D.S.A.I. for cybersecurity

A research paper by **Abhishek Srivastava** under the guidance of **Dr. Rajiv Pandey** (Assistant Professor)(A.I.I.T. Amity University Lucknow campus)

Abstract:

domain specific artificial intelligence model (DSAI) is a model or branch of A.I. which we train on a specific set of information about our specific need, combining the power of artificial intelligence's algorithm to find and seek patterns in the field of cybersecurity can be very beneficial, it can help us detect a threat or a malware early in the stage because it can recognize even the smallest anomaly which can be ignored by humans,

there are many things which can be done and enhanced when we combine the pattern seeking power of Artificial Intelligence in the field of Cybersecurity, things like:

1. early detection and prevention of a threat or a malware
2. it can help us perform efficient pentesting also known as penetration testing
3. it can work as a 24×7 watcher which can keep a continuous check on the system and report if there is any issue immediately
4. it can analyze the issue and suggest best way to solve the problem based on the data it was trained on
5. it can help reduce scam, fraud and phishing websites by checking the credibility of the website or app before

this research paper is going to explore the potentials of Domain Specific Artificial Intelligence in the field of Cybersecurity, this paper will discuss about all the merits that is gained by using domain specific AI and all the demerits that come with using it, this paper will also include information about ***what is domain specific AI , what is cybersecurity , how does domain specific AI work and how to implement it in the field of cybersecurity***

Keyword:

domain specific AI, algorithm, cybersecurity, fine tuning, models, LLM, cybersecurity toolkit

Introduction:

in modern world cybersecurity is important because it protects everything which is on the internet like your photos, videos and personal data from attackers who try to steal these things to use it against you, this is a serious problem but it becomes more serious when the data belong to big companies or the government the attacker can potentially harm the whole nations economy and more

to prevent this type of problem cybersecurity comes into play, cybersecurity basically is a branch of computer science that deals with Internet of things and the main purpose of this science is to prevent and understand the vulnerabilities of a system or group of systems, but the main problem with this is that humans do all the work and sometime a malware can hide in plain sight and fool a human so to resolve this type of issue we can use Domain Specific Artificial Intelligence (DSAI) in the field of cybersecurity.

by integrating the domain specific AI models with your cybersecurity tools we can potentially boost the ability of the tools and protect system and people from getting attacked

the algorithm of domain specific AI can help to detect malware and threats beforehand because of the bulk data it is trained on, which can see pattern in the log files and predict if there is going to be an anomaly in the system or not, and because of its training it can also be able to perform system check / pentesting to find vulnerabilities in the software or the system

there are many advantaged and disadvantages in integrating the algorithm of domain specific AI in the field of cybersecurity

Review of Literature

the technology of domain specific AI in the field of cybersecurity can produce many advantages like threat prediction the DSAI can help by scanning the system continuously and checking for the anomaly in the system or the network this can help us get the information early about the threat and we can eradicate the root cause of threat so that our system can be secure and protected from any malware and attacks

there are also disadvantages of using the technology like because the DSAI is at the end a machine and it cannot be trusted fully because it can produce false results because of bug or the data the DSAI was trained upon

implementation of the technology in the field of cybersecurity there is no direct way but we can build a uncensored DSAI model and train it on the data we have custom or we can use a method called fine tuning to train the LLMs that are there for our use we can use fine tuning and train the LLM for our custom need

Methodologies

- ***Early threat detection and prevention***

if we integrate the pattern seeking abilities of a domain specific AI which is trained on data of how and what are the basic and complicated problems a system might face and how to deal with all the threats, then the DSAI can help us see even the smallest anomaly that occurs in a system and when it will inform the expert about the anomaly the expert can then make sure if that anomaly is an attack, malware or just a glitch

the domain specific AI will be trained on bulk data like log files, previous attacks, and all the potential attacks that can happen, information about the system and then we can just let the DSAI work by it continuously monitoring the log files and if it finds any anomaly in the user or the system it can prevent that by either blocking the access of the user or by reporting the user to the experts who can make sure that the anomaly is real threat

the domain specific AI can also help to keep the system safe by continuously reading the traffic and because of its training and pattern seeking algorithm it can predict the possibility of a incoming attack or a malware travelling through traffic which can harm the system and cause data breech and more potential lose

if we give the domain specific AI more power than just to monitor and report we can reduce the human labor and a company can save a fortune by implementing DSAI model in their security protocols, the DSAI when granted power can automatically block user control if the DSAI detects or predicts any type of threat from the user to the system

it can help the humans working to resolve some issue or attack by suggesting them methods to solve the problem in a efficient way and to patch it afterward completely, the DSAI with control can also be able to perform pentesting to see all the vulnerability of the system and help in patching those vulnerability to make the system more efficient and secure

the domain specific AI can watch a system, user, network, log files and more simultaneously and detect the smallest issue that can occur or will occur in the

system, it can report the issue to an human expert who can see and understand the problem and also the DSAI can itself analyze the issue and provide suggestion to the best possible ways to eradicate the ongoing problem

