Maratha Vidya Prasarak Samaj's

Karmaveer Adv. Baburao Ganpatrao Thakare College of Engineering

Udoji Maratha Boarding Campus, Near Pumping Station, Gangapur Road, Nashik

Permanently Affiliated to Savitribai Phule Pune University

KBTCOE

ACCREDITED BY NBA NATIONAL BOARD OF ACCREDITATION

- MECHANICAL ENGINEERING
- COMPUTER ENGINEERING
- INSTRUMENTATION AND CONTROL ENGINEERING
- CIVIL ENGINEERING
- INFORMATION TECHNOLOGY (IT)

5 Programs are Accredited By National Board of Accreditation (2022-2025)

MVP SAMAJ'S KBT COLLEGE OF ENGINEERING

DEPARTMENT OF

IFORMATION & TECHNOLOGY

TECHNICAL MAGAZINE

TECHZINE

VOLUME 7

ISSUE 1

DEPARTMENT TECHNICAL MAGAZINE

EDITORIAL BOARD

FACULTY MEMBERS

- Dr. Sopan Talekar. (HOD)
- Mr. Dhiraj Birari.

STUDENT COMMITTEE MEMBERS

- President: Ayush Patel.
- Vice president: Smriti Kshatriya.
- Secretary: Atharva Bhusal.
- Treasurer: Soham Gurule.
- Event Manager: Prerna Jadhav.
- Manager: Rushikesh Binnar.

ART DESIGN

- Ms. Dhanashri Palde.
- Ms. Snehal Mogal

MAGAZINE DESIGN

- Ms. Vaidehi Chavan

ABOUT THE DEPARTMENT

The Department of Information Technology is established in 2008-09. The Department has intake of 120 students. The Department of Information Technology was established with a vision to develop quality engineers to meet the current trends in the emerging world of IT. Department has well qualified faculty members to impart knowledge to the students about the latest technologies in IT field. Department has 9 laboratories which are well equipped with necessary software along with WI-FI connectivity. The Department is also intended to provide technical support for Website development of different educational Institutions under MVP Samaj. Different Student development centered programs are arranged in the Department.

DEPARTMENT VISION

To be the Centre for excellence in the development of IT solutions with specific approach of industry interface, blended learning and project-based learning leading to the development of globally competent graduates and life-long learners.

DEPARTMENT MISSION

Committed to develop students as competent IT professionals for employment and self-employment by adapting to the innovative and interactive academic process to acquire domain specific technical knowledge, soft skills and social responsibilities

DEPARTMENT PROGRAM EDUCATIONAL OBJECTIVES

- Graduates will analyze, design and implement modern computing problems by applying their knowledge of mathematics, information technology, and emerging technologies.

- Graduates will possess an attitude and aptitude for research, entrepreneurship, and higher studies in the field of Information Technology.

- Graduates will be aware of their professional, ethical, legal, and social responsibilities and contributions towards the betterment of society through active engagement with professional societies and other community activities.

TABLE OF CONTENT

Department of IFORMATION & TECHNOLOGY technical magazine

Regret Minimization in Tech Learning

AI in Your Pocket: A Boon with Responsible Guidelines

Welcome, fellow technologists, to the rollercoaster ride that is mastering new technologies! If you've ever felt the sting of regret for not taking the initiative to learn the latest programming language or diving into a cutting-edge framework, you're not alone. In fact, you're in the majority. Today, we discuss on how to avoid this with the powerful tool of Regret Minimization.

The Fear of Regret

As developers, our love for solving problems often goes hand-in-hand with the fear of missing out on the next big thing. The daunting prospect of regret looms large, whispering, "What if you're left behind? What if your skills become obsolete?" It's a mental bug that we must debug with finesse.

Enter the growth mindset, the ultimate debugger for our cognitive code.

Regret Minimization starts with the realization that learning is a lifelong process, and every outdated skill is an opportunity to iterate and improve. Just like we debug our programs, we must debug our approach to learning.

Minimizing Regret One Step at a Time

The path to tech mastery is not about sprinting to the finish line; it's about navigating each function, method, and module with precision. Here are some practical steps to minimize regret in the learning process:

1. Set Realistic Milestones:

Instead of aiming to conquer an entire technology stack in one go, set achievable milestones. Break down your learning journey into manageable tasks, and celebrate each accomplishment. Remember, progress is progress, no matter how small the step.

2. Focus on Small Victories:

Tech learning is a series of battles, and every successful line of code written is a victory. Rather than getting overwhelmed by the vastness of a new technology, focus on solving specific problems. Small victories build confidence and pave the way for more significant achievements. If you're learning a new web framework, start by building a simple "Hello, World!" application. Once that's conquered, gradually add features and complexity.

3. Embrace Incremental Learning:

Just like iterative software development, adopt an incremental learning approach. Learn a concept, apply it in a practical project, and then iterate. This way, you're not just memorizing syntax; you're ingraining the knowledge through hands-on experience.

4. Accept Not Knowing Everything:

One of the biggest sources of regret is the pressure to know it all. Accept that you won't understand every nuance immediately. Tech learning is an ongoing process, and gaps in knowledge are not failures but opportunities to improve your understanding.
For example, in machine learning, start with the fundamental algorithms and build your knowledge gradually. You don't need to grasp advanced concepts immediately.

5. Leverage Learning Resources:

The tech community is rich with resources, remember that somewhere, someone has solved the problem. Leverage tools like stackoverflow, blogs, github, online documentation to your advantage. Don't hesitate to consult to comment on them faced with challenges, as someone will respond and accelerate your learning curve.

Future proofing

In essence a adopting a patient and strategic and continuous approach to learning is essential for , minimizing regret. Each step forward, no matter how small, will contribute to the larger framework of your expertise.
So, break down the learning process, celebrate the victories, and conquer the challenges one step at a time.

EQUALITY IN AI

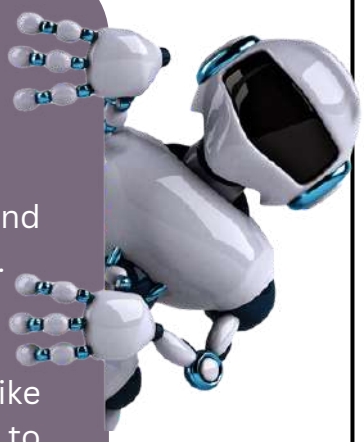
AI-based software can inherit and perpetuate existing biases present in the data used to train them. If the training data contains biased or discriminatory patterns, the AI models learn and replicate those biases, potentially exacerbating existing inequalities.

ALGORITHMIC BIAS

Scenario: Movie Recommendation Algorithm

Objective:
An online streaming service develops an algorithm to recommend movies to users based on their viewing history and preferences.

Algorithm Training:
The recommendation algorithm is trained using user data like viewing history, ratings, and genre preferences. The goal is to provide personalized movie recommendations to enhance user satisfaction.



GENRE BIAS

If the training data predominantly includes certain genres due to user preferences, the algorithm will start becoming more and more biased towards recommending movies from those genres more frequently. Users with may receive recommendations that are skewed towards some genres, potentially limiting the variety of movies suggested.

