This assignment is worth 40% of the subject assessment.

Due Date: Thursday the 8th of Sept 2022 at 23:59pm.

Introduction:

In recent decades, the development of Internet and communications technologies has

introduced a virtual world to everyone’s daily life. In this virtual world, people are able to do

a large number of activities similar in the real world. Especially with the growth of Internet of

Things (IoT) and 5G, the field of IT security is becoming more important.

**To help you better**

**understand the field, you are required to write a literature review on any one of the following**

**related IT security topics, either from the attack or defence view. The literature review should**

**consist of 2500-4000 words (at least 6 pages, single spaced, 12pt fonts, on a normal A4**

**paper).**

Topics:

Choose One only:

• Attacks:

o Advanced persistent threat

o Insider threat

o Emerging Attacks on Blockchain or the defences

o Emerging Attacks on IoTs or the defences

o Emerging Attacks on AI or the defences

o Backdoor attacks or the defences

o Denial of service or Distributed Denial of service

o Eavesdropping

o Exploits

o Malware

o Spam

o Phishing

o Ransomware

o Vulnerabilities

• Defences:

o Access control

o Application security

o Secure coding

o Authentication

o Multi-factor authentication

o Authorization

o Data-centric security

o Encryption

o Intrusion detection/prevention system

o Mobile security

o cloud security

• or you are allowed to choose your own IT security topic even it is not listed above

2

Amount of work:

Each student should spend at **least 30 hours** working on the assignment. **Documentary**

**evidence of the time taken** may be requested by the convenor after submission, so **log books,**

**repositories** should be maintained. The literature review should consist of **2500-4000 words**

(at least **6 pages, single spaced, 12pt fonts, on a normal A4 paper**).

Marks will be allocated depending on the amount of original work submitted. 0 Mark will be

given for plagiarized and/or un-attributed work. eForensic examination of the assignment will

be carried out to verify its authenticity.

Grading:

This assignment will be graded as Fail, Pass, Credit, Distinction or High Distinction.

Please see the details of the marking criteria at the end of this document.

Submission

Submissions should be made through https://swinburne.instructure.com/ (Canvas) before the

due date. **Reports should be in commonly used PDF document format (.pdf) and should not**

**exceed 15 pages in length**.

• The first page should be a filled-in copy of the cover sheet available on Canvas.

• The second page must be a title page indicating:

o the unit code and title,

o title of the assignment,

o the topic,

o the authors (by name and student ID),

o the submission date/time,

o the due date/time.

**Pages must be numbered starting with the first page AFTER the cover sheet and title page**. A

table of contents is NOT to be used.

Appendices and a list of references will not be included in the page count.

Late submissions will be penalised by 10% per day (for 3 days maximum), submissions which are 3

days after due date will not be allowed and 0 mark will be given.

References

All externally sourced information (i.e. not common knowledge or course material) must be

cited. Referencing conventions required for this unit are: Vancouver (as used by IEEE).

Helpful information on referencing can be found at

https://www.swinburne.edu.au/library/referencing/

https://ieeeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf

Each citation must have a corresponding reference at the back of the report.

**ALL REFERENCES MUST BE CITED.**

There is no minimum requirement for the number of references.

3

Structure:

For this assignment, students should choose one topic and deliver a report about its literature review.

The report should follow a similar structure listed below.

• Cover sheet

Swinburne University of Technology

*Faculty of Science, Engineering and Technology*

**ASSIGNMENT AND PROJECT COVER SHEET**

Unit Code: COS30015 Unit Title: IT Security

Assignment number and title: Assignment 1 Research Project Due date: 8th Sept 2022

Lab group: Thursday 8:30AM Tutor: Jamie Ooi Lecturer: Lin lin

Family name: Rezwan Identity no: 103172423

Other names:

# To be completed if this is an INDIVIDUAL ASSIGNMENT

I declare that this assignment is my individual work. I have not worked collaboratively, nor have I copied from any other student’s work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for me by another person.

Signature: S M Ragib Rezwan

# To be completed if this is a GROUP ASSIGNMENT

We declare that this is a group assignment and that no part of this submission has been copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for us by another person.

