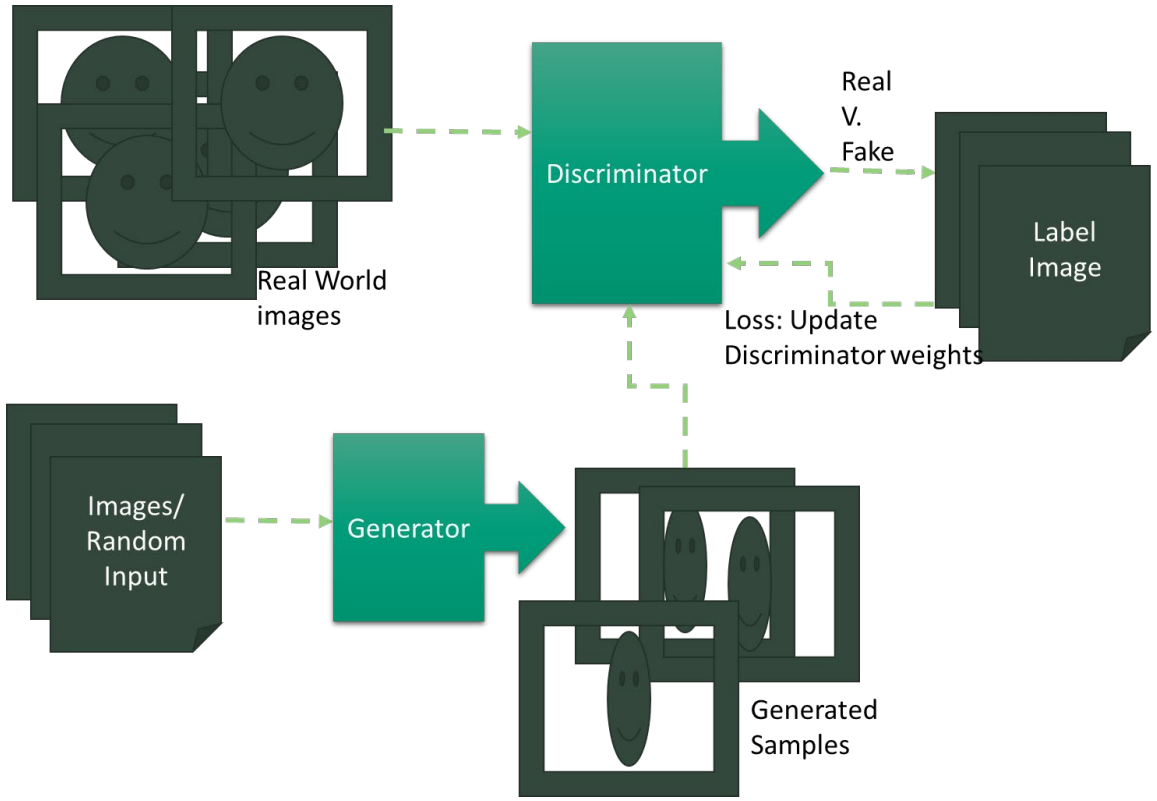
- A discriminator takes input and labels the input as belonging to a certain class. In this example the input can be images and the output is the label for the images as belonging to a certain class
- On the other hand the generator can take the images (or distributions as a starting point) and learn from the distribution to produce new outputs in this case new images. The new images may not be realistically comparable to the original but emulate the distribution

- In a GAN, the two components interact in a two player game where each is trying to win over the other maximizing the similarity to the original distribution
- Here the generative model emulates the probability distribution to match the original data and the discriminative model tries to distinguish whether the generated sample came from the original distribution or from the generative model



Generative Adversarial Networks (GAN)