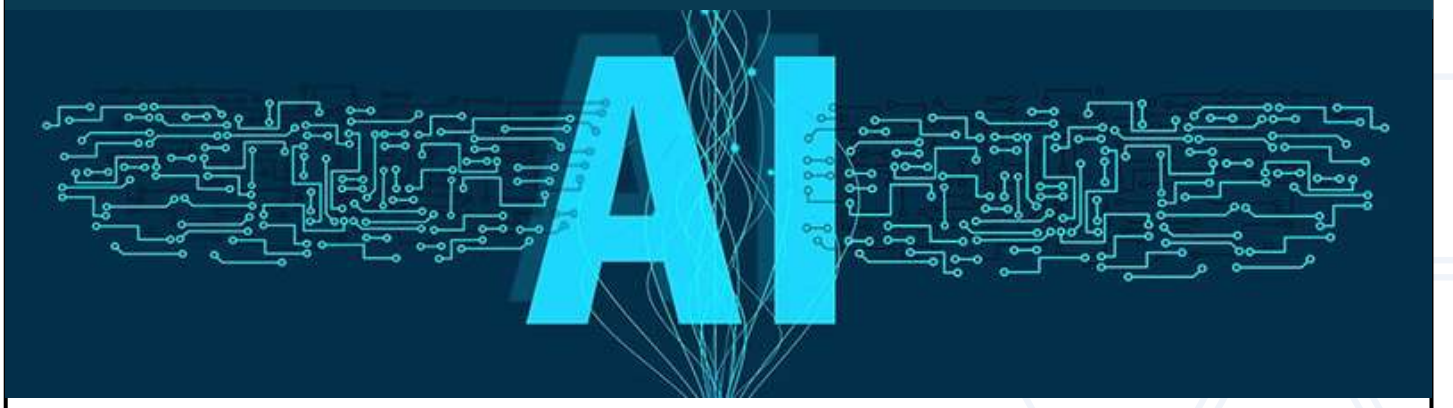
POPULARITY BIAS

The algorithm, when recommending movies, may prioritize popular or trending titles over lesser-known, independent films. This can result in a feedback loop where popular movies receive more views and further reinforce their prominence in the algorithm's recommendations.

IMPACT ON RECOMMENDATIONS:

Due to these biases, users may find their movie recommendations limited to a narrow set of genres, popular titles, and potentially missing out on discovering a broader range of content.

Department of IFORMATION & TECHNOLOGY technical magazine



DATA REPRESENTATION BIAS

Scenario: Bias in Predictive Healthcare Model

Objective:
A healthcare organization is developing an AI model to predict patient outcomes based on historical medical data.

Data Representation Bias:

- Socioeconomic Bias in Health Records - Health records used to train the predictive model may not reflect the correct distribution of socioeconomic status, with a majority of data coming from patients with higher incomes and / or better access to healthcare.
- Geographic Bias - If the model is trained on data from urban areas and lacks sufficient representation from rural communities, it may not generalize well to predict outcomes for patients in those underserved regions.

IMPACT ON THE MODEL :

The model may perform well for populations well-represented in the training data but may struggle to generalize to diverse demographic groups.

EQUALITY AND AI

It's essential to note that AI has the potential to contribute to more equitable outcomes when designed and implemented with fairness in mind.
Cognizant steps need to be taken to mitigate bias in AI systems not only when they are designed and implemented, but also over the long term, when the model continuously re-trains itself.
Ultimately, whether AI exacerbates or mitigates existing biases depends on how it is developed, implemented, and monitored. Ethical AI practices and going efforts to improve transparency and fairness are essential for ensuring that AI contributes to a more equal and just society.

Web3 - Asset Tokenization in Real Estate Industry

The Real Estate Industry needs a more secure, transparent, and efficient way to manage assets. The traditional process of buying, selling, and managing real estate is often time: consuming and cumbersome. NFTs provide a new way to manage real estate transactions faster, more secure, and more transparent manner. The decentralized nature of blockchain technology makes it possible to transparently transfer ownership of real estate assets without the need for intermediaries, such as banks or real estate agents, thereby reducing the costs. Some of the advantages of using NFT in the real Estate Domain are as follows

1) Real-time Asset Management

Real-time asset management refers to the ability to manage real estate assets in real-time, without delay or lag. By tokenizing real estate assets as NFTs, ownership, transfer, and other critical data can be stored on the blockchain, allowing for real-time access and management of these assets. With real-time asset management, processes such as the transfer of ownership, rent collection, and property management can be completed quickly and efficiently, reducing the time and cost involved in managing real estate assets. Additionally, this real-time access to information about real estate assets allows for better decision-making, as stakeholders can access up to date information about the asset at any time.

2) Transfer of ownership

The transfer of ownership refers to the process of transferring ownership of a real estate asset from one person or entity to another. By tokenizing real estate assets as NFTs, ownership of the assets is recorded on the blockchain, making it a tamper-proof and secure record of ownership. When ownership is transferred, the NFT can be transferred to the new owner, representing the transfer of ownership of the real estate asset. The decentralized nature of blockchain technology ensures that the transfer of ownership is transparent and secure, with a clear and unalterable record of ownership available on the blockchain. This reduces the risk of fraud, counterfeiting, and other ownership disputes.

3) Trading of assets

The trading of assets refers to the buying and selling of real estate assets. By tokenizing real estate assets as NFTs, these assets can be bought and sold on blockchain platforms, much like stocks or other financial assets. The unique code of each NFT represents ownership of a specific real estate asset, making it possible to buy and sell these assets in a secure and transparent manner.

4) Investment opportunities

The use of NFTs (Non-Fungible Tokens) in real estate provides new investment opportunities for individuals and institutions looking to invest in real estate assets.
NFTs allow real estate assets to be tokenized and traded on blockchain platforms, making it possible to invest in smaller and more affordable portions of real estate assets. This opens up the market to a wider range of investors, including those who might not have previously been able to invest in real estate due to its high cost and barriers to entry.

Furthermore, the real-time asset management, transfer of ownership, and trading capabilities provided by NFTs make it easier for investors to manage their investments and quickly respond to market conditions, providing greater flexibility and control over their investments.

However, the adoption of NFTs in real estate is not without its challenges. Lack of understanding and education, difficulty in integrating NFTs with existing systems, and legal and regulatory considerations are some of the challenges that must be addressed for NFTs to be widely adopted in the real estate industry.

A) Adoption and understanding

One of the potential challenges with the adoption of NFTs in real estate is the general lack of understanding of the technology and its potential benefits. Many people, including investors, buyers, and sellers, may not be familiar with the concept of NFTs and how they can be used in real estate. This lack of understanding may result in a slower rate of adoption and limit the growth potential of the market.

B) Integration with existing systems

Integrating NFTs with existing systems, such as property registries, could pose a challenge. The process of updating these systems to accommodate NFTs may be time-consuming and require significant resources. In addition, there may be concerns about compatibility and interoperability with existing systems, as well as the need to establish new standards for NFTs in the Real Estate Industry.

