VIDYAVARDHINI'S COLLEGE OF ENGINEERING AND TECHNOLOGY

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
MR. ALOK PAL

BIOHACKING AND THE FUTURE OF HUMAN ENHANCEMENT

The Rise of Biohacking

The convergence of technology and biology is ushering in a new era of human enhancement, a movement commonly referred to as "biohacking." It is a diverse and evolving field that encompasses a wide range of practices, from various biology experiments to the use of cutting-edge technologies. At its core, biohacking seeks to optimize the human body and mind through science, self-experimentation, and a deep understanding of biology.

Gene Editing: The Power to Rewrite our DNA

One of the most groundbreaking technologies in biohacking is CRISPR gene editing. CRISPR-Cas9 has revolutionized genetic engineering, enabling scientists and biohackers alike to modify DNA with unprecedented precision. While it holds immense potential for treating genetic diseases, it also raises ethical questions about "designer babies" and the unintended consequences of genetic manipulation.

Neural Interfaces: Merging Mind and Machine

Neural interfaces, such as brain-computer interfaces (BCIs), have the potential to transform the way we interact with technology. These devices can enable direct communication between the human brain and computers, opening up possibilities for controlling devices with our thoughts and even enhancing cognitive abilities.

Biometric Implants: Upgrading the Human Body

Biohackers are increasingly turning to biometric implants to enhance their physical capabilities. These implants can range from RFID chips for contactless payments to magnets that provide sensory augmentation. The ethical debate here revolves around bodily autonomy and potential health risks associated with implantation.

.

The Future of Biohacking

As biohacking gains popularity, ethical dilemmas and societal concerns emerge.The future of biohacking holds promises of personalized medicine, enhanced human potential, and improved quality of life. However, it also requires thoughtful regulation, robust safety measures, and an ongoing dialogue about the boundaries of human enhancement.In conclusion, biohacking represents an exciting frontier where technology meets human biology. While it offers the potential for remarkable advancements, it also demands careful consideration of the ethical and societal implications. As we navigate this brave new world of biohacking, finding the right balance between innovation and responsibility will be paramount in shaping a future where human enhancement benefits all of humanity.

GOOGLE CLOUD ARMOR

What is the Google Cloud Armor?

Google Cloud Armor is a web application firewall (WAF) that protects web applications from common attacks, such as cross-site scripting (XSS) and denial-of-service (DoS) attacks. It is a fully managed service that can be deployed in minutes. It uses a variety of techniques to protect web applications which includes: Rule-based filtering which allows you to create rules that define what traffic is allowed and what traffic is blocked; Signature-based detection: Google Cloud Armor uses signatures to identify known attack patterns and uses machine learning to identify new and emerging attack patterns.

Features of Google Cloud Armor

Google Cloud Armor provides a variety of features to help you manage your web application security, including:

•Logging and monitoring: Google Cloud Armor provides detailed logs of all traffic that is blocked. This information can be used to identify and respond to attacks.

• Reporting: The armor provides reports that can be used to track the effectiveness of your security measures.
• APIs: It also provides APIs that can be used to integrate with your existing security systems.
• Policy framework with rules: It configures one or more security policies with a hierarchy of rules. Apply a policy at varying levels of granularity to one or many workloads.
•IP-based and geo-based access control: Filters your incoming traffic based on IPv4 and IPv6 addresses or CIDRs. Identify and enforce access control based on geographic location of incoming traffic.

How to use Google Cloud Armor?

To use Google Cloud Armor, you first need to create a WAF (Web Application Firewall) policy. A WAF policy defines the rules that will be used to protect your web application. You can create a WAF policy from scratch or you can use a predefined policy. Once you have created a WAF policy, you need to attach it to your web application. You can attach a WAF policy to a load balancer or to a Cloud CDN (Content Delivery Network).

.

Conclusion

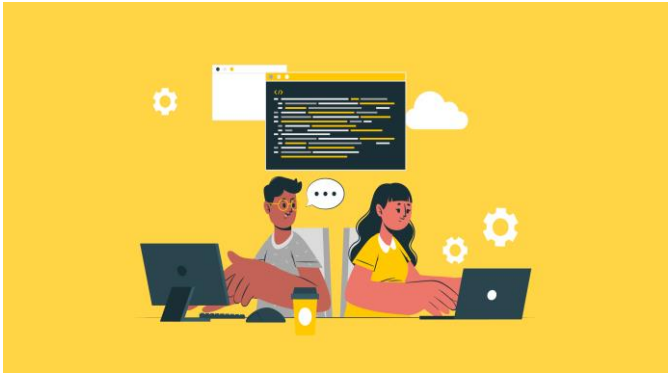
Google Cloud Armor is a powerful tool that can help you protect your web applications from a variety of attacks. It is a fully managed service that is easy to deploy and use. If you are looking for a way to protect your web applications from a variety of attacks, Google Cloud Armor is a good option to consider.