ID Number Name Signature

Marker's comments:

Total Mark:

# Extension certification:

This assignment has been given an extension and is now due on

Signature of Convener: Date: / 2022

• Title page

Unit Code: COS30015 Unit name: IT Security

Title of the assignment: Research Report On AI

Topic: Emerging Attacks on AI

Author: S M Ragib Rezwan (103172423)

Submission Date:

Due Date: 8th Sept 2022

• Abstract (say brief about ict in world---brief about AI and the hype its gaining

o Adequate background (1~2 sentences)---breif about AI means and its importance in digital area or ict or public

o Correct definitions of the problem and key terms (2~4 sentences)-breakdown the prob, why is ai being attacked? What form of attacks? Any priority level in attack type or impact level of attack?

o Key findings –main avenue of attack/attack type --- like most attacks are on the “service” that uses AI and not the AI itself--- or smth--- but say you will only focus on attack on the ai itself as they most of the attacks on those services are extensions on the types of attack on the ai itself

o Convincible importance (2~4 sentences)—out come of the attacks, and why we need to protect ai? I guess… ++ also say as the note: Here I am using Machine learning interchangeably with AI. That’s because Machine learning (ML) is basically a subset of AI that solves specific tasks by learning for the data given. Thus although there is a slight difference between them, in terms of the attacks, all attacks that affect ML will also definitely affect AI in the same way….

**“AI solves tasks that require human intelligence while ML is a subset of artificial intelligence that solves specific tasks by learning from data and making predictions**. This means that all machine learning is AI, but not all AI is machine learning”---ref(<https://www.freecodecamp.org/news/ai-vs-ml-whats-the-difference/> )

• Introduction

o Adequate background—say details about ai and its importance in current world (maybe give a bit about history of ai to current world importance? Like… it had been first made by…. who used it only for… but now, its been spread almost everywhere were people are using it for….)---like services ai provides

o Convincible importance---say where where ai is being used currently (like processing what type of data or simulation or prediction, auto driving cars, voice assistant, etc –use references!) and what will happen if they fail or not work properly or accurately…

(all the various important cyber sec services where ai is being used……<https://www.spiceworks.com/tech/artificial-intelligence/articles/adversarial-ai-attack-tools-techniques/> )

o Correct definitions of the problem and key terms—say the avenues of ai being attacked… like maybe ~~some try to ddos it,~~ maybe some try to feed it false data, maybe some try to break it open and cause it to malfunction…etc (need to find proper ones with references!!!)--- say that ai is not always the end goal of the target but instead the end goal is bringing down or disrupting the service that is using the AI. But the attack still ends up acting on the ai…. (need something to say here, cant find the actual words… maybe give refence or quote saying that although attack purpose is to stop or disrupt the service, attack is performed on the ai)

o Originality of the report (own ideas, views, analysis, etc.)—using all the data I have gathered, I was trying to compare and contrast between the different ways AI has been attacked in order to summarise and catagorise them and thus provide either a general defencive method that would be applicable in all cases or a list of method that can be used in order to address all of these issues and mitigate them (in an efficient and effective manner)---like a manual of sort

~~see if there a simple/ integrated way to resolve all variations of attacks on ai?.~~

~~....or maybe say, that you are trying to use all information about the attack type and depth to rank them (in terms of likelihood and impact of the attack) and thus prepare a guideline of steps to take in order to mitigate all of the emerging attack in an effective an efficient manner--- like a manual of sorts~~

o Structure of the report – say that in order to do so you had gone through several research papers , articles and blogs and organized them in the report in the following order: Overview area--- to address how I had located my information, literature review area—where I noted down all the information I had gathered about the topic (alongside issues I had faced), discussion area—where I anaylsed the literature to determine my own opinion and finally the conclusion area----where I summarized my findings and thoughts

