VIDYAVARDHINI'S COLLEGE OF ENGINEERING ANDTECHNOLOGY

BYTE

THE TECHNICAL NEWSLETTER OF COMPUTER ENGINEERING DEPARTMENT.

STAFF INCHARGE: MR. VIKRANT AGASKAR
EDITORS: MR. SAHIL KULABKAR
MR. SIDDHESH THAKARKAR
TECHNICAL TEAM: MS. BRAMHETI PATIL
MS. ANUSHKA SUPE

RUST – THE NEW AGE PROGRAMMING LANGUAGE

What is the Rust Program Language?

Rust is an open-source, multi-paradigm programming language focused on safety and performance. It is developed by the Mozilla Foundation and is used in many places, including the Firefox web browser. Rust emphasize memory safety and efficient use of resources, making it ideal for developing systems programming.

Features of Rust

Rust is an open-source, multi-paradigm programming language focused on safety and performance. It is developed by the Mozilla Foundation and is used in many places, including the Firefox web browser. Rust emphasizes memory safety and efficient use of resources, making it ideal for developing systems programming.

Advantages of Rust Programming

Rust brings a number of advantages. It is designed to be secure and reliable, making it ideal for critical systems. It also has excellent support for parallel and concurrent programming, making it great for developing high-performance applications. Rust has a simple and consistent syntax, making it easy to learn and understand. It also has a powerful ecosystem of packages and libraries, reducing development time.

Downsides of Rust

Despite its many advantages, Rust does have some downsides. It is not as widely used as other languages, making it harder to find qualified developers. It is also more difficult to debug than some other languages. Rust's speed and flexibility comes at the cost of extra complexity, making it more difficult to develop with.

Conclusion

Rust is a powerful and versatile programming language with a focus on safety and performance. It is designed for developing secure, reliable, and high-performance applications. It has a simple and consistent syntax and a rich ecosystem of packages and libraries. While it does have some downsides, such as a smaller user base and more complex development, Rust offers many advantages that make it an attractive language for developers.

AI ART GENERATOR

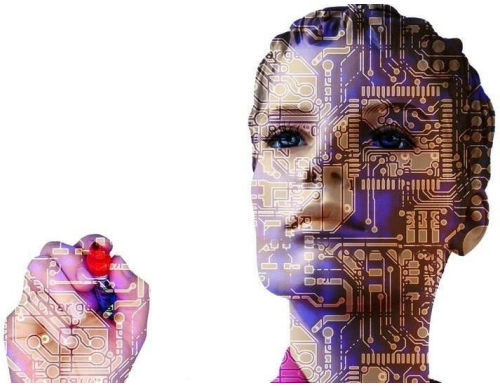
What is AI Art Generator?

Artificial intelligence art is any artwork created through the use of artificial intelligence (AI) programs such as text-to-image models. In recent years, there have been advances in artificial intelligence (AI), and people have been exploring its possible applications in various domains, including art. Yet, comprehension and appreciation of art are widely considered exclusively human capabilities.

History of AI Art Generator

The history of AI art dates back to 1973, when American computer scientist Harold Cohen created the first-ever AI painting. Cohen's painting was created using a program he developed called AARON. AARON is an artificial intelligence program that generates art based on a set of rules Cohen programmed into it–for example, one of the rules might have been to "paint a blue line." Using this rule, AARON would generate a painting that consisted of various blue lines. Cohen's "paintings" were abstract, and they were often compared to the work of Jackson Pollock. But unlike Pollock, Cohen did not drip paint onto his canvases. Instead, he instructed the algorithms he developed to draw for him. Although AARON was the first digital AI art creator, it was not the first time we had been introduced to intelligent machines. For example, Gordon Parks developed a machine called MusiColour in 1953. MusiColour was a reactive machine that responded to environmental sound to drive an

array of lights, and was one example of an intelligent machine at the time, as many others were in the development process.



Working of AI Art Generator

Art pieces that are generated by AI-based algorithms involve GANs. With a GAN, two sub-models are trained at the same time. The first is a generator model that is trained to generate new examples, and the second is a discriminator model that attempts to classify examples as either real or fake. The two models are trained simultaneously until the discriminator model is tricked about half of the time. Once this occurs, the generator model is generating plausible examples.