THE RISE OF LOW-CODE AND NO-CODE DEVELOPMENT

In the ever-evolving world of software development, two remarkable trends are transforming the landscape: low-code and no-code development platforms. These innovative approaches to application creation are democratizing the development process, allowing individuals with varying levels of technical expertise to build powerful software solutions.

Low-Code Development

Low-code platforms provide a visual environment for developing applications with minimal hand-coding. Developers can design user interfaces, set up data integrations, and configure logic flows using drag-and-drop components and pre-built templates. Low-code platforms still require some level of coding but significantly reduce the amount of custom code needed. They are suitable for organizations looking to streamline development processes and reduce the reliance on highly specialized programmers.



No-Code Development

No-code platforms take simplicity to the next level by enabling users with limited or no coding experience to build applications. These platforms offer visual builders and templates for a wide range of use cases, from creating websites and mobile apps to automating workflows and data processing. No-code tools abstract most of the technical complexities, making application development accessible to non-technical staff, such as business analysts, marketers, and subject matter experts.

The Benefits of Low-Code and No-Code

The rise of low-code and no-code development is not coincidental. These platforms offer several advantages that are driving their adoption across industries:
•Accelerated Development: Both low-code and no-code platforms significantly reduce development time, allowing organizations to bring applications to market faster.
•Cost-Efficiency: By reducing the need for extensive coding and specialized developers, these platforms can lead to cost savings in development and maintenance.
•Accessibility: No-code platforms democratize development by allowing non-technical users to participate in application creation, fostering innovation across departments.
•Cross-Functional Collaboration: These platforms encourage collaboration between technical and non-technical teams, breaking down silos within organizations.

Conclusion

Low-code and no-code development platforms are revolutionizing the way software is created, empowering a broader audience to participate in the digital transformation journey.As technology continues to advance, embracing the potential of low-code and no-code development may be the key to unlocking innovation and staying competitive in a rapidly evolving digital landscape.

IoMT - INTERNET OF MEDICAL THINGS

IoMT is a network of internet-connected medical devices, hardware infrastructure, and software applications used to connect healthcare information technology. IoMT allows wireless and remote devices to securely communicate over the Internet to allow rapid and flexible analysis of medical data. IoMT has the potential to revolutionize healthcare by making it more efficient, accessible, and personalized. It is still a relatively new technology, but it is rapidly growing and

evolving. As IoMT devices become more sophisticated and affordable, they are likely to become even more widely used in healthcare.

Benefits of IoMT

•Improved patient care: IoMT can help to improve patient care by providing real-time monitoring and data analysis. This can help to identify and treat health problems early, which can improve outcomes.

•Increased efficiency: IoMT can help to improve efficiency in healthcare by reducing the need for paperwork and manual tasks. This can free up healthcare professionals to spend more time with patients.

•Reduced costs: IoMT can help to reduce costs in healthcare by reducing the need for hospital visits and other procedures

•Improved quality of life: IoMT can help to improve the quality of life for patients by allowing them to stay at home and receive care remotely. This can be especially beneficial for patients with chronic conditions.

Here are some examples of IoMT devices:

•Wearable devices: Wearable devices, such as fitness trackers and smartwatches, can be used to track heart rate, steps taken, and other health data.

•In-home medical devices: In-home medical devices, such as blood pressure monitors and glucose meters, can be used to monitor patients' health at home.

•Hospital devices: Hospital devices, such as infusion pumps and MRI machines, can be connected to the internet to allow for remote monitoring and control.

•Telehealth devices: Telehealth devices, such as video conferencing systems and remote patient monitoring systems, can be used to provide healthcare services to patients remotely.

There are also some challenges associated with IoMT, such as; Security: IoMT devices collect and transmit sensitive health data, so it is important to ensure that they are secure from cyberattacks. Privacy: Patients have a right to privacy, so it is important to ensure that their health data is not shared without their consent. Interoperability: IoMT devices from different manufacturers may not be compatible with each other, which can make it difficult to integrate them into a healthcare system. Cost: IoMT devices can be expensive, which can make them out of reach for some patients. Despite these challenges, IoMT has the potential to revolutionize healthcare. As the technology continues to develop, it is likely to become more affordable and accessible, and it will have a positive impact on the quality of care for patients.

MOJO PROGRAMMING

Introduction

In the ever-evolving landscape of programming languages, Mojo emerges as a breath of fresh air. Designed to simplify and streamline software development, Mojo offers an expressive and efficient coding experience that appeals to both novice and seasoned developers. In this brief introduction, we'll take a glimpse into the world of Mojo, exploring its origins, key features, and what sets it apart in the dynamic realm of programming.

Mojo is a relatively young programming language with a mission: to make software development more straightforward without sacrificing power and flexibility. It's the brainchild of a passionate community of programmers, drawing inspiration from Perl and Perl 6. This lineage infuses Mojo with a rich syntax and ideas while introducing a fresh perspective on modern coding.

Key Features of Mojo

•Expressive Syntax: Mojo's syntax is designed to be clean and expressive, reducing verbosity and boilerplate code. This allows developers to write code that is both concise and easy to understand.