- ***Efficient Pentesting***

Pentesting is a very important part of security analysis of a system it provides us information about system its vulnerabilities and its strengths and by using the concept of domain specific AI in the pentesting process we can reduce the time and efforts taken for testing a system, the role of DSAI in pentesting a system is to attack a system in different ways like phishing mails, finding backdoor in system and more

domain specific AI can read the code of the system and can find issues or backdoors through which the attack might happen, it will detect the issue and report it so that the issue might ret resolved

we can use the pattern seeking algorithm if domain specific AI to scan a system multiple times and find a weak spot in the system

automation of the pentesting process can also be done using the domain specific AI the DSAI trained on data from all the pentesting done by experts will have the knowledge to perform the pentesting on a system without the need or help of a human this can help the companies and save a fortune of money just by automating the process of pentesting

if the system has faced any attacks before, the DSAI can prioritize the pentesting by checking all the possible ways the system might be in danger from future attacks and the DSAI can prevent those attacks by reconfiguring the system and patching all the issues that it might face

the DSAI can generate test cases to check against the system code which can reduce human effort and labor by generating manual test cases to check against the system

pentesting is not a one time process only a system needs continuous pentesting and bug fixes to be efficient and by domain specific AI we can have continuous watch over the system and test the system rigorously to find any vulnerability that can cause error and fixing that issue to make the system efficient and secure

by using the algorithm of domain specific AI we can make the process of pentesting more productive and make the system more secure by finding and fixing all the issues that the system might face now or in future

- ***Behavior Analysis***

cybersecurity relies on the “normal” working of the system and network, and that’s why the we have to keep an eye on the traffic and system configuration but doing it continuously is a very tedious task at hand, by implementing domain specific AI we can keep a continuous watch on the user logs, system files and working and also the network traffic

with the help of DSAI we can detect the slightest change in the system that is not normal and can be regarded as anomaly, the anomaly then is to be reported to the experts or is to be eradicated from the system

- ***Encryption and Decryption***

there are many good encryption algorithm that help us keep the data secure throughout the internet algorithms like “RSA” which is a Asymmetric encryption algorithm that has a private key and a public key the data is encrypted with one users public key and can only be decrypted by the other users private key this type of algorithms are widely used in apps like “Signal” which is an alternative to the popular messaging app WhatsApp which uses E2EE (end to end encryption)

the use of domain specific AI in the encryption and decryption can be very beneficial, the DSAI can analyze the system and can suggest the best possible algorithm that can be effectively implemented to keep the system, data and the users secure from malwares and the attackers

by using domain specific AI we can detect the anomaly in the encryption key and the DSAI can suggest hoe to fix the problem efficiently and make the system more secure

the DSAI can be also implemented to create a new type of encryption algorithm based on the knowledge of existing algorithms and the with the help of some cryptologist that can be fast and secure

with DSAI we can also decrypt files if we integrate the tools used for decryption of information with DSAI and then implement that new tool the enhanced tool can retrieve the information

for decryption we have many open source tools that we can integrate with the algorithm of DSAI tools like “John the Ripper”, “Metasploit”, ”Hashcat”, ”Ophcrack” and more

homomorphic encryption is one of the way that the DSAI can use to analyze the data without disturbing the encryption and without decryption the data inside

this type of encryption can be implemented with the help of DSAI in which the data can be analyzed without breaking the confidentiality and the trust of the user by keeping the data encrypted

the DSAI can be used to change the type of encryption used in a system from time to time based on the security it is providing if there is a more secure algorithm the DSAI should recommend that algorithm to the expert or implement that algorithm to the system by itself to keep the system secure and protected

- ***Advance Threat Prediction***

the point **Behavior Analysis** also lies under this point, the traditional way of threat prediction consist of human experts watching user logs and network traffic looking for something unusual in the system but this method of searching leads to no result majority of the time

but by implementing the algorithm of pattern recognition and continuous searching the system for unusual activities DSAI can reduce the effort of human labor and increase the efficiency of scanning the system by automating the task at hand