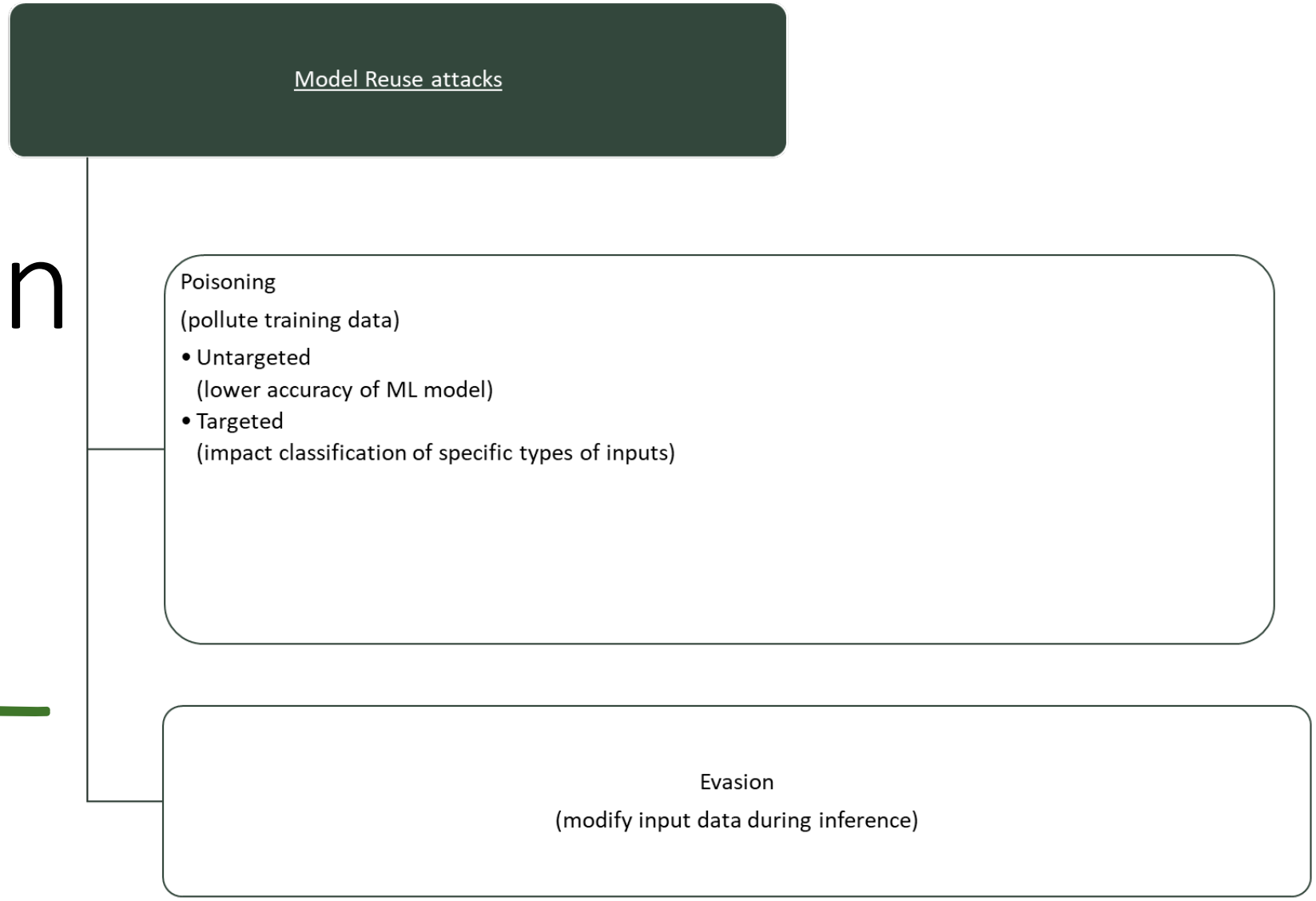
- We can see that the two components are pitted against each other
- Here an input (combination of noise and random images) is provided to the generator, which generates samples
- On the other hand the discriminator which is trained on the real world images examines these generated samples
- These samples are labelled as real or fake. In addition, the discriminator also learns from the loss of labelling the samples and corrects the weights in the discriminator
- This process can iteratively improve the learning from a discriminator
- Based on game theoretic concepts an “adversarial” concept is generally used however this could also be a “cooperative” setting where the discriminator can share the information with the generator (Goodfellow 2016)
- Other types of adversaries, such as adaptive adversaries, have also been discussed in a request-answer game theoretic setting (Gormley 2000, Ben-David 1990)
- Such adaptations have not been shown in computational Deep learning models yet



Model Reuse

- As machine learning and in general data analytics models become more easily available, they are being pervasively used and reused
- Many repositories have emerged where models are checked in by researchers and others are reusing these
- For example, the Open Neural Network exchange format (ONNX), Azure AI gallery, Caffe Model Zoo
- It is only a matter of time before models are as easily available and searchable as pubic datasets
- There is a clear danger in reusing machine learning models without understanding the provenance of the models and the model pipelines
- This has been a well-studied problem in software reuse (Kath 2009, Paul 2002)
- Vulnerability databases have been established to study known software defects to prevent propagating them to other users and applications
- If reuse of vulnerable software and code in general is not prevented it can lead to massive disruptions and attacks such as in the case of the heart bleed bug (Carvalho 2014)
- This level of understanding has been as well established in machine learning models
- Recently some studies have shown that manipulating even simple building blocks of a machine learning model can lead to model reuse attacks (Ji 2018) where corrupted models can lead to the host systems to behave anomalously when certain types of input triggers are introduced into the system
- To understand the impacts of such an attack, consider an autonomous vehicle which has to evaluate several images from multiple camera inputs in an ensemble learning system. In such a complex system if a trigger results in an anomalous decision this can have far reaching impacts for the immediate vicinity where the vehicle is driving and also in the long term for the company who has developed the autonomous vehicle and the systems processing the images
- Indeed studies have shown how researchers have hacked into driverless cars (Versprille 2015) and studied potential risks in smart car functionalities (Weimerskirch 2018)
- Model reuse attacks can bring in a new wave of cyber attacks where complex systems that rely on machine learning behave erratically when certain trigger inputs are introduced