C) Legal and regulatory considerations

Legal and regulatory considerations may be a potential challenge in the adoption of NFTs in real estate. Laws and regulations around NFTs and tokenization are still in their early stages and may vary across different jurisdictions. This can create uncertainty and make it difficult for stakeholders to understand their rights and responsibilities.
The outlook for NFTs in real estate is promising as the technology continues to evolve and mature. The adoption of NFTs in real estate is expected to grow as more people become aware of the benefits they offer, and the potential challenges are addressee

Department of IFORMATION & TECHNOLOGY technical magazine

The Rapid Rise of DeFi and its Impact on Traditional Financial Systems

With the introduction of decentralized finance, also known as DeFi, the world of money has undergone a paradigm shift. This new notion is upending existing financial systems by giving individuals greater control over their assets and upsetting the banking industry's established conventions. In this article, we will look at the rapid emergence of DeFi and its far-reaching implications for traditional financial institutions.

Decentralized Finance: A New Paradigm

DeFi is a decentralized financial ecosystem based on blockchain technology that eliminates the need for intermediaries such as banks, brokers, and insurance firms. It makes use of smart contracts, which are programmable agreements that execute themselves when certain criteria are satisfied, assuring transparency, security, and efficiency.

Unprecedented Adoption and Growth

DeFi has grown at an exponential rate since its establishment, drawing both retail and institutional investors. The total value locked (TVL) in DeFi protocols has risen to unprecedented heights. This expansion can be ascribed to a variety of factors, including increased cryptocurrency accessibility, the promise of large rewards, and the growing popularity of decentralized apps (dApps).

The Benefits of DeFi

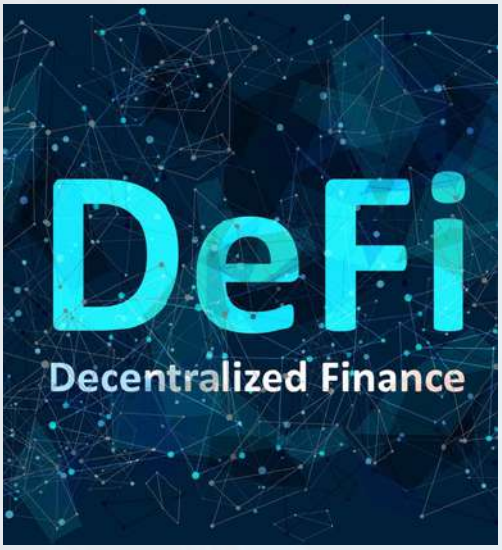
In comparison to traditional financial systems, DeFi has several notable advantages. For starters, it promotes financial inclusion by providing services to unbanked people who do not have access to regular banking services. Anyone with an internet connection can use DeFi to engage in financial activities like lending, borrowing, and investing without the requirement for a bank account. Second, DeFi eliminates the need for intermediaries, lowering transaction costs and enhancing transaction speed.

Traditional banking systems sometimes require many intermediaries, which causes delays, complexity, and extra fees. Transactions can be completed directly between parties via DeFi, which streamlines the process and saves both time and money. Furthermore, DeFi allows for increased transparency and security. All blockchain transactions are immutable and can be audited by anybody, assuring trust and accountability. Furthermore, the implementation of smart contracts reduces the risk of human error or manipulation, improving total f inancial transaction security.

Challenges and Threats

While DeFi has enormous potential, it is not without difficulties and risks. The lack of regulatory control is one of the major problems. Unlike traditional financial institutions, which are subject to stringent regulations, DeFi works in an unregulated environment. This legislative ambiguity complicates investor protection, anti-money laundering (AML) procedures, and market stability. Furthermore, the quick pace of DeFi innovation has resulted in the introduction of new and complicated financial products. While these products present exciting possibilities, they also pose hazards, such as smart contract flaws, hacking incidents, and market manipulation. Addressing these issues and implementing solid security measures will be critical to DeFi's long-term success as it evolves.

The Repercussions on Traditional Financial Systems



The rise of DeFi has serious consequences for existing banking institutions. It challenges centralized institutions' supremacy by providing alternative financial services that are more accessible, efficient, and transparent. As DeFi gets popularity, incumbent banks, payment processors, and other intermediaries may see less demand for their services. Furthermore, through spreading economic power, DeFi has the potential to democratize finance. Traditional financial systems are frequently centralized, with established organizations and affluent individuals benefiting. DeFi, on the other hand, ensures that all participants have equitable access to f inancial services and receive returns on their assets without relying on centralized gatekeepers.

Empowering Individuals

One of the key aspects of DeFi and Web3 is the empowerment of individuals. These technologies allow anyone with an internet connection to access financial services without relying on banks or other intermediaries. Users can borrow, lend, trade, and invest their assets directly from their digital wallets, eliminating the need for third-party approvals or lengthy bureaucratic processes. This level of f inancial inclusivity has the potential to revolutionize access to capital, particularly in underserved regions where traditional banking services are limited. Additionally, DeFi enables users to maintain ownership and control over their funds at all times. Unlike traditional financial systems, where custodial control is handed over to intermediaries, DeFi allows individuals to retain full custody of their assets. This means that users have the ultimate say in how their funds are used and can avoid potential risks associated with centralized custodianship, such as hacks, freezes, or mismanagement.

The Power Grab

As DeFi and Web3 gain mainstream adoption, they are challenging the entrenched power dynamics within the financial industry. Centralized institutions, such as banks, asset managers, and exchanges, have long held significant control over financial transactions, decision-making, and the overall direction of the economy. However, the rise of DeFi and Web3 is shifting this power to the individual level. By leveraging decentralized networks, blockchain technology, and cryptographic principles, DeFi and Web3 enable individuals to transact directly with each other, creating a peer-to-peer financial ecosystem. Smart contracts ensure transparency and automate trust, reducing the need for intermediaries and intermediation fees. This disintermediation is disrupting traditional business models and threatening the dominance of established institutions.

The Need for Institutional Adaptation

Institutions that fail to recognize the potential of DeFi and Web3 risk falling behind in a rapidly evolving landscape. While some traditional players have started exploring blockchain technology and tokenized assets, many are still grappling with the implications and potential disruptions. These institutions will need to adapt their business models, embrace innovation, and leverage the benefits of decentralization to stay relevant in the future. Collaboration between traditional institutions and the DeFi/Web3 ecosystem can foster innovation and bridge the gap between old and new financial paradigms. Institutions can learn from the transparency, efficiency, and inclusivity offered by DeFi, while DeFi projects can benefit from the expertise, regulatory compliance, and broader customer bases of established institutions. Synergies between these two worlds can lead to the development of hybrid models that combine the best of both centralized and decentralized systems.

Looking Forward

As DeFi grows in popularity, regulators, policymakers, and industry participants must work together to create a framework that combines innovation with investor protection and market stability. Regulatory certainty would not only reduce risks, but will also increase trust in DeFi, attracting additional players and capital. To summarize, decentralized finance is altering the financial environment as we know it. DeFi is positioned to alter how we interact, invest, and access financial services due to its various benefits and ability to disrupt established financial institutions. While problems and threats exist, DeFi's revolutionary power cannot be overlooked. As we negotiate this changing terrain, encouraging innovation and ensuring responsible growth will be critical to realizing decentralized finance's full potential.