Conclusion

A New Era of Art. AI applications like starryai, NightCafe Creator, Artbreeder, Deep Dream Generator, and many others are ushering in a new era of AI-generated art. They are offering state-of-the-art approaches that allow anyone around the world to be an artist. These applications are also helping create this new ecosystem of NFTs and digital art, which is an incredibly fast growing market that is revolutionizing the virtual world.

HYDROELECTRIC VEHICLE

What actually Hydroelectric Vehicle is?

Fuel cell electric car (also called as Hydroelectric Vehicle) are powered by the most abundant element in the universe: HYDROGEN. As these cars runs on electricity but with the newly modification it becomes easy to stabilize the vehicle by the help of Hydrogen element. Basically, in hydroelectric vehicle the hydrogen reacts electrochemically to produce electricity to power the car. The range and performance of

hydrogen fuel cell vehicles are comparable to those of gasoline powered vehicles. They are also incredibly energy-efficient, silent, and emit no pollutants. Range, refueling time, emissions, power, and performance are valued by drivers as vehicle attributes. Fuel cell cars are available for sale or lease by major automakers in popular vehicle types, including sedans and compact SUVs. As the numbers increase, stakeholders are working to ensure hydrogen is widely available to drivers.

How it works:

Fuel cell vehicles are propelled by compressed hydrogen gas that is fed into an onboard fuel cell "stack" that converts the chemical energy of the fuel into electrical energy rather than burning the gas. The electric motors of the automobile are then driven by this electricity. There are no emissions from the tailpipe, and the only waste generated is clean water.

1. Fuel Cell Stack: A collection of multiple fuel cells that use oxygen and hydrogen to produce electricity and power an electric motor is known as a fuel cell stack.
2. Fuel Tank: To supply fuel to the fuel-cell stack, hydrogen gas is kept in carbon fibre reinforced tanks.
3. Electric Motor: Fuel cell stack energy powers the electric motor, which propels the vehicle.
4. Battery: Stores energy from regenerative braking and gives the electric motor more power.
5. Exhaust: Water vapor, a consequence of the process taking place in the fuel cell stack, is released through the exhaust.

Benefits of hydroelectric cars

1. Fun to drive.
2. Instant torque and constant, dependable power.
3. A high-tech, low-upkeep product.
4. With no emissions.
5. Speedy refuelling (3-5 minutes).
6. Having use of carpool lanes and other benefits. 7.attractive leasing rate frequently includes complimentary gasoline and maintenance.

Conclusion:

The globe depends on hydropower plants as a source of electricity. Water is a dependable and effective fuel. It is necessary to continue pursuing the usage, construction, and development of power plants. Conservation of powerplants becomes very important for us in the future for such more hydrogen fuel cells cars development

---

EXTENDED DETECTION & RESPONSE(XDR)

What is Extended Detection and Response (XDR)?

The XDR system works by collecting and correlating data across various network points such as servers, email, cloud workloads, and endpoints. The data is then analysed and correlated, lending it visibility and context, and revealing advanced threats. Thereafter, the threats are prioritized, analysed, and sorted to prevent security collapses and data loss.

The XDR system helps organizations to have a higher level of cyber awareness, enabling cyber security teams to identify and eliminate security vulnerabilities.

The term XDR was coined by Nir Zuk of Palo Alto Networks in 2018. XDR improves malware detection and antivirus capabilities over Endpoint Detection and Response (EDR). XDR enhances EDR's ability to deploy high-quality security solutions with state-of-the-art technology that proactively identifies and collects security threats and applies strategies to detect future cybersecurity threats. It is an alternative to reactive endpoint security solutions such as EDR and Network Traffic Analysis (NTA).

What does XDR means?

Extended Detection and Response (XDR) is a Layered Security Technology that protects your IT infrastructure. This is achieved by collecting and combining data from multiple security layers including endpoint, application, email, cloud and network to increase visibility into an organization's technology landscape. This allows security teams to detect, investigate, and respond to cyber threats quickly and effectively. XDR is considered a more advanced version of endpoint detection and response (EDR). Whereas EDR focuses on endpoints, XDR focuses more broadly on multiple security control points to detect threats more quickly, using deep analytics and automation.