DSAI can read bulk of data within minutes and can find even the smallest anomaly in that data or the system itself, which can be reported as a advance threat to the system the anomaly can be anything unusual log report, malware, suspicious file

one of the data set on which domain specific AI is trained on is previous attacks and potential attacks by learning how an attack can take place in the system the DSAI can continuously keep watch for such activities and if anything like that happens the DSAI can report it as threat so it can be delt with before the system is compromised

the DSAI can use **Behavior Analysis** to regular scan the system, data logs, user logs and check for suspicious activities in then and even the smallest unusual activity can be regarded as potential threat and can be kept under more surveillance when and if the threat grows the threat is to dealt with by blocking the access of threat to the system or eradicating the threat by specific tools

real time threat detection is a thing that DSAI can provide us with, it can be trained on user logs and data and network logs but it can also watch them in real time and from there only it can detect the threat to the system inn real time and with current data at its disposal

with the help of DSAI pattern that are be hidden to human experts can be found and checked if it is safe for the system or not

by implementing the DSAI the advance threat detection process can be improved by automating most of the manual work that were done by human, the pattern detection algorithm of the domain specific AI can detect patterns in the system that can be regarded as threat and can eradicate the threat by either reporting it or by dealing with the issue

- ***Explainability***

the domain specific AI can offer suggestions for the problems or issue occurs in the system but it cannot give the reason why it came to that particular conclusion this is where Explainability of AI is efficient because with it the DSAI can provide us with the solution to a problem and also why and how it came to that conclusion it can provide that information too

with Explainability in DSAI it can built a trust with the experts because it will not only provide with the solution to a problem it can also explain why and how it came to that conclusion to solve issue this can lead to experts trusting the decision of DSAI and implementing the solution without any hesitation

the explainability reduces biasness, because the DSAI will provide with the reason how it came to a conclusion, which can lead to better implementation of the cybersecurity methods and protection of data

the DSAI's explainability leads to efficient collaboration between human experts and the DSAI because of the trust that explainability brings for human satisfaction to trust a machine, it provides the chain of processes it did before giving the conclusive result

accountability is one more thing that explainability brings because it give us how it came to the result so the result if false is accountable by the DSAI only not the data it was trained on, and because of its providing the way it get the result the detection of result correctness ca also be done efficiently and risk of error can be reduces by implementing the wrong method to protect the system in the time of a issue or attack

with explainability in DSAI we can remove and reduce error and issue in the model and make the model efficient, because it can show and explain that how it came to a particular conclusion we can see if the model's reasoning is working properly or there is a bug or issue in the DSAI which is causing it to

give incorrect results we can remove the issue and make the DSAI efficient to provide and help us in the field of cybersecurity

Result & Conclusion

there is no direct way of implementing the algorithm of domain specific AI to cybersecurity because cybersecurity is branch of computer science that deals with securing our data and information from people who want to exploit them for their own benefit, we can implement the algorithm of domain specific AI in the field of cybersecurity by integrating the algorithm with the tools used in cybersecurity

we can integrate the algorithm with the most popular cybersecurity dedicated Operating System out there “Kali Linux” which preinstalled contain some of the most popular pentesting and cybersecurity toolkits out there and there are all open source and free for use

this image above is the view of a “Kali Linux” Operating System running as a virtual machine as we can see there are some tools given at the bottom of the Linux distro tools like “Metasploit”, “Wire Shark”, “Burp Suite” if we integrate tools like “Wire Shark” with the algorithm of domain specific AI we can train the tool to search for anomaly throughout the network traffic incoming and outgoing

tools to which we can integrate the algorithm of domain specific AI are “Hashcat”, ”John the Ripper”, “Autopsy” and more we can use these with integrated DSAI to enhance the cybersecurity of the system and do pentesting to improve the system’s security by finding vulnerabilities in the system and the network

we can also use the DSAI as an individual application or software running on the system and providing us with the insights about the system and the network and it can also give us suggestions about what to do when the system is at risk of getting attack or there is a bug in the system that can cause potential damage

we can also implement the concept and the algorithm of domain specific AI in different fields of cybersecurity like threat detection and prevention, we can integrate the algorithm of domain specific AI with threat detection tools like “Nmap” a network mapping toolkit which sees the network traffic incoming and outgoing and if we integrate it with DSAI algorithm we can scan particularly for the abnormal network activity, malware travelling through network and can read bulk of traffic data within minutes

we can train human as well as the algorithm to work in coordination with one another to make the system and the network more secure and robust by implementing several training practices that can train the humans how to efficiently use the technology of DSAI to get the suitable result according to need of user “Prompt engineering” is a better way to describe this training because to ask DSAI for a specific kind of result you must know how to write sophisticated English clear and concise because then only the algorithm will be able to understand you and what exactly you want it to do means what is your question and what kind of result are you expecting from the algorithm

training the algorithm on bulk of data related to cybersecurity can make it have more knowledge about the field than a human expert but human are creative and that’s the skill which when we combine the knowledge have by trained DSAI and the creativity and problem solving skills of a human expert we can create a system and network that is nearly impenetrable by any kind of attack or any kind of malware

if using the DSAI in a company security we can install a web scanning tool integrated with the algorithm on domain specific AI on each of the computer and network that is used in the company to keep an eye on the actives of the user and to continuously scan each computer and network for scam or phishing email and websites