Department of IFORMATION & TECHNOLOGY technical magazine

ZERO TRUST ARCHITECTURES: AN AWS PERSPECTIVE

By Mark Ryland and Quint Van Deman | on 23 NOV 2020 | In Foundational (100), Security, Identity, & Compliance | Permalink | Comments | Share

Our mission at Amazon Web Services (AWS) is to innovate on behalf of our customers so they have less and less work to do when building, deploying, and rapidly iterating on secure systems. From a security perspective, our customers seek answers to the ongoing question What are the optimal patterns to ensure the right level of confidentiality, integrity, and availability of my systems and data while increasing speed and agility? Increasingly, customers are asking specifically about how security architectural patterns that fall under the banner of Zero Trust architecture or Zero Trust networking might help answer this question. Given the surge in interest in technology that uses the Zero Trust label, as well as the variety of concepts and models that come under the Zero Trust umbrella, we'd like to provide our perspective. We'll share our definition and guiding principles for Zero Trust, and then explore the larger subdomains that have emerged under that banner. We'll also talk about how AWS has woven these principles into the fabric of the AWS cloud since its earliest days, as well as into many recent developments. Finally, we'll review how AWS can help you on your own Zero Trust journey, focusing on the underlying security objectives that matter most to our customers. Technological approaches rise and fall, but underlying security objectives tend to be relatively stable over time. (A good summary of some of those c

Definition and guiding principles for Zero Trust

Let's start out with a general definition. Zero Trust is a conceptual model and an associated set of mechanisms that focus on providing security controls around digital assets that do not solely or fundamentally depend on traditional network controls or network perimeters. The zero in Zero Trust fundamentally refers to diminishing—possibly to zero!—the trust historically created by an actor's location within a traditional network, whether we think of the actor as a person or a software component. In a Zero Trust world, network-centric trust models are augmented or replaced by other techniques—which we can describe generally as identity-centric controls—to provide equal or better security mechanisms than we had in place previously. Better security mechanisms should be understood broadly to include attributes such as greater usability and flexibility, even if the overall security posture remains the same. Let's consider more details and possible approaches along the two dimensions.

One dimension is the network. Do we achieve Zero Trust by allowing all network packets to flow between all hosts or endpoints, but implement all security controls above the network layer? Or do we break our systems down into smaller logical components and implement much tighter network segments or packet-level controls—so-called micro-segments or micro-perimeters? Do we add some kind of gateway or proxy technology that enforces a new kind of trust boundary? Do we still use VPN technology for network isolation but make it more dynamic and hidden from the user experience, so that users don't even notice that network boundaries are being created and torn down as needed? Or some combination of these techniques?

The other dimension is identity and access management. Are we talking about human actors with their PCs, tablets, and phones trying to access web applications? Or are we talking about machine to-machine, software-to-software communication, where all requests are authenticated and authorized using other kinds of techniques? Or perhaps we're thinking of some combination of the two. For example, certain security-relevant properties or attributes of the user's situation—strength of authentication, device type, ownership, posture assessment, health, network location, and others—are propagated to and through the software systems with which the user is interacting, and alter their access dynamically.

Thus, as we start to look more closely at Zero Trust, we can immediately see the possibility of confusion—because many different topics and concepts are implicated—but also a clear indication of opportunities to build better, more flexible, and more secure software systems. What are some of the principles that can help guide us through both the confusion and the opportunities? Our first guiding principle for Zero Trust is that while the conceptual model decreases reliance on network location, the role of network controls and perimeters remains important to the overall security architecture. In other words, the best security doesn't come from making a binary choice between identity-centric and network-centric tools, but rather by using both effectively in combination with each other. Identity-centric controls, such as the AWS SigV4 request signing process, which is used to interact with AWS API endpoints, uniquely authenticate and authorize each and every signed API request, and provide very fine-grained access controls. However, network centric tools such as Amazon Virtual Private Cloud (Amazon VPC), security groups, AWS PrivateLink, and VPC endpoints are straightforward to understand and use, filter unnecessary noise out of the system, and provide excellent guardrails within which identity-centric controls can operate. Ideally, these two kinds of controls should not only coexist, they should be aware of and augment one another. For example, VPC endpoints provide the ability to attach a policy that allows you to write and enforce identity-centric rules at a logical network boundary—in that case, the private network exit from your Amazon VPC on the way to a nearby AWS service endpoint.

Our second guiding principle for Zero Trust is that it can mean different things in different contexts. Arguably one of the key reasons for the ambiguity surrounding Zero Trust is that the term encompasses many different use cases which share only the fundamental technical concept of diminishing the security relevance of a network location or boundary. Yet those use cases differ substantially in what they're trying to achieve for the organization. As we noted above, common examples of Zero Trust goals range from ensuring workforce agility and mobility

—using browsers and mobile apps and the internet to access business systems and applications—to the creation of carefully segmented micro-service architectures inside of new cloud-based applications. By focusing on a specific problem that we're trying to solve, and approaching it with fresh eyes and new tools, we can avoid getting mired in low-value discussions around whether a new approach to a security challenge is really—or to what degree it is—an application of the Zero Trust concept.

Our third guiding principle is that Zero Trust concepts must be applied in accordance with the organizational value of the system and data being protected. Over time, the application of the Zero Trust conceptual model and associated mechanisms will continue to improve defense in depth, and continue to make security controls we already have work better through the increased visibility and software-defined nature of the cloud. Applied well, the tenets of Zero Trust can significantly raise the security bar, especially for critical workloads. However, if applied in strict orthodoxy, Zero Trust methods can limit the incorporation of more traditional technologies into upgraded or new systems, and stifle innovation by overly taxing organizations where the benefits aren't commensurate with the effort. For many business systems, network controls and network perimeters will continue to be important and usually adequate controls for a long time, perhaps forever. We believe it's best to think of Zero Trust concepts as additive to existing security controls and concepts, rather than as replacements.

Examples of Zero Trust principles and capabilities at work today within the AWS cloud

The most prominent example of Zero Trust in AWS is how millions of customers typically interact with AWS every day using the AWS Management Console or securely calling AWS APIs over a diverse set of public and private networks. Whether called via the console, the AWS Command Line Interface (AWS CLI), or software written to the AWS APIs, ultimately all of these methods of interaction reach a set of web services with endpoints that are reachable from the internet. There is absolutely nothing about the security of the AWS API infrastructure that depends on network reachability. Each one of these signed API requests is authenticated and authorized every single time at rates of millions upon millions of requests per second globally. Our customers do so confidently; knowing that the cryptographic strength of the underlying Transport Layer Security (TLS) protocol—augmented by the AWS Signature v4 signing process—properly secures these requests without any regard to the trustworthiness of the underlying network. Interestingly, the use of cloud-based APIs is rarely—if ever—mentioned in Zero Trust discussions. Perhaps this is because AWS led the way with this approach to securing APIs from the start, such that it is now assumed to be a basic part of every cloud security story.