How does XDR works?

XDR improves security performance by integrating visibility and control across endpoints, networks and clouds to improve detection and response capabilities. Linking data from disparate security solutions improves threat visibility and reduces the time it takes to detect and respond to attacks. XDR simplifies advanced investigation and discovery of threats across multiple domains from a single console. Broadly, there are three aspects to how XDR security works:

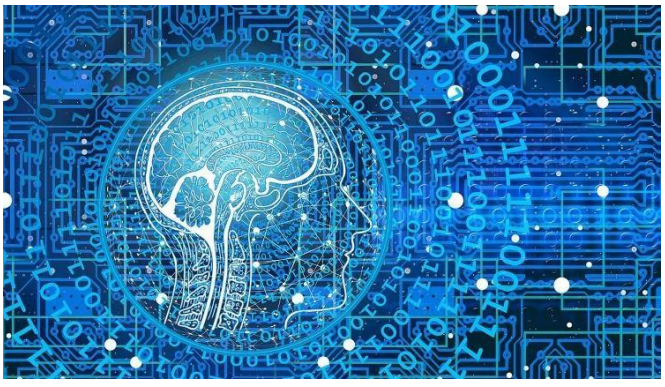
1. Data gathering: The first step is gathering and normalizing large volumes of data from endpoints, cloud workloads, email, network traffic, virtual containers and more. All data is anonymized and comprises only those elements need to identify potential anomalies and threats.
2. Detection: Then, the focus is on parsing and correlating data to automatically detect covert threats using advanced artificial intelligence (AI) and machine learning (ML).
3. Response: Next, it's about prioritizing threat data by severity so that security teams can analyze and triage new events in a timely manner and automate investigation and response activities. The response process should take place from a single centre, comprising relevant data, context and tools. XDR technology is useful for showing analysts the steps an attacker took by revealing the sequence of processes before the final attack. The attack chain is enriched with information from assets inventory, such as vulnerabilities related to the asset, the assets' owner or owners, business role, and observable reputation from threat intelligence.

Security teams often receive a high number of alerts on a daily basis, so automating the triage process and providing contextual information to analysts is the best way to manage the process. XDR allows security teams to use their time efficiently by focusing on the alerts that can cause the most damage.

NEUROMORPHIC COMPUTING

What is Neuromorphic Computing?

Neuromorphic Computing is a branch of computer science and engineering that aims to create Artificial Neural Networks that mimic the structure and function of the human brain. The goal of neuromorphic computing is to develop computing systems that are capable of learning and adapting to new information in the same way as the human brain. Neuromorphic computing implements aspects of biological neural networks as analogue or digital copies on electronic circuits. The goal of this approach is twofold: Offering a tool for neuroscience to understand the dynamic processes of learning and development in the brain and applying brain inspiration to generic cognitive computing. Neuromorphic hardware aims at mimicking a biological synapse that monitors and remembers the signal generated by the stimuli.ScN is used to develop a device mimicking a synapse that controls the signal transmission as well as remembers the signal. Neuromorphic computing systems are designed to be energy-efficient, highly parallel, and capable of processing large amounts of data in real-time.



What does Neuromorphic Computing work?

The working mechanism of neuromorphic computing involves the use of Artificial Neural Networks (ANN) made up of millions of artificial neurons, similar to those in the human brain. These neurons pass signals to each other in layers, converting input into output through electric spikes or signals, based on the architecture of Spiking Neural Networks (SNN). This allows the machine to mimic the neuro-biological networks in the human brain and perform tasks efficiently and effectively, such as visual recognition and data interpretation. These systems are based on analog or digital circuits that

mimic the behavior of neurons and synapses in the brain. These circuits can be used to build artificial neural networks that are capable of performing tasks such as image recognition, natural language processing, and robotics control. Guided by the principles of biological neural computation, neuromorphic computing uses new algorithmic approaches that emulate how the human brain interacts with the world to deliver capabilities closer to human cognition.