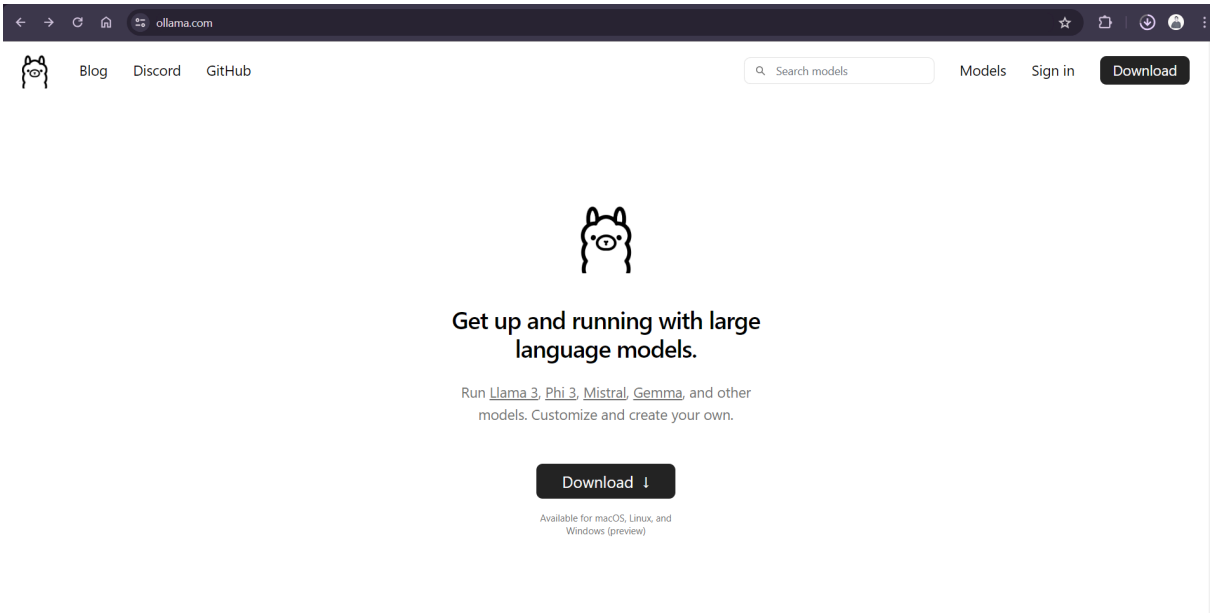
there are many different real world use of the algorithm of domain specific AI like the cost efficiency which reduces the money spent on maintaining a cybersecurity team to perform a task that the DSAI can perform in less resources and in less time period which not only makes it cost efficient but also work efficient too

we can perform many tasks just by harnessing the capabilities of DSAI effectively and efficiently, tasks like robust treat detection in the system and the network which can be performed in real time with bulk of incoming, outgoing traffic coming and going through the system and the network the algorithm can detect even the smallest anomaly in the traffic and can fix it through pre trained data sets or it can report the anomaly to a human who can analyze and fix the error

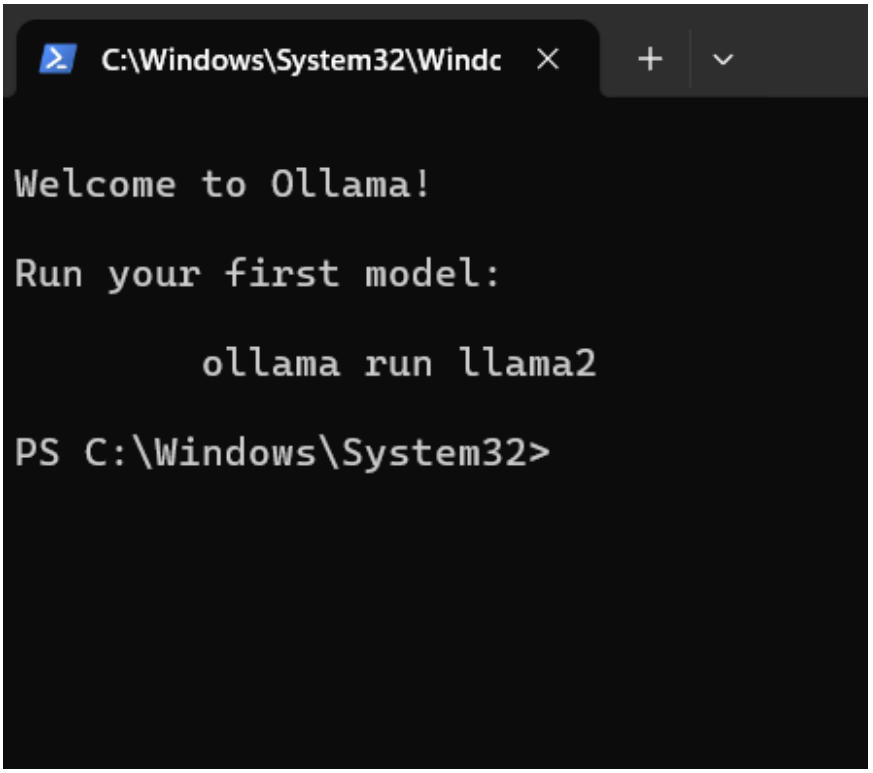
continuous monitoring and threat hunting is a thing that use the algorithm of domain specific AI to scan for the vulnerabilities in the system and the network continuously so that any issue can be found and fixed as soon as possible without causing much damage to the system and the network which can result in loss of money, resources and data