Similarly, but perhaps not as well understood, when individual AWS services need to call each other to operate and deliver their service capabilities, they rely on the same mechanisms that you use as a customer. You can see this in action in the form of service-linked roles. For example, when AWS Auto Scaling determines that it needs to call the Amazon Elastic Compute Cloud (Amazon EC2) API to create or terminate an EC2 instance in your account, the AWS Auto Scaling service assumes the service-linked role you've provided in your account, receives the resulting AWS short-term credentials, and uses these credentials to sign requests using the SigV4 process to the appropriate EC2 APIs. On the receiving end, AWS Identity and Access Management (IAM) authenticates and authorizes the incoming calls for EC2. In other words, even though they're both AWS services, AWS Auto Scaling and EC2 have no inherent trust, network or otherwise, of one another and use strong identity-centric controls as the basis of the security model between the two services as they operate on your behalf. You, the customer, have full visibility into both the privileges that you're granting to one service, as well as an AWS CloudTrail record of the use of those privileges. Other great examples of Zero Trust capabilities in the AWS portfolio can be found in the IoT Service. When we launched AWS IoT Core we made a strategic decision—against the prevailing industry norms at the time—to always require TLS network encryption and modern client authentication, including certificate-based mutual TLS, when connecting IoT devices to service endpoints.

We subsequently added TLS support to FreeRTOS, enabling modern, secure communication to an entire class of small CPU and small memory devices that were previously assumed to not be capable of it. With AWS IoT Greengrass, we pioneered a way of working with existing no-security devices using a remote gateway that relied on local network presence but also was able to run AWS Lambda functions to validate security and provide a secure proxy to the cloud. These examples highlight where adherence to AWS security standards brought key foundational components of Zero Trust to a technology domain where vast amounts of unauthenticated, unencrypted network messaging over the open internet was previously the norm.

How AWS can help you on your Zero Trust journey

To help you on your own Zero Trust journey, there are a number of AWS cloud-specific identity and networking capabilities that provide core Zero Trust building blocks as standard features. AWS services provide this functionality via simple API calls, without you needing to build, maintain, or operate any infrastructure or additional software

To help best frame the conversation, we'll consider these capabilities against the backdrop of three distinct use cases:

- Authorizing specific flows between components to eliminate unneeded lateral network mobility.
- Enabling friction-free access to internal applications for your workforce.
- Securing digital transformation projects such as IoT.

Our first use case focuses mainly on machine-to- machine communications—authorizing specific f lows between components to help eliminate lateral network mobility risk. Otherwise put, if two components don't need to talk to one another across the network, they shouldn't be able to, even if these systems happen to exist within the same network or network segment. This greatly reduces the overall surface area of the connected systems and eliminates unneeded pathways, particularly those that lead to sensitive data. Within this use case, our discussion should begin with security groups, which have been a part of Amazon EC2 since its earliest days.
Security groups provide highly dynamic, software-defined network micro-perimeters for both north-south and east-west traffic. Security group assignments occur automatically as resources come and go, and rules in one security group can reference one another by ID, either within the same Amazon VPC or across larger peered networks in the same or different regions. These properties allow security groups to act as a kind of identity system in which group membership becomes a relevant property for determining whether or not to permit particular network flows. This helps enable you to author extremely granular rules without the associated operational burden of keeping them up-to-date as membership in a group ebbs and flows. Similarly, PrivateLink provides an extremely useful building block in the general space of micro-perimeters and micro-segmentation. Using PrivateLink, a load-balanced endpoint can be exposed as a narrow, one-way gateway between two VPCs, with tight identity-based controls determining who can access the gateway and where incoming packets can land. Initiating network connections in the other direction isn't allowed at all, and the VPCs don't even need to have routes between one another. Thousands of customers use PrivateLink today as a fundamental building block of a secure micro-services architecture, as well as secure and private access to PaaS and SaaS services from their suppliers.
Going back to our discussion about AWS APIs, the AWS SigV4 signature process for authenticating and authorizing API requests is no longer just for AWS services.

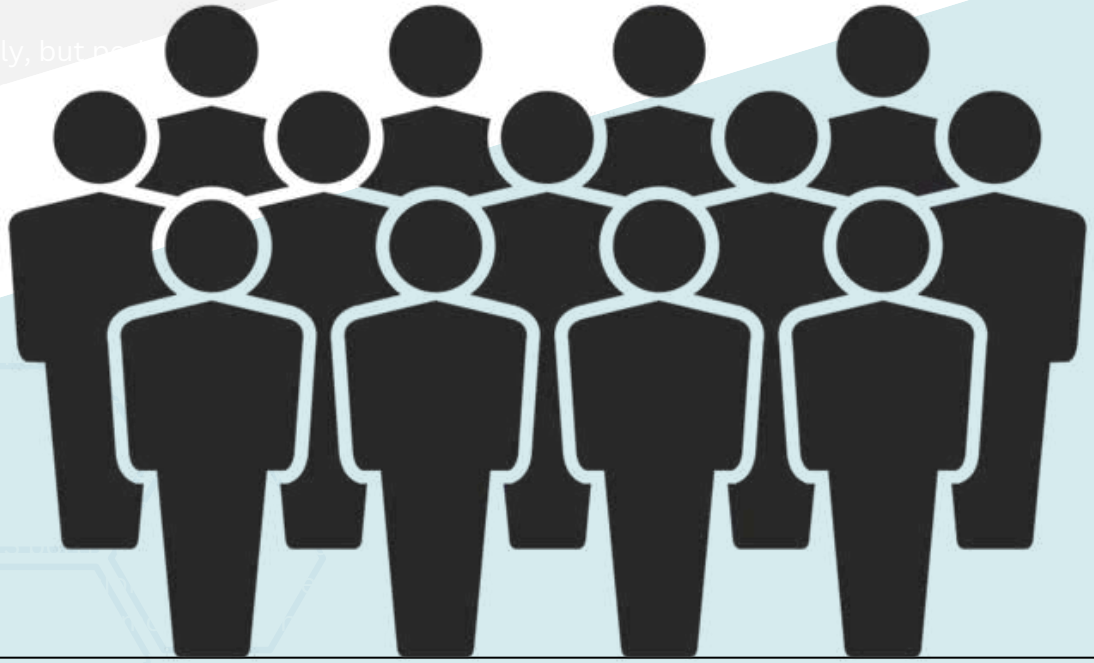
You can achieve the same kind of hardened interface approach using the Amazon API Gateway service, which allows software interfaces to be securely available on the open internet. API Gateway provides distributed denial of service (DDoS) protection, rate limiting, and AWS IAM support as one of several authorization options. When you choose AWS IAM authorization, you author standard IAM policies that define who can call your API and where they can call it from, using the full expressiveness of the IAM policy language.