*a format template for this part taken from a medical + AI article…*

*---“ In this paper, we survey different types of newly invented adversarial attacks against medical imaging informatics and various defense techniques. In Section**[2](https://www.sciencedirect.com/science/article/pii/S095741742200272X" \l "sec2), a brief introduction to deep learning based medical imaging and its variants is discussed. In* *[3](https://www.sciencedirect.com/science/article/pii/S095741742200272X" \l "sec3), we explain adversarial attacks and different types of generating adversarial examples. In Sections**[4 Attacks to medical learning algorithms](https://www.sciencedirect.com/science/article/pii/S095741742200272X" \l "sec4),* *[5 Defense methods against attacks to medical learning algorithms](https://www.sciencedirect.com/science/article/pii/S095741742200272X" \l "sec5), the most recent adversarial attack and defense approaches to medical imaging DNNs has been summarized. Finally in Sections**[6 Discussion](https://www.sciencedirect.com/science/article/pii/S095741742200272X" \l "sec6),* *[7 Conclusion](https://www.sciencedirect.com/science/article/pii/S095741742200272X" \l "sec7), we discuss different aspects and deficiencies of the methods, possible future challenges, and provide concluding remarks.”*

• Overview/Background

o Overview of the literature review (How literature is organized in Literature Review?)

o Selection criteria of the literature (How do you select the literature to review?)

(say that you decided to go via two pronged attack: First you went and looked through google scholar and swin library to find information givn by scholars and literary experts regarding theory. But say that you weren’t able to find too many data regarding this as most of the research were kept confidential (specially ones regarding cutting edge techniques )… Thus also looking through articles and blogs given by cyber sec companies and corporations and also tech companies, specially ones dealing with AI to see the current level of technology …(.for all of these mention which author’s articles you looked at in brackters for easier reference later on )---say that after doing this you had found lots of various types of ai attacks, which you had organized under the following catagories: (mention the catagories) in order to simplify it. These catagories had been decided on after going through articles written by: ……. All writer’s names

~~so you decided to fist organize the attacks in terms of attacking a certain area of service…..later on try to re arrange all of these into a further simplief or generalized type of attack for ai (that can be referred to when speaking about the different ai attacks)…~~

o Any further background about the problem you mentioned/reviewed?

• Literature Review

o Adequate description of major issues/challenges (challneges involving attacking AI, secrecy of research surrounding it, etc)—like ai is too widespread and used in various purposes (like….), each with their own avenue of attack and mitigation. Thus, in order to better compare and contrast, the attacks have been devided into the following catagories:

(put everything in this table)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of attack | Sub type of the attack | Explaination | Example of attack | Existing solution |
|  |  |  |  |  |

1. Adverserial Input type attacks:

Attacks where data is provided to an AI system in order to alter its output in a certain way (usually in one that is desired by attackers)

(can also be used to evade detection and stuff)

Can be of: perceivable, non perceivable, digital or physical attacks + Online adversarial attack

(give a table to explain them) + some types of adversarial attacks that have been used in medical areas…. Like FGSM, JSMA, PGD, etc… ++ Psychoacoustic Hiding, laser and other attacks used in Ai voice assistant----use all of these as examples of the types of attacks

|  |  |  |  |
| --- | --- | --- | --- |
| ~~Type~~ | ~~Explaination~~ | ~~Example of attack~~ | ~~Existing solution~~ |
|  |  |  |  |

1. Poisioning type attacks:

These are similar to input attacks, except that occur during the development and training phrase of an AI system when data being used to train the system are corrupted

Can be of: dataset poisioning, algorithm posiiong, model poisioning

--insert incorrect or mislabeled data to the set of datas leading to machine learning wrong patterns leading to wrong outcomes

---Federated learning….utilising weakness in algorithm used to learn the model

---altering or replacing a legit model with a poisonous one at any point in distribution line….

(give table to explain them)

+++add the preventing posiingn attacks parts from the papers of preventing poisoning attacks on ai based threat inteliigence system

|  |  |  |  |
| --- | --- | --- | --- |
| ~~Type~~ | ~~Explaination~~ | ~~Example of attack~~ | ~~Existing solution~~ |
|  |  |  |  |

1. Model Stealing attacks:

Similar to model posisioning type attack except here the entire model is duplicated instead of being altered via different techniques---used for….---can be used to “transfer learning” (research paper With Great Training Comes Great Vulnerability: Practical Attacks against Transfer Learning, Bolun Wang et al., describe the ability of threat actors to use ML training models to understand weaknesses in ML processes, increasing the probability of fooling ML into making incorrect conclusions, and enabling other attack vectors----need to find the link for this!!!)---( like Inception, Xception, VGG etc which are used to transfer learning between image classification in a legitimate manner)