Threats in Model Reuse



Consider ethical decision making at every step of your data analytics cycle

Ethical Thinking in the Data Analytics Process

Ethics

Everyone needs to address ethics – in today's time and context – especially data scientists and AI experts

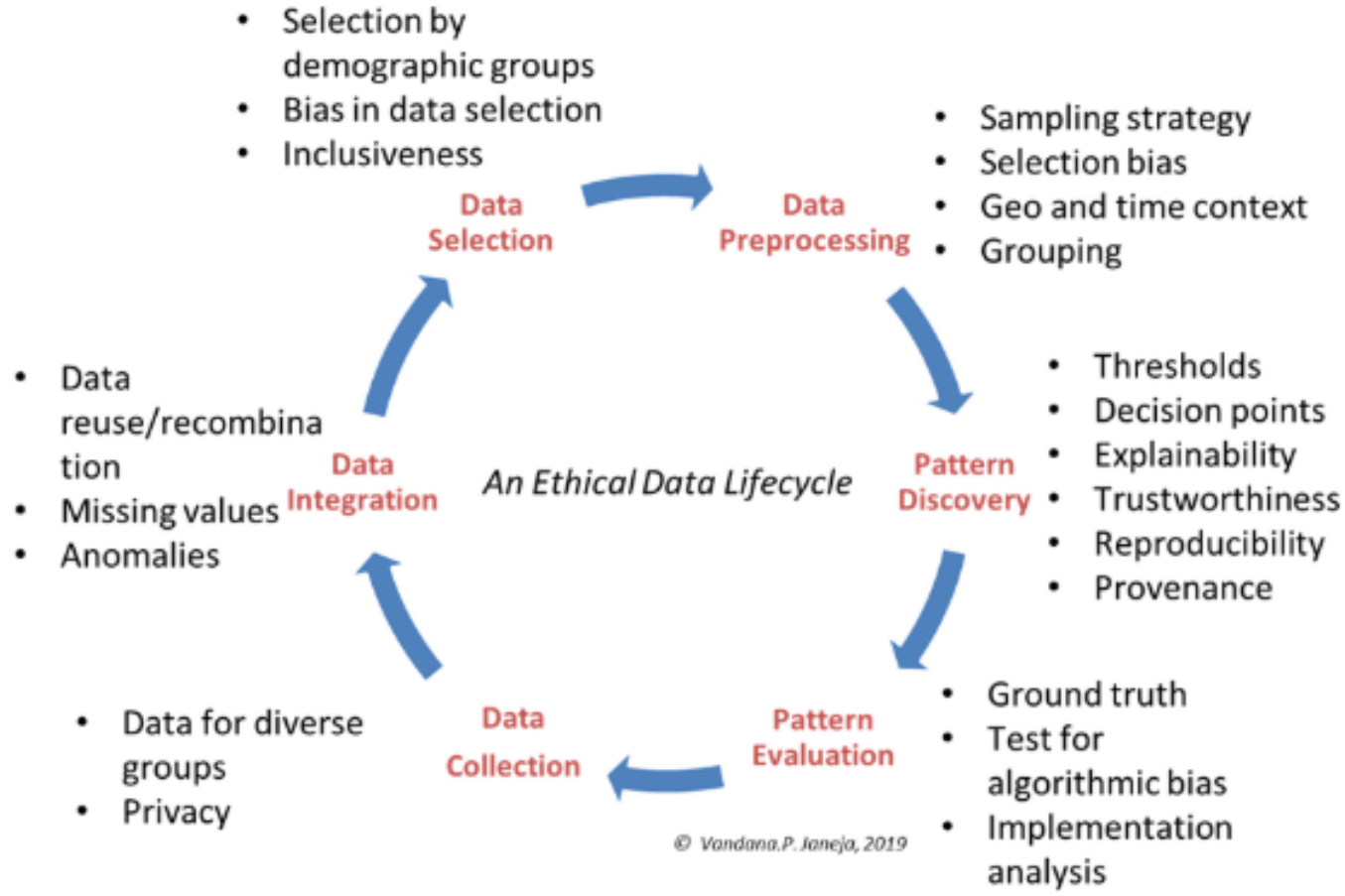
Why Ethics in Cyber Data Analytics?