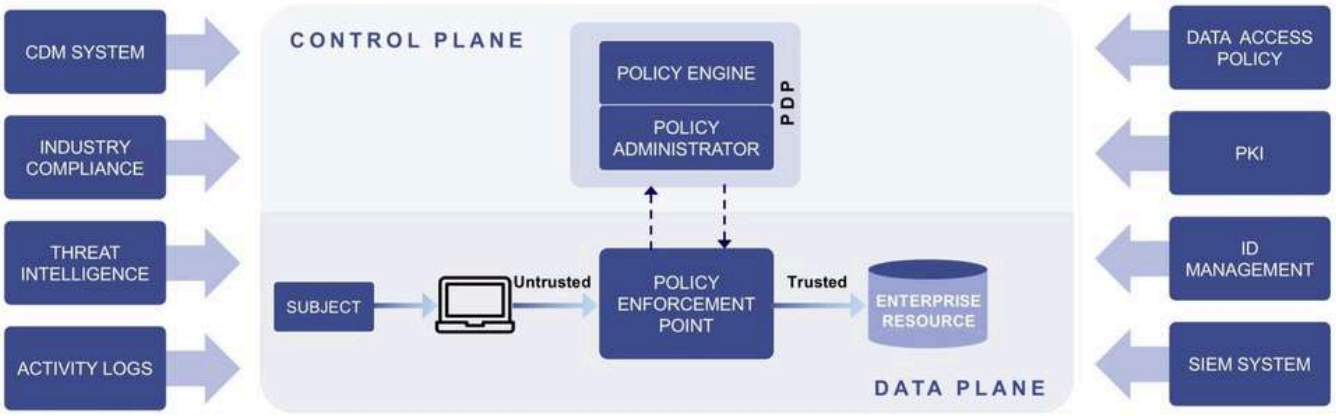
Callers sign their requests using their AWS credentials, typically delivered in the form of IAM roles attached to compute resources, and IAM uniquely authenticates and authorizes every single call to your API according to those policies. With one step, your API is protected behind the massively scaled, super performant, globally available IAM service that protects AWS APIs—with nothing for you to manage or maintain. Calls from the API Gateway front-end to your back-end implementation are secured by mutual TLS, so you're assured that only API Gateway is able to invoke the back-end implementation. With this strong identity-centric control in place, you have two choices.

You can safely place your back-end implementation on the public network, or add the VPC integration model such that the API Gateway call to your back-end implementation running inside of your VPC is protected by an identity-centric control (mutual TLS) and a network-centric control (private connectivity from API Gateway to your code). The security achieved by these feature combinations, arguably only possible in the cloud, makes discussions of east-west concerns seem underwhelming and rooted in constraints of the past.

Our second use case, enabling friction-free access to internal applications for your workforce, is all about improving workforce mobility without compromising security. Traditionally these applications have existed behind a strong VPN front door. However, VPNs can be expensive to scale and aren't necessarily compatible with the full array of mobile devices that the modern workforce demands. The objective in this case is to make the locks on the individual applications so good that you can eliminate the VPN-based front door. To achieve this, our customers have told us that they want a range of technical solutions to choose from according to their industry, risk tolerance, developer maturity, and other factors. At one end of the spectrum, we have many customers who prefer to use desktop as a service—Amazon Workspaces—or application as a service—Amazon AppStream 2.0—models to provide a powerful and flexible pixel proxy approach to Zero Trust. Traditional security controls are applied to those intermediary virtual devices, and then any user with a PC, tablet, or HTML5 client can reach those virtualized desktops or applications over the internet—or behind additional network controls and perimeters, if they so desire—to provide a rich, desktop-like experience without having to worry about the security of the final device in the hands of the user.

Similarly, customers have asked for a better way to access their enterprise applications securely from mobile phones without deploying mobile device management or other such often cumbersome and expensive technologies. To meet that requirement, we launched Amazon WorkLink, providing a secure proxy service that renders complex web applications in the AWS cloud. Amazon WorkLink streams only pixels—and a very minimal amount of JavaScript for interactivity—to mobile phones. No sensitive enterprise data is ever stored or cached on the mobile device At the other end of the spectrum, we have customers who want to connect their internal web applications directly to the internet. For these customers, the combination of AWS Shield, AWS WAF, and Application Load Balancer with OpenID Connect (OIDC) authentication provides a fully managed identity-aware network protection stack. Shield provides managed DDoS protection services that provide always-on detection and automatic inline mitigations that minimize application downtime and latency. AWS WAF is a web application firewall that lets you monitor and protect web requests before they reach your infrastructure using your desired combination of rule groups provided by AWS, the AWS Marketplace, or your own custom ones. By enabling authentication in Application Load Balancer—beyond the normal load balancing capabilities—you can directly integrate with your existing identity provider (IdP) to offload the work of authenticating users, and to leverage the existing capabilities within your IdP—such as strong authentication, device posture assessment, conditional access, and policy enforcement. Using this combination, your internal custom applications quickly become just as flexible as SaaS applications, allowing your workforce to enjoy the same work-anywhere flexibility as SaaS while unifying your application portfolio under a common security model powered by modern identity standards.





Our third use case—securing digital transformation projects such as IoT—is markedly different from the first two. Consider a connected vehicle, relaying a critical stream of instrumentation over mobile networks and the internet into a cloud based analytics environment for processing and insights. These workloads have always existed entirely outside the traditional enterprise network, and require a security model that accounts for that situation. The family of AWS IoT services provides scalable solutions for issuing unique device identities to every device in your fleet, and then using those identities and their associated access control policies to securely control how they communicate and interact with the cloud.

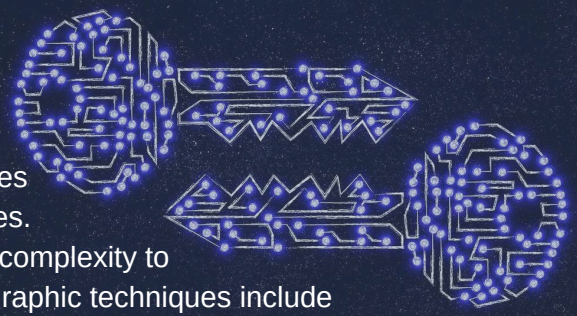
The security of these devices can be easily monitored and maintained with AWS IoT Device Defender, over-the-air software updates, and even entire operating system upgrades—now built in to FreeRTOS—to keep devices safe and secure over time. Moving forward, as more and more IT workloads move closer to the edge to minimize latency and improve user experiences, the prevalence of this use case will continue to expand, even if it isn't applicable to your business today

Department of IFORMATION & TECHNOLOGY technical magazine

Post-Quantum Cryptography: The Future of Secure Communication Amid Rise of Quantum Computing

Cryptography plays a vital role in secure communication, using mathematical computations to encode and decode messages. Classical cryptographic techniques, such as the RSA and AES algorithms, face threats from advancements in computing power, particularly quantum computers. Post-Quantum Cryptography (PQC) is a modern approach designed to withstand attacks from both classical and quantum computers. The development of PQC is crucial for maintaining long-term security of sensitive information. The history of cryptography includes the development of the Data Encryption Standard (DES), the Diffie Hellman key exchange, and the Advanced Encryption Standard (AES). Mathematics, particularly one way functions, play a crucial role in cryptography, as do digital signatures.

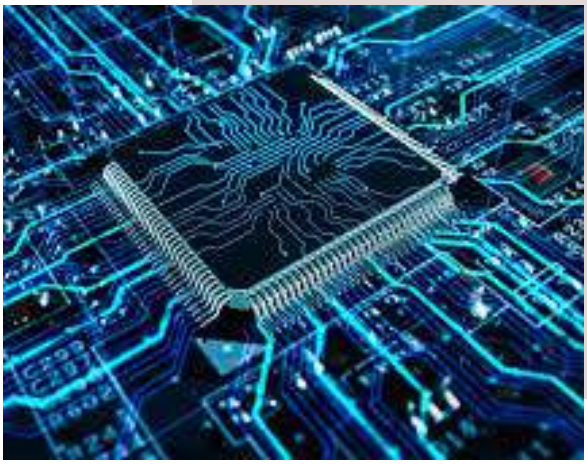
What is the Role of Cryptography in Secure Communication?