--can be used to perform “data phising privacy attack” by reverse engineering the dataset present in the model

|  |  |  |  |
| --- | --- | --- | --- |
| ~~Type~~ | ~~Explaination~~ | ~~Example of attack~~ | ~~Existing solution~~ |
|  |  |  |  |

1. DDos

-----providing it with complicated problems to make the lreaning process useless

1. Ai model attacks

SCA (side channel attacks on AI model) using Fuzzy

++add papers and articles while searching for existing solutions to all these problems!!! (try doing at least 15 to be on safe side)

(Voice AI attacked using psycho hiding and other adversarial attacka dns oand other attacks: <https://link.springer.com/content/pdf/10.1007%2F978-3-030-68449-5_26> )

(some information regarding adversarial attacks---except here they speak about ethical ones… <https://link.springer.com/content/pdf/10.1007/s43681-021-00113-9.pdf> )

(some exaples of transfer learning attacks: <https://analyticsindiamag.com/a-comparison-of-4-popular-transfer-learning-models/> )

(some more attacks: <https://www.excella.com/insights/ml-model-security-preventing-the-6-most-common-attacks> )

(some different types of ai attacks: <https://www.spiceworks.com/tech/artificial-intelligence/articles/adversarial-ai-attack-tools-techniques/> )

(different types of ai attacks: <https://elie.net/blog/ai/attacks-against-machine-learning-an-overview/> )

(Input vs poisioning attack details

<https://analyticsindiamag.com/what-is-poisoning-attack-why-it-deserves-immediate-attention/> )

(summary of input and positioning and some variations in their types

<https://www.belfercenter.org/publication/AttackingAI> )

|  |
| --- |
| FGSM, JSMA |
|  |
| FGSM, PGD, MIFGSM, |
| DAA, DII-FGSM |
| FGSM and other adversarial input attacks used in medical purposes---https://www.sciencedirect.com/science/article/pii/S095741742200272X#b53  (preventing ai based poisoining attacks on threat intelligence system  <https://arxiv.org/pdf/1807.07418.pdf> ) |

o Proper description about existing systems, methods, strategies, mechanisms, solutions,

etc. (What it is and how it works?)—maybe use table system for this

o Proper analysis of these existing systems, methods, strategies, mechanisms, solutions,

etc. (What issue/challenges they solved and why can be solved?)--- maybe use table system for this

o At least 10 references and proper citation of them (yellow highlight—attack on ai itself and not just on service)

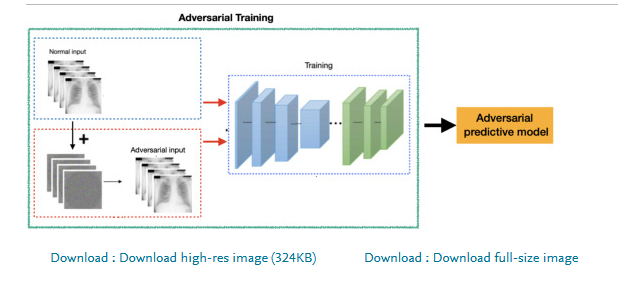
~~can use this but only as example of an attack-----ai voice assistant attack: Adversarial Attacks via Psychoacoustic Hiding (attack by hiding commands in audio file human ear cant detect), laser attack(using laser to make gadget believe voice commands were being inputted), surfing attack(using voice commands encrypted in ultrasound wave)----all of these can be done via advert, news, hidden app voice message etc (for the non laser related attacks) ---simplify or summaraize all of these into type of attack directly on ai or on service assisted by ai—possible solution to make the AI better at understanding voice, but wont work as these can still be faked with voice recordings0—so best solution is not expose it to such scenarios (ie like keeping voice assistant off when not using it)~~