future scope of DSAI in cybersecurity can consist of evolving DSAI which means the algorithm which can train itself on the data it collects while working to resolve issues in the system and the network this self evolving DSAI will be more effective in solving creative problems like humans because it can train itself based on errors

explainability in DSAI is one more thing that might be a essential feature in future the algorithm can provide the solution to a problem in the system and the network and can also explain why it has given that solution only it will explain its chain of processes based on which it concluded this result



there is a website called `ollama.com` which help us install Large Language Models on out computers and systems locally so can fine tune them and train them on our set of data so that we can use them as we like to protect our system and network



this is the how the software ollama software is going to be we can run it from the terminal by simply writing the command `ollama run <model name>` and pressing enter using this method of fine tuning the models and not building them from

the scratch can save us lots of time and resources and with the technique like fine tuning we can make the LLM (Large Language Model) our own and trained on custom data

for fine tuning a model first we have to select a custom model like llama, Bert, GPT and more then we have to prepare the input format and check the training data is compatible with the input format or not if not we have to then choose other LLM but if yes we can proceed forward in fine tuning the model then we fine tune our model using a framework like TensorFlow, Pytorch, Pandas and more

```
# Import libraries (replace with your chosen framework)
from transformers import AutoModelForSequenceClassification, AutoToken
izer

# Load the pre-trained LLM and tokenizer
model_name = "bert-base-uncased"  # Replace with your chosen model
tokenizer = AutoTokenizer.from_pretrained(model_name)
model = AutoModelForSequenceClassification.from_pretrained(model_nam
e)

# Prepare your data (replace with your data loading and preprocessing logi
c)
train_data = ...  # List of training data points (text and labels)
val_data = ...  # List of validation data points

# Define optimizer and loss function (replace with your chosen functions)
from transformers import AdamW
optimizer = AdamW(model.parameters(), lr=2e-5)  # Learning rate adjustm
ent might be     needed
loss_fn = ...  # Choose a loss function relevant to your task (e.g., cross-entr
opy for  classification)

# Fine-tuning loop (replace with framework-specific training loop)
for epoch in range(num_epochs):
    # Training loop on batches of data
    for data in train_data:
        # Prepare model inputs (replace with your data structure)
        input_ids = tokenizer(data["text"], padding="max_length", truncation=
```

```
True)
        labels = data["label"]

        # Forward pass, calculate loss
        outputs = model(**input_ids)
        loss = loss_fn(outputs.logits, labels)

        # Backward pass, update weights
        loss.backward()
        optimizer.step()
        optimizer.zero_grad()

    # Evaluate on validation set (replace with framework-specific evaluation)
    # ...

# Save the fine-tuned model (replace with your chosen saving method)
model.save_pretrained("my_fine-tuned_model")
```

this code shows us a example of how we can fine tune a model and train it on our own set of data to make it compatible with the needs we have in the field of cybersecurity, fine tuning uncensored LLM models we can achieve the same result as developing a custom DSAI all from scratch

Discussion

from the above advantages, disadvantages and implementation we can see that there are many positive as well as negative side of the point in using the algorithm of domain specific AI in the field of cybersecurity

the positive side being:

1. Early threat detection and prevention
    a. this elaborates the use of domain specific AI as a prediction algorithm based on its training data and the system configuration it can predict what might cause an error in the system and the network
2. Efficient Pentesting
    a. using the power of algorithm as a pentester is one more thing that we can achieve and by doing this we can brute force our way into the

system telling and finding all the vulnerabilities that the system might hold

3. Explainability
    a. this is a developing concept now but we can use the technology of DSAI with full trust if we can understand how it comes to a conclusion that's why explainability is one of the most crucial part in using and trusting the DSAI

the negative side being:

1. data quality & quantity
    a. one of the most important problems of DSAI is its training because cybersecurity is a very private sector not many data is there to train the algorithm and what data is there can be either incomplete or inconsistent
2. human expertise
    a. the trust is a very valid point as we cannot trust the algorithm fully we need human experts to oversee all the work done by the DSAI algorithm validate and check the credibility of the solution provided by the algorithm
3. misuse
    a. there are many different ways that a good thing can be used for bad purpose like the algorithm of DSAI can be used for extracting all the information about the system its vulnerabilities and how it can be harmed

so the use of DSAI in the field of cybersecurity is possible but with some adjustments in the DSAI like introducing the “XAI” so called explainability AI in the DSAI so that it can build a trust of humans in the algorithm and make them work efficiently and effectively

Conclusion

this paper contains the possibility of using the algorithm of domain specific AI for real world issues and also how we can use the pre existing models and with the help of fine tuning we can make the LLM our own by training them on set of data that we want from the field of cybersecurity

in this paper we have discussed about what is advantages and the disadvantages of using the concept and the algorithm of domain specific AI in the field of cybersecurity and how we can make the algorithm better to be used in cybersecurity or any field more efficiently any effectively and can provide results

so using the algorithm of DSAI in the field of cybersecurity can be beneficial but it comes with it's own set of disadvantages and problems so if we want to integrate the technology of DSAI we first need to advance the technology of DSAI by using many different methods which are discussed above in the paper like fine tuning and explainability

Limitations

- ***Data Quality and Quantity***

DSAI holds immense potential in the field of cybersecurity, but it has disadvantages too like the data the DSAI is trained upon it clings to that data to produce outcome and if the data is by chance wrong the result will be full of errors

the data DSAI is trained upon is bias which impacts the result the algorithm generates, and because of the biasness of the result the DSAI cant be trusted fully and all the suggestion and solutions the algorithm generates has to be tested by human expert before implementing it it the system

if the data the DSAI is trained on is by any chance incorrect, incomplete or bias it can create lots of problem for the system the faulty algorithm can flag a harmless activity as a major threat and can report it which can cause panic among the experts because the activity is harmless so experts cannot be able to find threat in the activity this will waste time and resources of the company and even can lead to potential threat generation while solving a non existing threat

fault in training data can also lead to missing threat which can cause attacks to the system and potential loss of data the system holds, the DSAI because of its data fault can regard a threat as a harmless activity which leads to system vulnerability

to train DSAI algorithm bulk of data is required but in the field of cybersecurity cyberattacks are very scarce and and not all attacks are public so that we can train the algorithm on them most of the companies keep these types of information classified to prevent the image and reputation of the company

which leads to less training data on which we can train the algorithm and because of less and incomplete data on which the algorithm is trained upon it can result in incorrect results, missing threat and more

the companies often outsource the task of cybersecurity to security firms which means that any company might not agreeing to share their sensitive information about their users and network because of security concerns

- ***Explainability***

the DSAI can detect threats but can be black box when it comes to explaining the reasons it concluded the result as it did and why it regards something as threat to the network or the system, this lack of explainability of the DSAI can leads to many problems between human and DSAI collaboration and coordination

because of lack off explainability the DSAI can cause lack of trust for itself from human experts that can lead to humans rechecking every solution the DSAI provides them to ensure the solution is safe for the system which takes up time and resources and can cause damage to the system if there is a critical issue at hand to solve

the DSAI can cause error and false information if the data it was trained on was in any sense incorrect or incomplete and to pinpoint the exact reason and data from where the fault is generating can be a very tedious task because of lack of explainability of algorithm we cannot find out what part of the algorithm is generating the error and causing incorrect and faulty answers

without explainability in the algorithm the DSAI can produce bias results without explaining how it came to that conclusion which will be the result of the data it was trained upon and can cause discrimination among better solution to that problem

accountability is thing that DSAI lacks because it is unable to explain the chain of processes it did before getting the result so no one can know if the result the algorithm came up with is the result of the data the DSAI was trained upon or the computation it did while searching for the answer from the training data

because of the algorithm lack of explainability it is difficult to use the DSAI in the field of cybersecurity because it might cause more harm than good if implemented, one of the main problems it will cause is the trust issue between the human and the algorithm

- ***human expertise***

the DSAI can provide solutions to resolve issues that occur in the system but they rely on human experts to check the solution the algorithm has provided them to see if the solution is valid or not for particular issue at hand

the humans oversee all the work done by the algorithm and they validate the work of DSAI then only the solution provided by the DSAI is to be implemented in the system, humans acts as a supervisor to the algorithm validating and rejecting every result the algorithm provides for any issue in the system

the algorithm needs human experts to prompt it about the specifications of the threat they are facing and the goal the experts have in mind about this threat, human experts prompt the algorithm about what is the priority in the system and which type of threat should be dealt with first if there are multiple threats to the system

the DSAI training data is also been curated by humans to train the algorithm about the possible threats and the previous threats that occurred or can occur in the system so that the algorithm can give solutions about the issue that the system might facing

the algorithm need human to monitor its performance and assess the result the DSAI is providing to check the quality of the result, the biasness of the result and accuracy of the result so that if the algorithm is at fault it can be repaired and be made better so that it can perform its work efficiently

humans experts are responsible for establishing guidelines and policies according to which the DSAI should perform its computation and generate the output, they put some censorship so that data about the company security may not be at risk of getting leak

the algorithm can provide solution but the human experts have to interpret the solution provided to check and see how is that solution going to work in that situation