Cryptography is a critical component in ensuring the security of sensitive information and facilitating secure communication. Classical cryptography, which has been used for centuries, relies on mathematical computations to encode and decode messages. This method uses mathematical algorithms and computational complexity to secure communication and data. Examples of classical cryptographic techniques include substitution ciphers like the Caesar cipher and transposition ciphers like the Rail Fence cipher. These techniques typically use keys to encrypt and decrypt messages, with the security often dependent on the confidentiality of the key. Notable classical cryptographic algorithms include the RSA algorithm for public-key encryption, the AES algorithm for symmetric-key encryption, and the Diffie-Hellman key exchange protocol. However, classical cryptography faces potential threats from advancements in computing power and the development of new mathematical techniques. In particular, the rise of quantum computers, which are capable of compromising many existing cryptographic schemes such as RSA and ECC, poses a significant challenge.

How Does Post-Quantum Cryptography Compare to Classical Cryptography?

Post-Quantum Cryptography (PQC) is a modern cryptographic approach designed to withstand attacks from both classical and quantum computers. The goal of PQC is to create cryptographic algorithms that remain resilient even in the face of powerful quantum computers. PQC algorithms typically stem from mathematical problems that are difficult for both classical and quantum computers to solve. Examples include lattice-based cryptography, code-based cryptography, hash based cryptography, and multivariate polynomial cryptography. The development of PQC is crucial for maintaining the long-term security of sensitive information in an era expected to see the rise of quantum computers. Efforts are currently underway to standardize PQC algorithms to ensure widespread adoption and compatibility across various systems and applications. As interdisciplinary collaborations progress, the aim is to establish new cryptographic standards that ensure the enduring security of information in the post-quantum era.



In the early 1970s, IBM established a crypto group that developed a block cipher to protect its clients' data. In 1973, the United States adopted it as a national standard, known as the Data Encryption Standard (DES), which remained in use until its vulnerability was exposed in 1997. In 1976, Whitfield Diffie and Martin Hellman introduced the concept of the Diffie-Hellman key exchange, revolutionizing cryptography by dynamically generating a pair of keys for each correspondence, eliminating the need for prearranged code keys.

Quantum cryptography was initially proposed in 1984 by Bennett and Brassard. In 2000, the Advanced Encryption Standard (AES) superseded DES, providing enhanced security. AES employs symmetric-key encryption, requiring both the user and sender to possess the same secret key. In 2005, Elliptic Curve Cryptography (ECC) emerged as an advanced public-key cryptography scheme, enabling shorter encryption keys and offering heightened security compared to RSA and Diffie Hellman.

How Does Post-Quantum Cryptography Compare to Classical Cryptography?

Mathematics plays a crucial role in cryptography. One-way functions in cryptography serve as a fundamental tool, offering a mathematical process that is easy to execute in one direction but extremely difficult to reverse. When provided with an input, it's straightforward to calculate the corresponding output. However, when presented with the output alone, it becomes computationally impractical, if not impossible, to discern the original input without access to specific knowledge or additional data. One-way hash functions play a pivotal role in cryptography, serving various purposes such as securely storing passwords, generating message digests for data integrity verification, and deriving cryptographic keys. Certain one-way functions possess a unique property known as a trapdoor, enabling efficient computation of the inverse under specific conditions. These trapdoor functions are integral to asymmetric encryption schemes like RSA and Diffie-Hellman key exchange, facilitating secure communication and key establishment over insecure channels.

What is the Role of Digital Signatures in Cryptography?

In digital signature algorithms, one-way functions are utilized to generate and verify signatures, thereby ensuring the authenticity and integrity of digital documents. By applying one-way functions to the message along with a private key, a digital signature is generated. This process ensures that the message has not been tampered with during transmission, providing a layer of security and trust in digital communications. Digital signatures are a critical component of modern cryptography, providing a means to verify the authenticity of digital messages and documents.

Department of IFORMATION & TECHNOLOGY technical magazine

ADVANCEMENTS IN HUMANOID ROBOTS

HUMANOID robots are meticulously designed machines that closely imitate human appearance and behaviour, proficiently replicating functions such as perception, decision-making, and interaction. Inspired by human intelligence and adaptability, these robots have made significant advancements that surpass previous limits. The primary goal is to create humanoid robots capable of ongoing learning and adaptation in unstructured and dynamic environments, ultimately benefiting individuals and propelling the advancement of humanity.

Humanoid robots possess distinct advantages compared to other robot forms. Their human-like design, encompassing torso, arms, and legs, enhances their adaptability to human-centric environments, fostering societal acceptance and enabling complex interactions. This anthropomorphic design facilitates natural human interaction, making them valuable for fields like healthcare and education. Bipedal mobility allows humanoid robots to navigate human spaces efficiently, while their advanced manipulation and dexterity make them capable of intricate tasks. Their cognitive abilities enhance autonomy and adaptability. Moreover, their human safety features, social acceptance, and adaptability to human environments contribute to their suitability for collaborative roles. Despite these advantages, challenges such as balance and energy efficiency persist, making continued research crucial for unlocking their full potential across various domains.

Humanoid robotics, an interdisciplinary field encompassing mechanics, electronics, computer science, artificial intelligence, sensing, and actuation, stands at the forefront of scientific and technological research. Through progressive research, our comprehension of the structural and functional aspects of humanoid robots has significantly advanced.

Department of IFORMATION & TECHNOLOGY technical magazine

Advancements in Humanoid Robots

Pioneering breakthroughs in biomimetic structures, materials, biological information perception, and brain-inspired intelligent control have yielded remarkable experimental applications, showcasing the vast potential of humanoid robots. Nevertheless, a notable disparity remains between the current functional capabilities of humanoid robots and the intricate capacities exhibited by humans Furthermore, humanoid robots serve as prominent symbols of a nation's technological capabilities and innovative prowess, owing to the intricate mechanical and electronic components they embody. Significant progress has been made in enabling these robots to navigate bipedally in diverse environments, demonstrating their adaptability and versatility. The design and control processes of humanoid robots have received significant attention, leading to rapid advancements in motion planning, robot vision, and behavioural control through the implementation of learning algorithms. However, achieving highly intelligent and versatile humanoid robots remains a formidable challenge in the fields of robotics and artificial intelligence. Unleashing their full potential requires further

breakthroughs in both hardware and software domains. Despite persistent challenges, humanoid robots hold extensive potential for applications across various domains of human life, including military operations, industry, rescue missions, healthcare, education, assistance, entertainment, and agriculture. Their widespread utilization drives the development of next-generation industries and expands the scope of robotic applications, encompassing areas such as national defense, intelligent manufacturing, and social services. Looking ahead, humanoid robots are poised to assume a prominent role in daily life applications, emerging as one of the most significant forms of intelligent robots. Humanoid robots have reached the apex of technological innovation, propelling the advancement and evolution of next-generation industries. This comprehensive paper provides an in-depth review of the current status, advancements, and future prospects of humanoid robots, encompassing key technologies and research endeavors. By addressing emerging challenges and emphasizing the integration of bionics, brain-inspired intelligence, mechanics, and control, the paper serves as a valuable resource for researchers and practitioners. It contributes to the continuous evolution and potential of humanoid robots in diverse domains, fostering interdisciplinary integration and propelling advancements in various fields such as bionics, artificial intelligence, computer science, and material science. Ultimately, this review informs future development and planning, promoting the integration of disciplines for the next generation of humanoid robotic systems.

