ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 3, pp: (60-64), Month: July - September 2023, Available at: www.researchpublish.com

AI in the Network Monitoring

Marek Zidek

Affiliation: Dhahran, Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.8189223

Published Date: 27-July-2023

***Abstract*: This article talks about the implementation of AI in network monitoring, its biggest advantages but also threats. It discusses in detail the history of the creation of the network and its forecasts, as well as the future in the field of protection, analysis, and improvement of services.**

***Keywords:* network monitoring, AI, artificial intelligence, IT, internet, network.**

1. INTRODUCTION

We live in the 21st century, which brings an incredible number of possibilities. Perhaps the biggest changes and advances have taken place in the field of information technology. We can give the exact year of the Internet as 1974, when the TPC / IP protocol was introduced to the world for the first time. However, as we know it today, it was recognized in 1983, and belonged to only a few important researchers and scientists who exchanged knowledge in this way.

A milestone for all people was the year 1989, when scientist Tim Berners Lee invented the WWW - that is, the World Wide Web. In 1990, the HTML formatting language was written. And in 1993, the WWW code became available to the masses, while in our country the Internet did not become widespread until after 2000.

What is a network and why should it be monitored?

We have already talked about when the Internet was created, and now let's talk about the network. A network is considered to be two or more computers that are connected in such a way that they can share their resources and allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

We know two types of networks, and they are:

1. LAN – Local Area Network –

it is a network that was created first and connects only a small area and only a smaller number of computers. It is still used in universities, laboratories, state institutions (such as prisons, where access to information must be limited), some companies and the like. You may remember this network under the name "Intranet", and it was very limited, especially at the beginning of its use. Today, however, most institutions prefer the classic Internet network. However, it should be noted that LAN monitoring is much easier.

A LAN can only operate with a few hundred devices at a time, and its performance is thus considerably limited. Devices are mostly connected to the LAN network using cables. Sometimes you can also meet the designation Wireless LAN (WLAN).

2. WAN – Wide Area Network –

Wide Area Networks (WANs) connect networks in larger geographic areas, such as countries or the world. Dedicated transoceanic cabling or satellite uplinks may connect with this type of global network.

Using a WAN, people in Slovakia can communicate with places like another continent in seconds, without paying enormous phone bills. Two users a half-world apart with workstations equipped with microphones and webcams might teleconference

in real-time. A WAN is complicated. It uses multiplexers, bridges, and routers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN.

Network monitoring is absolutely necessary

With the growth of the Internet and the necessity of using computers for work and also for entertainment, new threats in the form of viruses, malware and the like have appeared on the scene. However, network monitoring is also important for determining the performance of the given network and improving the quality of services.

Monitoring is important because it helps point out the exact location of any network problems, or prove that the network is not the source of a problem. Continuous monitoring can also help to identify potential issues before they occur, so problems can be proactively solved before they impact users.

Computer network monitoring consists of two basic parts: operation monitoring and data analysis

- **Operation monitoring -** is the use of a system that continuously monitors the computer network, slow or failing elements. The network administrator thus obtains an overview of the availability of services and servers, utilization of lines, CPUs, routers, switches, and other devices. Information for evaluation is obtained mainly via the SNMP protocol.

- **Data analysis -** is the use of a system for the collection and subsequent analysis of data in order to detect anomalies that indicate the possible infiltration of attackers into the internal infrastructure: use of the NetFlow protocol, Network Behavior Analysis and packet filtering.

We must also mention troubleshooting, which is a prompt solution to problems that have already arisen on the network. Network monitoring tools should be able to deal with every threat.

Real Time Monitoring (FMC)

this is real-time monitoring within the data infrastructure, centralized and integrated into the surveillance center, monitoring of uplinks and fixed data networks for the needs of "what, where, how, with whom". Monitoring of performance and operational parameters of communication infrastructure.

Network Behavior Analysis (ADS)

is the detection of any security or operational anomaly, threat, or unrecognizable risk within communication data networks. The system must be integrable into SIEM solutions or other third-party security solutions.

Network behavior analysis is focused on attacks (port scan, dictionary attacks, DoS, Telnet, APT, Zero Day), traffic anomalies (DNS, multicast, high variability of communication, VoIP), behavior anomalies of IP addresses (change of behavior profile), unwanted application (P2P networks, online communicators, TOR, TeamViewer), malware (viruses, spyware, botnets, communications with addresses on blacklists), email (outgoing SPAM, illegitimate mail servers), operational problems (delay, overload, reverse DNS records, service outages), potential data leaks (upload to public servers, web storage) and violation of security policies (bypassing proxy servers, unknown devices).