•Asynchronous Programming: Mojo embraces asynchronous programming, making it well-suited for building scalable web applications and APIs that can handle multiple concurrent connections efficiently.

•Built-in Web Framework: One of Mojo's standout features is its built-in web framework, which simplifies the development of web applications. With features like routing, templates, and plugins, developers can create web applications with ease.

•CPAN-like Ecosystem: Mojo has its own ecosystem of modules and extensions, similar to Perl's CPAN (Comprehensive Perl Archive Network). This allows developers to tap into a wide range of pre-built solutions to accelerate their projects.

•Real-time Applications: Mojo's support for WebSockets and

event-driven architecture makes it well-suited for real-time applications, such as chat applications and online gaming.

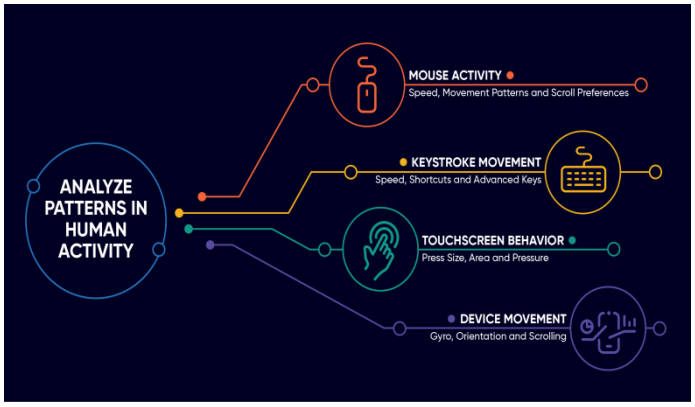
Conclusion

Mojo is not just a programming language; it represents a fresh perspective on modern development. Its emphasis on simplicity, expressiveness, and asynchronous capabilities aligns with the demands of contemporary web development. Whether you're a developer seeking a language that streamlines your workflow or an enthusiast exploring the evolving landscape of programming languages, Mojo offers an exciting journey into the world of modern development.

BEHAVIOURAL BIOMETRICS: THE PASSWORD YOU CAN'T FORGET

Behavioral biometrics takes authentication further by requiring the user to not only provide a valid fingerprint to log in, but also prove that they are who they say they are during the session. It takes into account the way a person interacts with the device, such as the force with which they press a key, the sweep angle of the touch screen or the speed of typing. By monitoring and analyzing these areas, users can safely use the same "password" - their behavior - every time they log in. In this way, the user becomes part of the security solution instead of the problem.

We need to change the way we think about security in terms of passwords, static and behavioral biometrics. Because almost all authentication technologies can be compromised, financial institutions should not rely on a single control to approve high-risk transactions, but instead should take a multi-layered approach to security, combining the various authentication technologies available to improve both accuracy and user experience.



How behavioral biometrics work?

Unlike biometrics based on static or immutable biological characteristics such as fingerprints, behavioral biometrics analyzes customer activity against a backdrop of continuous authentication. This is why behavioral biometrics are often described as passive. Behavioral biometrics look at a person's unique movement patterns to enable continuous comparison with past behavior and continuous authentication throughout the banking session, enhancing fraud protection. Such an analysis results in a score that estimates the likelihood that the perpetrator of the actions is a legitimate customer. The higher the similarity score, the less a financial institution has to worry about a person's identity and intent, thus improving the user experience. In contrast, the lack of similarity of customer behavior to their historical profile requires additional layers of authentication, such as fingerprint scanning. Behavioral biometrics combined with machine learning, which can analyze vast amounts of data to detect anomalies in real time, and risk assessment techniques can help reduce fraud.

Replicating behavioral biometrics is difficult because each person has a profile of their habits and movements, which are constantly compared to the activities performed during a banking session. There are few privacy concerns because the customer's behavioral data is converted into mathematical representations in their profile that would be meaningless to a fraudster who has access to it. Biometric behavioral algorithms can ensure that the person actually participating in a banking session is who they should be.

The market for behavioral biometrics

The market for behavioral biometrics is booming worldwide. The behavioral biometrics market is expected to witness significant growth from 2023 to 2030 due to increasing demand across types (on-premises, cloud, hybrid) and applications (government and defense, energy and utilities, banking, financial services and insurance services). (BFSI), IT and Telecom, Healthcare, Retail, Manufacturing, Others). Market growth is fueled by factors such as size, segmentation, emerging trends, sales volumes, and demand and supply dynamics. In addition, the wider adoption of advanced technologies and investments in R&D are expected to create lucrative opportunities for market development.

Conclusion

Advanced technologies have become part of our life. The more industries rely on digitalization, the easier it becomes to use them and the more sophisticated the ways that digitalization can be misused become. Behavioral biometrics allows you to stay ahead of the curve in security and improve the experience of both users and organizations.

ARTICLES SUBMITTED BY:
BRAMHETI PATIL
KARAN SANKHE
SRUSHTI GAWANDE
ALOK PAL
SAHIL KULABKAR
PRATIMA BOMBE

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