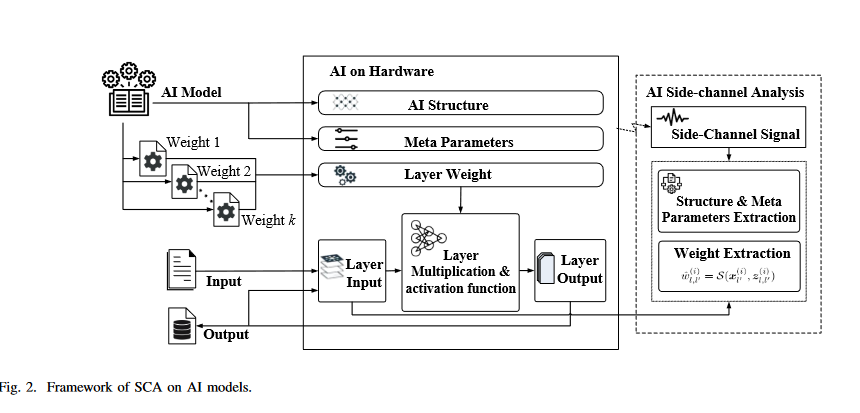
**~~mainly speak about these and the next input and poinoining point~~**~~……..general purpose attack on ai-🡪~~ *~~adversarial machine learning(like~~* ***~~evasion attack,~~******~~poisoning attack~~****~~,~~* ***~~exploratory attack~~****~~….)--- all variations of fooling a normal legal ai solution in order to make them malfunction (can be used to attack medical imaging, intelligent transport, personal cars,etc)---solution: detecting the attacks, (personal thought: here they said using EAA (ethical adversarial attack)—to target malicious systems that use AI to attack. Maybe use that to attack non malicious systems using ai to see how they react and thus find out ways to not only detect the attack (via symptom analysis ---take analogy from medical or biology or doctor treatment here) but also on ways to mitigate or safeguard from it and also on what steps to take in worst case scenario~~*

~~can say as an example attack for model type attack? Attack on AI model🡪Accessibility to smart devices provides opportunities  
for side-channel attacks (SCA) on artificial intelligent (AI)….. , existing liter-  
ature exposes some shortcomings: (i) incapability of quantifying  
and analyzing the leaked information through side channels of  
the intelligent IoT and (ii) inability to devise efficient and accurate  
SCA algorithms….. o address these challenges, we propose a side-  
channel fuzzy analysis empowered AI-model extraction attack  
in intelligent IoT.~~

~~(basically side channel attack on ai model)--- The main challenge for the SCA on AI models  
is that existing analysis methods cannot be adopted directly  
to describe attacks accurately and design efficient extraction  
algorithms.--- While the target AI system is performing on a hardware  
platform, it inevitably results in unintentional physical leakage,  
e.g. energy consumption, execution time, and electromagnetic  
emanations released while data computation. Adversary mon-  
itors these physical leakages at runtime through preset probes  
and analyze them to deduce sensitive information. AI models  
consist of structure, metaparameters, weights, etc. Thus, the  
extraction of the AI models includes multiple types. With  
physical control of the hardware, attackers extract the structure  
and parameters of AI models running on the hardware based  
on the multi-dimensional side-channel signals. Memory access  
patterns and timing are commonly utilized side-channel signals  
to infer AI-model architectures [----Side-channel attackers have physical access to the hardware  
deploying AI models and observe side-channel signals, with-  
out the capability to manipulate operations. Adversaries can  
control the execution of target AI models by crafting their  
inputs. Then, the adversary observes corresponding outputs  
and side-channel signals to obtain AI models~~

~~--- aditional capacity definition can not be directly  
applied to the proposed SCA on AI, because side channels  
are not designed to transfer signals but steal information by  
feeding query samples. Therefore, we develop a method to  
quantify the information leakage adapting to features of the  
SCA on the AI system. We define the capacity of SCA  
on AI models as the maximum leaked information amount  
through per query.~~

~~~~

~~~~

~~---ref~~ [~~https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9772948~~](https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9772948)