- ***Misuse***

the data on which algorithm is trained upon can be inherently biased and because of this issue the algorithm yields the result which is discriminating the expert who trained the algorithm because of his/her training data the algorithm can be misused to flag things and activities that are of a particular type

algorithm can be misused to find all the vulnerabilities in the system and all the security flaws the network and the system holds which can lead to network and the system being attacked and compromised

if the algorithm is trained on information about the companies security and vulnerabilities the DSAI become one of the important piece of software for the company and one of the most dangerous piece of software also because if used wrongly or misused by someone the algorithm can reveal all the sensitive data and information about the company's security and issues with it

attacker might get bypass the algorithm's security and can alter the data on which the algorithm was trained upon to get the result which the attacker wants and if implemented to the system the attacker can easily bypass and crawl into the system and network to steal data

the attacker if understood how the algorithm protects the system he/she can use that information to their advantage and can exploit the vulnerabilities of the algorithm to get access to the system and network like the attacker can craft a malicious malware that he/she can let wander through the system's network which can be bypassed by the algorithm because of its normal activity like disguise

constant monitoring the user can lead to user too getting attacked by the attacker because the algorithm if cracked can lead to users information too that are stored on the system and the attacker can use that information to exploit the user that is present on the system

- ***Attacker DSAI***

the algorithm for DSAI can be present or made by the attacker too which can cause trouble for the system and network to protect itself from attacks caused by an automated algorithm that is trained to brute force its way into the system and get all the data from the system and the network

the attacker algorithm can write better malware that can go undetected by the experts and the attacker algorithm can read and analyze the security DSAI to predict and break its security methods by writing a bug or a malware that can go undetected

algorithm used by the attacker can use tools like social engineering toolkit (S.E.T.) to create a perfect replica of any social web app and can mail it to look like just a reel or a funny meme but as the user enter the web app algorithm can access the system through the bug it hid in the S.E.T. web app it has created

attackers can use the algorithm to automate dumping attacks on the system continuously without pause which can cause the security DSAI to choke on the

large amount of attacks coming without break that can give the attacker algorithm to reach and infect the system and network

the algorithm used by attacker can increase and innovate new ways to attack the system which makes it much more harder for the security experts and the security DSAI to analyze threat and prevent it from happening in advance

the attacker's algorithm can mimic the security DSAI and can help the human attacker to make the attack he/she is planning more complicated and more difficult to be predicted, analyzed and resolved by the real security experts and the security DSAI

the algorithm used by attacker can be used to monitor the system continuously for any security vulnerabilities that are not found yet and exploiting those for the sake of stealing data, information and doing sinister activity with control over system

- ***Job Replacement***

the rise of DSAI in the field of cybersecurity will bring concerns about the topic if they are going to replace human workers with machines and DSAI because the use of algorithm is more efficient, productive and cost saving as compared to human

threat monitoring can be automated so that if there is any slight issue in the system the algorithm can detect and repair the issue for the system to run efficiently and this automation needs no human guidance so humans will loose their job as threat management expert

security response can also be managed by the algorithm by containing the data that is causing security issues to the system by doing so the algorithm also takes one more job of security response team whose work is to detect and contain the threat to the system

because of the bulk of data it is trained upon the DSAI also has more knowledge than any cybersecurity expert which make the algorithm's suggestion and solution about potential issue more reliable than that of human's

the algorithm can also be used as a pentester to detect security flaws that the system might has so that we can resolve those issues at hand and make the system efficient and more effective

DSAI can perform the work of a security professional the algorithm can analyze the system an can provide us with insights about the system and network and what are the issue they are facing now or in the coming future

the algorithm is cost efficient means it require less money than to maintain a team of cybersecurity experts to keep company's security at check but with the algorithm all task can be performed by it and it require only some set of GPU's to work efficiently and fast

DSAI can analyze the vast amount of data and traffic in minutes which can take human labor to analyze in months and with human analysis of vast amount of data error can also be generated in the analysis