Monitoring of application performance parameters (APM)

this provides accurate and detailed information about how the given application works for each user, how long it takes to process individual transactions, how big is the delay on the network layer, how many users are working with the application when the application is the most loaded and many other details. It's a great way to identify even the smallest problems before the user does.

Do you know the main benefits of network monitoring?

- increasing network security and the possibility of detecting external and internal attacks, analyzing long-term statistics with a breakdown of individual computers, applications and conversations, detailed monitoring of users and services, effective planning of line capacities.

- fast and accurate network troubleshooting, immediate identification of any anomaly through automated alerting.

- through qualified reporting, obtaining clear statements about network traffic, easy planning and monitoring of QoS, peering control and service quality agreements (SLA).

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 3, pp: (60-64), Month: July - September 2023, Available at: www.researchpublish.com

Who or what performs network monitoring?

At the very beginning of the computer era, before sophisticated network monitoring protocols were developed, this function was performed by an authorized worker. At that time, of course, it was much easier, because only a few local computers were connected to the network.

With the mass advent of the Internet, of course, this would not be physically possible, and therefore network monitoring protocols had to be developed and constantly improved.

In addition to the well-known protocols for network monitoring (most tools use protocols like SNMP, NetFlow, Packet Sniffing, or WMI), there is a huge number of privately and corporately used software on the market.

Thanks to the constantly evolving market and various threats on the Internet, software engineers are forced to develop increasingly sophisticated and "smarter" network monitoring tools. Such tools include AI or artificial intelligence.

What is AI and when was it first used for network monitoring?

The term AI was first used in the 50s and means artificial intelligence, but as for the short history of AI, it first appeared on the scene in 1997, when IBM's Deep Blue became the first computer to beat a chess champion when it defeated Russian grandmaster Garry Kasparov.

With the massive development of technology, scientists also had the means to invent AI - a machine that is constantly learning and thus imitates human behavior and shows signs of individual intelligence.

The real milestone came after 2010

The discovery of the very high efficiency of computer graphics card processors served to speed up the computation of learning algorithms. The computing power of these cards (capable of more than a thousand billion transactions per second) has enabled considerable progress with limited financial costs (less than 1000 euros per card).

- For example - in 2012, Google X (Google's search lab) will be able to have an AI recognize cats on a video.

- In 2016, AlphaGO (Google's AI specialized in Go games) will beat the European champion (Fan Hui) and the world champion (Lee Sedol) then herself (AlphaGo Zero).

Where did this miracle come from? A complete paradigm shift from expert systems. The approach has become inductive: it is no longer a question of coding rules as for expert systems, but of letting computers discover them alone by correlation and classification, on the basis of a massive amount of data.[i]

The phrase "machine learning" thus acquires a completely different dimension.

The the benefits of AI network monitoring are as follows:

1. AI truly thrives is in automating repetitive tasks, acting quickly and efficiently, and freeing up staff or resources to be used in other areas. Sometimes, of course, the AI also needs to be checked to see if the system is working properly. The latest generations of AI can handle almost everything.

2. By taking over routine tasks and enhancing network efficiency, AI-driven automation can optimize network operations and reduce costs. (Many people, especially in automated operations, fear that AI will make them lose their jobs. This also applies in the IT sector. Unfortunately, innovation always comes at a price, so it's possible that some human-driven positions may disappear entirely within a few years).

3. AI led network monitoring helps you point out the exact location of any network problems, or prove that the network is not the source of a problem. Continuous monitoring can also help you to identify potential issues before they occur, so you can proactively solve problems before they impact users.

4. AI can detect unknown malware variants by analyzing their behavior. AI-based endpoint security solutions use machine learning algorithms to analyze endpoint behavior and detect potential threats. This also applies to new, potentially very dangerous viruses and malware.

5. AI operates 24x7 without interruption or breaks and has no downtime, which ensures 100% network monitorig. AI also augments the capabilities of differently abled individuals. which means a quick reaction, constant improvement, which in turn benefits the network and, last but not least, the people.

AI and data Processing and Analysis

The biggest challenge for monitoring systems is the amount of data, so they can sometimes "freeze". AI is an extremely powerful tool for quickly analyzing large amounts of data. Compared to humans or even other computers, it can process information at an incredible speed. This makes it ideal for investigating the vast amount of data generated by various network devices such as switches, routers, firewalls, intrusion detection/prevention devices, etc.