~~Adversarial attack on ai using bad inputs….-->In conventional machine learning systems, adversarial examples are inputs that have been manipulated and prepared to force the system to make incorrect classification and make difficulties in semantic segmentation. This type of attack, that causes problems in various domains such as spam filters,~~ [~~intrusion detection systems~~](https://www.sciencedirect.com/topics/computer-science/intrusion-detection-system) ~~and~~ [~~biometric authentication~~](https://www.sciencedirect.com/topics/computer-science/biometric-authentication) ~~(i.e. presentation attack), have been discussed for a few decades~~

~~Black box version—>attacker doesn’t know. White box version 🡪 attackers knows full details of system~~

~~Types: L-BGFS method, FGSM method, JSMA method, C&W attack, DeepFool attack model, model-based ensembling attack for targeted adversarial which is also “transferable”~~

~~--also has other attacks and defences against medical learning algos~~

| **~~Defense method~~** | **~~Attack type~~** | **~~Dataset~~** | **~~Model architecture~~** | **~~NN. type~~** | **~~Reference~~** |
| --- | --- | --- | --- | --- | --- |
| ~~Adversarial training~~ | ~~FGSM, JSMA~~ | ~~lung images (CT)~~ | ~~UNet＋ RPN~~ | ~~classification~~ | ~~Vatian et al.~~ |
|  | ~~brain MRI~~ |  |  |  |
| ~~PDT & adv\_train~~ | ~~FGSM, PGD, MIFGSM,~~ | ~~pneumothorax (X-ray)~~ | ~~DenseNet, ResNet,~~ | ~~classification~~ | ~~Rao et al.~~ |
| ~~DAA, DII-FGSM~~ |  | ~~VGG, IV3~~ |  |  |
| ~~NLCE~~ | ~~FGSM~~ | ~~lung (JSRT)~~ | ~~SLSDeep, NWCN, UNet,~~ | ~~segmentation~~ | ~~He et al.~~ |
|  | ~~skin lesion(ISBI2016)~~ | ~~InverNet, CDNN, ResNet~~ |  |  |
| ~~KD & LID~~ | ~~FGSM, PGD, BIM~~ | ~~DR (Fundos)~~ |  |  |  |
| ~~C&W~~ | ~~pneumothorax (X-ray)~~ | ~~ResNet~~ | ~~classification~~ | ~~Ma et al.~~ |
|  | ~~melanoma (skin images)~~ |  |  |  |
| ~~Unsupervised anomaly detection~~ | ~~FGSM, BIM, MIM,~~ | ~~pneumothorax (X-ray)~~ | ~~DenseNet, ResNet~~ | ~~classification~~ | ~~Li et al.~~ |
| ~~PGD~~ |  |  |  |  |
| ~~SSAT & UAD~~ | ~~FGSM, PGD,~~ | ~~DR (OCT)~~ | ~~ResNet~~ | ~~classification~~ | ~~Li et al.~~ |
| ~~C&W~~ |  |  |  |  |

~~--ref: https://www.sciencedirect.com/science/article/pii/S095741742200272X#b53~~

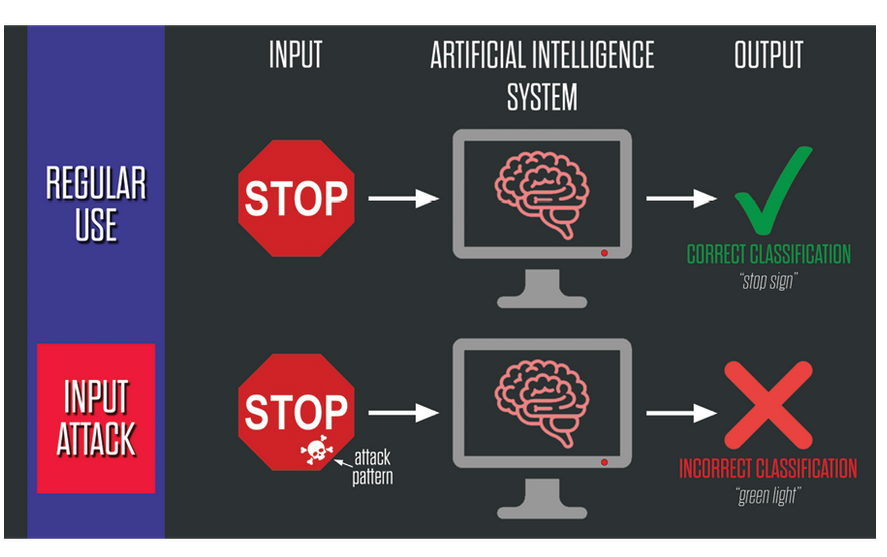
~~with a type of AI attack called an “input attack,” adversaries can craft patterns of changes to a target that will fool the AI system into making a mistake. This attack is possible because when patterns in the target are inconsistent with the variations seen in the dataset, as is the case when an attacker adds these inconsistent patterns purposely, the system may produce an arbitrary result—……………a few stray marks or subtle changes to a handful of pixels in an image are needed to destroy an AI system.~~