- ***not safe***

using the algorithm in sectors where security is not limited to a company or an organization sectors like weapons armory if the algorithm got a fault or a bug and is deployed in the weapons armory this can lead to catastrophic events like missile launched in areas where people can get hurt and if an attacker penetrates the DSAI security and get hold of the weapons the whole nation can be kept hostage to the attacker

algorithm in the cybersecurity of space organizations can also cause damage if there is a successful attack or a bug occur in the DSAI the problems which can be caused are satellite transmission will be interrupted potentially stopped, countries defenses of missile targeting using satellite will be stopped completely, communication will stop, the attack or the bug might send a country economy and development back nearly 4 to 5 years

DSAI in nuclear power plants as cybersecurity tool can be dangerous not only for the country but also for the world because in nuclear power plants one miss calculation can potentially cause a very horrible event and if the algorithm fails to protect the system nuclear catastrophe can occur

use of algorithm in the cybersecurity of power grid can also be considered unsafe because if there is faultiness in the DSAI it can cause a blackout and in the worst case scenario short circuit in the power station which not only cause huge money loss for the government it will cause disruption in the day to day life of ordinary peoples too

in all these scenarios the use of algorithm the domain specific AI integrated with cybersecurity can cause much harm to any system on which it was deployed to protect it if the algorithm comes with a bug or infected by bug or an attack is to happen on the system and network and the DSAI was unable to protect the system then the algorithm becomes the system's own worst enemy and can cause damage to the system and the network which can cause economic loss, increase in crime, and disruption of life of many peoples

- ***overdependency***

the development of DSAI in the field of cybersecurity will cause overdependency on the algorithm which gives the algorithm more control over the system and the network that can result in faults if there is an attack or bug in the algorithm

thee bug in the algorithm can cause the system to flag random activities as threats which can cause problems because the flag threat will be analyzed and cause waste of the system's resources to check a false threat

the algorithm will provide a false sense of security for the system and the network which ensures that the system and the network are safe but at the end the algorithm is a machine and can be vulnerable to bugs and attacks

DSAI can produce high amount of alerts if the system is at continuous attacks from outside source or the algorithm detects from the data analysis which can cause difficulties to identify the root cause of the problem and solve it

the algorithm is only trained on the existing problems and their solution but with rise in technology new ways of cyberattacks are also a major problem and the algorithm cannot solve new issues and attacks without having information about it

DSAI is not intelligent and creative with problems as humans so if there is any problem arrive which the algorithm cannot understand it could potentially harm the whole system and the network because of the overdependency and use of algorithm in the field of cybersecurity to protect the system and the network

the overuse and the overdependency of the DSAI in the field of cybersecurity can cause problems like debugging the issue if the algorithm itself is at fault or if any of the malware that travelled through the system got hold of the algorithm and infected it this can cause leak of all the vulnerabilities that the system and network might have

- ***computation cost***

the algorithm requires powerful computation resources to perform its task efficiently and without causing any issue

DSAI is trained on bulk of data which needs very powerful computation to be processed and this powerful computation require powerful costly resources which help us to train the algorithm according to the information we have or the data we possess that can be stored into the storage of the system where the algorithm is trained

running these powerful algorithms require high processing power which are provided to them by the costly Graphics Processing Units (GPUs) and Central Processing Units (CPUs) and without the GPU in the system the algorithm cannot be able to work properly like the “Chat With RTX” a NVidia’s custom AI model that will only run on the system containing its GPU “NVIDIA GeForce™ RTX 30 or 40 Series GPU or NVIDIA RTX™ Ampere or Ada Generation GPU with at least 8GB of VRAM” and the algorithm of “GROK-1” by “XAI” it is an open source AI model and require “cuda” to perform efficiently

the high computation and resource cost of the algorithm makes it more difficult for the small companies and industries to integrate it with their cybersecurity protocols only the companies and organization that are well stablished can integrate their security with DSAI and increase protection of data because they can afford the heavy costing of training the algorithm and the GPUs on which the algorithm is going to rely to do computation and provide the result

with increasing threat the cost and expenses of the algorithm is also going to be increasing because as the level of threat increases the algorithm is to be trained on the new threats so that it can protect the system and the network form evolving threats which require costly resources to train the DSAI

continuous working of the algorithm can make the hardware at fault frequently and replacing these hardware cause not only money but also stops the algorithm from working which makes a window for the attack and if the attack is placed at that time precisely the system can be compromised with all the data in it

References

- https://gemini.google.com
- https://www.ollama.com/
- https://github.com/ollama/ollama
- https://github.com/xai-org/grok-1
- https://huggingface.co/
- https://platform.openai.com/docs/guides/fine-tuning/analyzing-your-fine-tuned-model
- https://www.ibm.com/topics/fine-tuning
- https://iamtrask.github.io/2015/07/12/basic-python-network/
- https://victorzhou.com/blog/intro-to-neural-networks/

- https://www.youtube.com/playlist?list=PLAqhIrjkxbuWI23v9cThsA9GvCAUhRvKZ
- https://victorzhou.com/blog/intro-to-cnns-part-1/