The Metaverse: Myths and Facts

Any new technology involves a certain amount of ambiguity and myths. In the case of the Metaverse, however, many of the myths have been exaggerated and facts were misrepresented, while the Metaverse vision will take years to mature fully, the building blocks to begin this process are already in place. Key hardware and software are either available today or under development; and definitely stakeholders need to address Safety, Security and Privacy (SSP) concerns, and collaborate to implement open standards that will make the Metaverse safe, secure, reliable and interoperable, and allow the delivery of secured and safe services as seamlessly as possible. Despite the buzz about the Metaverse, many still don't completely understand it. For some, it is the future, while others think it is gimmicky. For now, the Metaverse is an interface or a platform that allows digital realities of people to come together to work, play and collaborate. Metaverse hopes to transcend geographical boundaries and become the next 'thing'. Since then, various developments have made milestones on the way toward a real Metaverse, an online virtual world which incorporates augmented reality (AR), virtual reality (VR), 3D holographic avatars, video and other means of communication.

The Metaverse, an online virtual world which incorporates augmented reality (AR), virtual reality (VR), 3D holographic avatars, video and other means of communication.

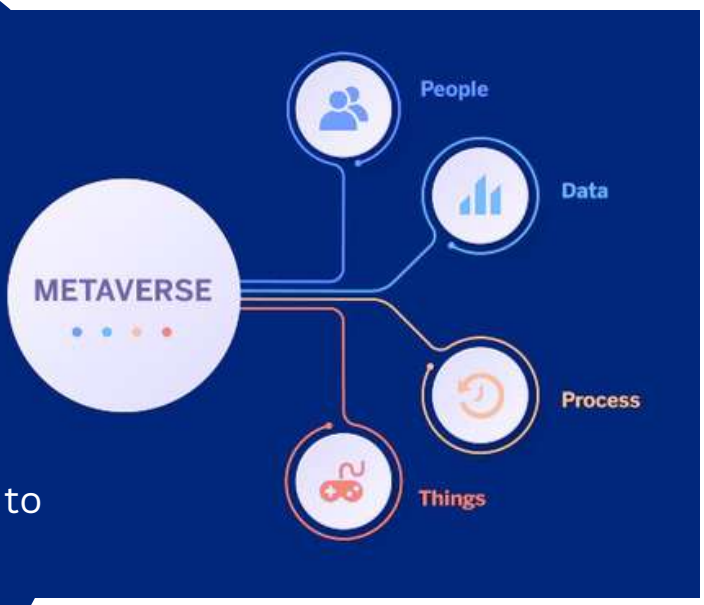
As the Metaverse expands, it will offer a hyper real alternative world or what Comic fans call parallel universe. But this description is like talking about "Frontend "in apps development only without explaining "Backend" side of the apps, to understand that side of this new X-verse we need to look at Metaverse from a different perspective.

DIFFERENT PERSPECTIVE OF THE METAVERSE

The Metaverse" is bringing together people, process, data, and things (real and virtual) to make networked connections more relevant and valuable than ever before-turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries". In simple terms: Metaverse is the intelligent connection of people, process, data and things. The Metaverse describes a world where billions of objects have sensors to detect measure and assess their status; all connected over public or private networks using standard and proprietary protocols.

PILLARS OF THE METAVERSE

- People: Connecting people in more relevant, valuable ways
- Data: Converting data into intelligence to make better decisions
- Process: Delivering the right information to the right person (or machine) at the right time
- Things: Physical and virtual devices and objects connected to the Internet and each other for intelligent decision making.



CHALLENGES FACING THE METAVERSE

No new technologies or concepts without challenges, and the Metaverse is no exception:

- Identity Management: it's difficult to confirm ID in current Web 2.0 apps, with Metaverse the problem is scaled up as we expand the use of the products and services, the last thing you want is to create a wild west in Metaverse.
- Security, Safety, and Privacy (SSP): As devices/people get more connected and collect more data resulting in accelerating the Metaverse expansion at a speed close to the speed of the real universe, privacy, safety and security concerns will increase too. How companies decide to balance customer SSP with this wealth of Metaverse data will be critical for the future of the Metaverse and more important customers' trust of the Metaverse and any future X-verse versions.
- Finance in Metaverse: using cryptocurrency is a challenge by itself, using it as a way of payment in Metaverse will add more complications to what is still unregulated payment system, one of the options to overcome this is to consider CBDC (Central Bank Digital Currency)
- Laws, regulations, and protections: new world and new territory for the law to explore and define the responsible parties and create new regulations to protect everyone using Metaverse including Intellectual Properties with the new found businesses like NFTs
- The emotional and mental impact of living in Metaverse: the same issues of non-stop social media usage and online gaming will transfer to the Metaverse on a large scale with another dimension added with near real-time interactions, this could create a lot of mental issues in the real world, and the line between real and imaginary world will be blurred with actions and words used in both worlds.
- Standardization of the Metaverse: this is usually one of the toughest parts in the early lifecycle of any new technology as everyone wants to be the "standard" and dominate the market, standards will cover all hardware/software, process, protocols and make interoperability fundamental to the design and implementation of the Metaverse.

THE FUTURE?

Data is embedded in everything we do; every business needs its own flavor of data strategy which requires a comprehensive data leadership. The Metaverse will create tens of millions of new objects and sensors, all generating real-time data which will add more value to their products and services for all the companies who will use Metaverse as another avenue of business. Enterprises will make extensive use of Metaverse technology, and there will be a wide range of products sold into various markets vertical and horizontal, an endless list of products and services.

For example: In E-commerce the Metaverse provides a whole new revenue stream for digital goods in a synchronous way instead of the current traditional 2D way of click and buy. In human resources (HR) significant training resources will be done with virtual reality (VR) and augmented reality (AR) that are overlaying instructions in a real-world environment and giving somebody a step-by-step playbook on how to put complex machine together or run a device or try a new product all will be done with virtual objects at the heart of the Metaverse. While in sales/marketing, connecting with customers virtually and sharing virtual experience of the product or service will be common similar to our virtual meetings during the past two years in the middle of Covid but the Metaverse will make it more real and more productive. Crypto products including NFTs will be the natives of the Metaverse adding another block to Web 3.0 puzzle.The pandemic forced us to be more online and accept many actions to be virtual which was like a preview for the Metaverse in 2D, the real Metaverse is 3D with time as the 4th dimension, but in the Metaverse we control time and space because we crate both in the Metaverse.