~~known as a poisoning attack—can stop an AI system from operating correctly in situations, or even insert a backdoor that can later be exploited by an adversary. Continuing the analogy, poisoning attacks would be the equivalent of hypnotizing the German analysts to close their eyes anytime they were about to see any valuable information that could be used to hurt the Allies.~~

* ~~Input Attacks: manipulating what is fed into the AI system in order to alter the output of the system to serve the attacker’s goal. Because at its core every AI system is a simple machine—it takes an input, performs some calculations, and returns an output—manipulating the input allows attackers to affect the output of the system.~~
* ~~Poisoning Attacks: corrupting the process during which the AI system is created so that the resulting system malfunctions in a way desired by the attacker. One direct way to execute a poisoning attack is to corrupt the data used during this process. This is because the state-of-the-art machine learning methods powering AI work by “learning” how to do a task, but they “learn” from one source and one source only: data. Data is its water, food, air, and true love. Poison the data, poison the AI system. Poisoning attacks can also compromise the learning process itself.~~

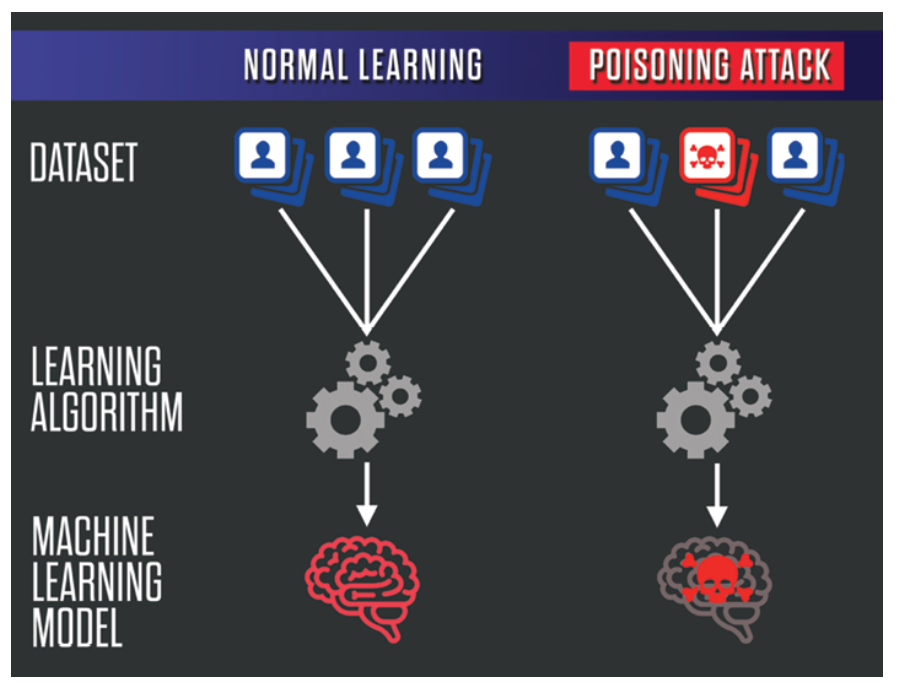
~~Reason to attack: casue damage, hide smth, reduce faith in system~~