Educating the [Unknowing] Decision Makers

[Data]Firefighters in the wild

* Infuse thoughtful design throughout the data life cycle
* Introduce qualitative thought processes in a quantitative setting
* Slow down [to think of implications] in your algorithms

An Ethical Data Life Cycle



Consider ethical decision making at every step of your data analytics cycle

https://www.aaaspolicyfellowships.org/blog/do-no-harm-ethical-data-life-cycle

References

- Simmon, E., Sowe, S. K., & Zettsu, K. (2015). Designing a cyber-physical cloud computing architecture. IT Professional, (3), 40-45.
- Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. Technical report, National Institute of Standards and Technology, 2009.
- Blasch, E., Kadar, I., Grewe, L. L., Brooks, R., Yu, W., Kwasinski, A., ... & Qi, H. (2017, May). Panel summary of cyber-physical systems (cps) and internet of things (iot) opportunities with information fusion. In Signal Processing, Sensor/Information Fusion, and Target Recognition XXVI (Vol. 10200, p. 102000O). International Society for Optics and Photonics.
- Nunes, D. S., Zhang, P., & Silva, J. S. (2015). A survey on human-in-the-loop applications towards an internet of all. IEEE Communications Surveys & Tutorials, 17(2), 944-965.
- Calvaresi, D., Marinoni, M., Sturm, A., Schumacher, M., & Buttazzo, G. (2017, August). The challenge of real-time multi-agent systems for enabling IoT and CPS. In Proceedings of the international conference on web intelligence (pp. 356-364). ACM.
- IoT Market – Forecasts at a glance, Oct 2014, https://iot-analytics.com/iot-market-forecasts-overview/
- Verizon wireless, Data Breach digest, 2017
- Janeja, V. P., Azari, A., Namayanja, J. M., & Heilig, B. (2014, October). B-dids: Mining anomalies in a Big-distributed Intrusion Detection System. In 2014 IEEE International Conference on Big Data (Big Data) (pp. 32-34). IEEE.
- Mezzour, G. (2015). Assessing the Global Cyber and Biological Threat.
- Caballero, J., Grier, C., Kreibich, C., & Paxson, V. (2011, August). Measuring pay-per-install: the commoditization of malware distribution. In Usenix security symposium (pp. 13-13).
- Wang, Q. H., & Kim, S. H. (2009). Cyber attacks: Cross-country interdependence and enforcement. WEIS.
- Janeja, V. P., Adam, N. R., Atluri, V., & Vaidya, J. (2010). Spatial neighborhood based anomaly detection in sensor datasets. Data Mining and Knowledge Discovery, 20(2), 221-258.
- Misal, V., Janeja, V. P., Pallaprolu, S. C., Yesha, Y., & Chintalapati, R. (2016, December). Iterative unified clustering in big data. In 2016 IEEE International Conference on Big Data (Big Data) (pp. 3412-3421). IEEE.
- Henanksha Sainani, Thesis 2018, IP Reputation Scoring - 'IP Reputation Scoring - A perspective on clustering with meta-features augmentation
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. nature, 521(7553), 436.
- Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. IEEE Access, 6, 48231-48246.
- Revow, M., Williams, C. K., & Hinton, G. E. (1996). Using generative models for handwritten digit recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 18(6), 592-606.
- Goodfellow, I. (2016). NIPS 2016 tutorial: Generative adversarial networks. arXiv preprint arXiv:1701.00160.
- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. In Advances in neural information processing systems (pp. 2672-2680).
- Ben-David, S., Borodin, A., Karp, R., Tardos, G., & Wigderson, A. (1994). On the power of randomization in on-line algorithms. Algorithmica, 11(1), 2-14.
- Gormley, T., Reingold, N., Torng, E., & Westbrook, J. (2000). Generating adversaries for request-answer games. In In Proceedings of the 11th ACM-SIAM Symposium on Discrete Algorithms.
- Carvalho, M., DeMott, J., Ford, R., & Wheeler, D. A. (2014). Heartbleed 101. IEEE security & privacy, 12(4), 63-67.
- Kath, O., Schreiner, R., & Favaro, J. (2009, September). Safety, security, and software reuse: a model-based approach. In Proceedings of the fourth international workshop in software reuse and safety.
- Ray J. Paul and Simon J. E. Taylor. 2002. Improving the model development process: what use is model reuse: is there a crook at the end of the rainbow?. In Proceedings of the 34th conference on Winter simulation: exploring new frontiers (WSC '02). Winter Simulation Conference 648-652.
- Ji, Y., Zhang, X., Ji, S., Luo, X., & Wang, T. (2018, October). Model-reuse attacks on deep learning systems. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 349-363). ACM.
- A. Versprille. 2015. Researchers Hack into Driverless Car System, Take Control
- of Vehicle. http://www.nationaldefensemagazine.org/articles/2015/5/1/2015may-researchers-hack-into-driverless-car-system-take-control-of-vehicle
- André Weimerskirch , Derrick Dominic Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles, University of Michigan, 2018