Advantages of Neuromorphic Computing

One of the key advantages of neuromorphic computing is its ability to perform complex computations with very low power consumption. This is because the architecture of neuromorphic systems is designed to minimize energy consumption by only activating neurons and synapses when they are needed. In addition, neuromorphic systems are highly parallel, which means that they can process multiple tasks simultaneously, resulting in faster processing times. Another advantage of neuromorphic computing is its ability to learn and adapt to new information. Unlike traditional computing systems that are programmed to perform specific tasks, neuromorphic systems can learn from experience and adjust their behavior accordingly. This makes them well-suited for tasks such as anomaly detection and pattern recognition, where the data may be constantly changing. There are several neuromorphic computing systems currently under development, including the BrainScaleS system developed by the European Union's Human Brain Project and the TrueNorth system developed by IBM. These systems are being used for a variety of applications, including autonomous vehicles, medical diagnosis, and cybersecurity.

Conclusion

Neuromorphic computing is a rapidly evolving field that aims to develop artificial neural networks that mimic the structure and function of the human brain. These systems are energy-efficient, highly parallel, and capable of learning and adapting to new information. With continued research and development, neuromorphic computing has the potential to revolutionize many areas of computing and engineering. Neuromorphic computing's innovative architectural approach will power future autonomous AI solutions that require energy efficiency and continuous learning. It promises to open exciting new possibilities in computing and is already in use in a variety of areas including, sensing, robotics, healthcare, and large-scale AI applications.

ZERO TRUST SECURITY MODEL

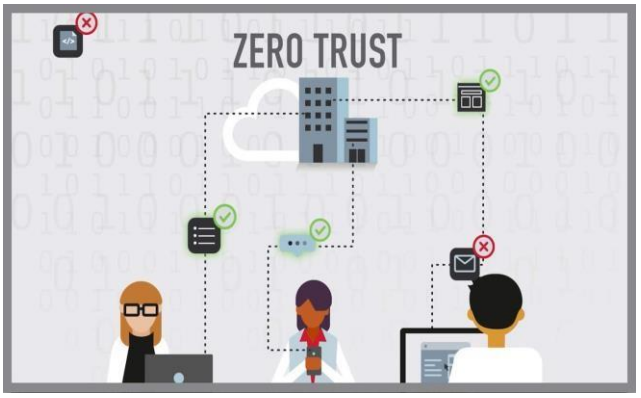
Introduction

In the age of digitalization where massive data is stored online and business processes are automated data breach is always a looming threat. It is becoming evident that the castle and moat security model is no longer adequate in protecting data infrastructures. Companies are now prioritizing cyber security by integrating security systems and implementing security policies to safeguard sensitive

data. This is why the corporate world is quickly adopting stiffer security models such as zero trust.

The zero-trust security model, also known as zero trust architecture (ZTA), zero trust network architecture or zero trust network access (ZTNA), and sometimes known as perimeter less security, describes an approach to the design and implementation of IT systems. The main concept behind the zero-trust security model is "never trust, always verify," which means that devices should not be trusted by default, even if they are connected to a permissioned network such as a corporate LAN and even if they were previously verified.

Zero trust is an IT security model, in which users and devices are granted access only when they have been authenticated and only to the resources, they need to operate. This model mandate's strict identity verification for every user or device inside and outside of the network perimeter.



History of Zero Trust Security Model

Zero trust was invented by John Kinderbag in 2010. The former forester research principal analyst, developed this model after concluding that the traditional security model which is based on the assumption that all entities within an organization's network can be trusted is an outdated approach to data security. The core principle of this approach is never trust always verify.

Advanced Technologies Used:

Since its inception zero trust has become one of the more popular concepts in cyber security the implementation of the zero-trust security model or architecture requires the combination of advanced technologies such as

- Identity and Access Management (IAM)
- Multiple Factor Authentication
- Next-Generation Endpoint Security Technology
- Identity Protection

These technologies will verify the user's identity and defend system security. The main goal of the zero-trust architecture is to prevent breaches and curb damage if the system is ever compromised.

ARTICLES SUBMITTED BY:
BRAMHETI PATIL
PRATIMA BOMBE
SIDDHESH THAKARKAR
SAHIL KULABKAR
ADITYA LAWATE

Do share your views, feedback and articles by mailing at bytemagvcet@gmail.com