~~These vulnerabilities are not “bugs” that can be patched or corrected as is done with traditional cybersecurity vulnerabilities. They are deep-seated issues at the heart of current state-of-the-art AI itself.---as we don’t understand how they are ctually working internally and instd treat it as black box~~

~~~~

~~Input attacks classification: perceivable, digital, imperciavable, physical~~

~~To poison an AI system, the attacker must compromise the learning process in a way such that the model fails on certain attacker-chosen inputs, or “learns” a backdoor that the attacker can use to control the model in the future. One motivation is to poison a model so that it fails on a particular task or types of input.~~

~~~~

~~Type of poisoning: dataset poinoing, algo poisoning, model poisoning,~~

~~Systems impacted by the attacks: Cnotent filters, military, law enforcement, business that use AI in their system,~~

~~Prioritize Research of Defense Mechanisms and More Robust Algorithms-- As such, even if complete mitigation is provably impossible, techniques to “harden” the methods, such as making attacks more difficult to execute by modifying the structure of the models themselves, will be of significant interest to AI users--- Guaranteeing AI Robustness Against Deception (GARD) program~~

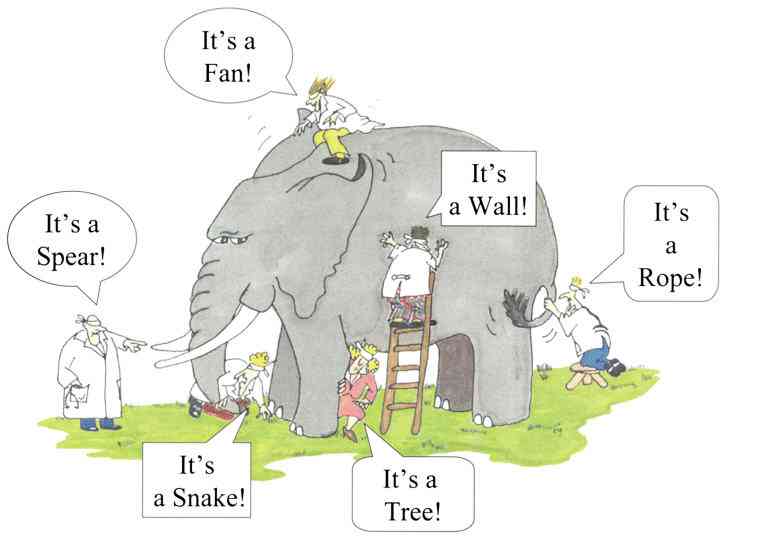
~~\_ref: https://www.belfercenter.org/publication/AttackingAI~~

• Discussion

(try to speak about the adv and disadv and impacts of the attacks and also their solutions like does one solution take more money or takes more time or needs more in depth understanding of solution and stuff)

o Critical analysis of these literatures (advantage and disadvantage)---say about the fact that some of them are articles and thus not peer reviewed so validation or accurate problem or smth--- (not finding the exact word to say here)… + try to google for issues with literature and try to use points from there + also say that different people focused on different aspects and named the same thing different like: like some called it input attack, some said adversarial input attack and other stuff (make sure to link all of them alongside which write spoke which key word) also justify why they had approached in which manner

o Proper arguments about their impacts (positive and negative)---say that since different write took different approaches to speak about the same thing, whenever you had spoken about a common point, the validity of information increased but when they delved into their own thoughts (ie like prediction and analysis or future thoughts and recommendations and stuff) they were no longer having similar thought and thus accurate of information got reduced… give exapm[les of this occuring and try to say this part using different analogy of people looking at same thing but saying different… (maybe a picture of people looking at same objects but coming to a different conclusion---also give reference to it)



o Possible solutions from your understanding (own ideas, views, analysis, etc.)—say ur own view regarding a global classification that can be applied to all problems and solution or manual that can be applied to all problems and solutions…+say about the eeffectiveness of prob or solution

• Conclusion

o Proper summarization of the problem reviewed and impact. (say that we need to be ready ---likenext step in evolution/digitization/metaverse (ref)--- so as not be swept by the tide----)---like say that currently ai still hasn’t fully reached its peak and is still bumd and thus we need to fix all these issues form now as otherwise later on if these iffuses remain, it will become harder to fix them—give an analogy here or real life stuff (like )

o Proper description of your findings and conclusion (summarize key points and your thoughts after comparing and conterasting the research papers)