AI is also a great addition to a human IT team - AI analytics customizes the network baseline for alerts, reducing noise and false positives while enabling IT teams to accurately identify issues, trends, anomalies, and root causes. AI techniques and crowdsourced data are also used to reduce unknowns and improve the level of certainty in decision-making.

Collecting anonymous data across thousands of networks provides learnings that can be applied to individual networks. Every network is unique, but AI techniques let us find where there are similar issues and events and guide remediation. In some cases, machine learning algorithms may strictly focus on a given network. In other use cases, the algorithm may be trained across a broad set of anonymous datasets, leveraging even more data.

This Al automation will be further improved in the coming years, therefore it is assumed that AI will become a leader not only in network monitoring.

AI vs automatic Problem Solving

As we mentioned above, AI excels especially in troubleshooting. This is very important because any wrong decision can be very expensive for the network administrator. Of course, while AI appears to be 100% compared to other platforms, it's better to settle for 99.99%. Why is that so?

There are two things at play - even AI has its limits (for now) and when an unexpected problem appears on the scene, even AI can misjudge it. The advantage is that he can find his mistake and fix it in seconds. The second situation can occur when the AI is misconfigured, or programmed to do certain things, while missing a detail somewhere else.

If today's generation of AI network monitoring can't handle something, it will automatically send a response to the IT team, which will either solve the problem directly or set the AI to do so.

Machine reasoning

Machine reasoning or simply put machine learning is another important category of AI. Machine reasoning uses acquired knowledge to navigate through a series of possible options toward an optimal outcome. MR is well suited for solving problems that require deep domain expertise.

Predictive analytics

Simply put, predictive analytics refers to the use of AI to anticipate events of interest such as failures or performance issues, thanks to the use of a model trained with historical data. Mid- and long-term prediction approaches allow the system to model the network to determine where and when actions should be taken to prevent network degradations or outages from occurring.

Disadvantages of AI network monitoring

Even AI is not omnipotent, so there will be situations where it cannot help, and/or can even cause troubles:

The main privacy concerns surrounding AI are the potential for data breaches and unauthorized access to personal information. With so much data being collected and processed, there is a risk that it could fall into the wrong hands, either through hacking or other security breaches.

The second thing, which is not even a disadvantage, but rather a potential threat, is the loss of jobs for human employees, which can globally and massively bring people's hostility and fear of AI. It may even lead to discrimination and favoring AI over humans in the job market. It is also necessary to legally enshrine the use of AI in companies and corporations.

As it happens in history, new innovations also attract new threats. Unfortunately, with the development of AI, we can also expect an increased level of cyber crime and cyber terrorism.

2. CONCLUSION

AI in network monitoring is the future and already more than 80% of companies globally are giving preference to automated types of AI in network protection. Despite the continuous improvement of AI and machine learning, it is also necessary to think about the potential risk, especially in data breach protection.

Also, complete replacement of SA people is not yet possible. AI won't be able to handle all tasks. Humans are still necessary because they can look past surface-level problems and dig deeper into underlying issues. Also,we must to remember that even though AI is getting smarter every day, it still doesn't always perform perfectly. Sometimes, humans are needed to correct mistakes made by machines. Before setting the AI to some algorithm, it is good to double check the collected data. Once you've got enough data, you can begin training machine learning algorithms.

When troubleshooting, it is necessary to sensitively observe and analyze the behavior of AI, and consistently set methods for solving problems on the network. When implementing AI in a company, you should keep in mind: AI is not neutral: AI-based decisions are susceptible to inaccuracies, discriminatory outcomes, and embedded or inserted bias.

It is necessary to be aware of the potential threat when AI falls into the wrong hands (this does not mean only the potential leakage of sensitive data, but also incorrectly programmed troubleshooting, etc.).

Nevertheless, Al in network monitoring brings indisputable advantages, fast and accurate data analysis, network monitoring, detection of possible threats, problem-solving, accurate statistics, automated tasks, and many others. Problems are addressed quickly and efficiently, reducing the risk of long-term negative impacts on performance.

If AI applications become more sophisticated, they can increase productivity in many ways. By automating mundane activities, AI can free up staff time to work on more engaging tasks. Smart algorithms can also help companies identify patterns and trends that traditional methods may have missed.

Last but not least, we should also mention the performance of AI, the ability to work 24/7. The initial investment is quickly recouped, and the company can expect savings where human workers would otherwise work.

Whether we want it or not, AI will have a presence in our lives more and more. we can first expect it in the IT sector, which also includes network monitoring. We must learn to make the best of it for humanity.

REFERENCES

[1] https://www.techtarget.com/searchnetworking/answer/What-are-the-benefits-and-challenges-of-AI-network-monitoring