



TECHLORE

“Insider Tips to Make Your Business Run Faster, Easier and More Profitable”

INSIDE THIS ISSUE:

Real-Time Demand Forecasting with AI Algorithms	Page 1	DeepFakes: The Good, The Bad and the AI	Page 2
Gadget of the Month	Page 1	Tip of the Month	Page 2
Ethical Guidelines for AI Development and Deployment	Page 2	What is 2FA?	Page 2
		Call to Action	Page 2



"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"
 -Ruben Diaz
 NeoLore Networks

Real-Time Demand Forecasting with AI Algorithms

Staying ahead of the competition requires more than just guesswork when it comes to predicting customer demand. Fortunately, artificial intelligence (AI) algorithms have revolutionized the way businesses can forecast demand in real-time.

Why Real-Time Demand Forecasting Matters?

Effective demand forecasting is crucial for businesses across various industries, from retail to manufacturing. It helps companies optimize their inventory levels, reduce costs, and improve customer satisfaction. But why is real-time forecasting so essential?

Rapid Market Changes – Markets are constantly evolving, and consumer preferences can change in the blink of an eye. Traditional forecasting methods often rely on historical data, which may not reflect current market conditions.

Supply Chain Optimization – Real-time forecasting allows businesses to adjust their supply chains dynamically. This agility can help avoid stock outs or overstock situations, reducing waste and increasing profitability.

Customer Satisfaction – Meeting customer demand is paramount. Real-time forecasting helps ensure products are available when customers want them, enhancing their satisfaction and loyalty.

AI Algorithms for Real-Time Demand Forecasting – AI algorithms have made it possible to analyze vast amounts of data quickly and accurately. Here are some ways AI is transforming real-time demand forecasting:

Machine Learning Models – Machine learning algorithms, such as neural networks and decision trees, can analyze historical and real-time data to predict future demand. These models adapt as new data becomes available, increasing accuracy over time.

Big Data Analysis – AI can handle enormous datasets, incorporating factors like social media trends, weather forecasts, and economic indicators. This comprehensive data analysis provides a more holistic view of demand drivers.

Predictive Analytics – AI-driven predictive analytics can forecast demand at different levels, from individual product SKUs to product categories, regions, or even customer segments. This granularity allows businesses to tailor their strategies accordingly.

Real-Time Updates – AI algorithms can provide real-time updates on demand forecasts, ensuring that businesses can make timely decisions to adjust production or replenish inventory.

Benefits of AI-Powered Real-Time Demand Forecasting

AI models continuously learn from data, leading to more accurate predictions compared to static, rule-based methods.

By optimizing inventory levels and reducing waste, businesses can lower their operational costs and improve profitability.

Meeting customer demand promptly increases satisfaction and fosters loyalty.

Businesses that can respond quickly to market changes gain a competitive edge over those using traditional forecasting methods.

Challenges and Considerations

While AI algorithms offer significant advantages, there are some challenges and considerations to keep in mind:

Accurate forecasting relies on high-quality data. Garbage in, garbage out – if the input data is flawed, the forecasts will be too.

Some AI models can be complex and challenging to interpret. It's important to strike a balance between accuracy and model transparency.

Deploying AI systems can be expensive, and businesses need to weigh the costs against the benefits.



Logitech Lift

Raise your hand into comfort. Realign into a more natural posture. And relax into focus, all day long with Lift Vertical Ergonomic Mouse — a great fit for small to medium hands, with a left-handed option available too.

Designed, developed, and tested in The Logi Ergo Lab, and with the stamp of approval from leading ergonomic institutions, you can rest assured Lift means business when it comes to your wellbeing in the workspace. Get yours at www.logitech.com

Ethical Guidelines for AI Development and Deployment

AI developers and organizations must maintain comprehensive documentation detailing the development process, algorithms, and data sources used in their AI systems. This documentation should be made available to relevant stakeholders to promote transparency and accountability.

Accountability for Outcomes –

Developers and organizations should accept responsibility for the outcomes and consequences of their AI systems. When AI systems make errors or exhibit bias, they must take corrective actions and learn from these mistakes to improve future iterations.

Fairness Assessment – Before deployment, AI systems should undergo rigorous fairness assessments to identify and rectify biases in their training data and

algorithms. Developers should use diverse and representative datasets to minimize biased outcomes.

Continuous Monitoring – AI systems should be continuously monitored for bias during deployment. If unfair outcomes are detected, developers should implement corrective measures promptly and transparently.

Redress Mechanisms – Developers should establish mechanisms for individuals to report and seek redress for instances of bias or discrimination caused by AI systems. These mechanisms should be accessible and responsive to user concerns.

Privacy and Data Protection – AI developers must adhere to the principle of data minimization, collecting only the data necessary

for the intended purpose and ensuring its protection throughout the data lifecycle.

Users must be provided with clear and understandable information about how their data will be used by AI systems, and they should have the option to give informed consent before data collection or processing. AI developers should employ state-of-the-art security measures to protect user data from unauthorized access or breaches. Data encryption and secure storage practices should be implemented.

Robustness and Safety – AI systems must undergo extensive testing and validation to ensure they operate reliably and safely in real-world scenarios. Developers should account for possible failure modes and put safeguards in

place. Developers must design AI systems with fail-safe mechanisms that can prevent or mitigate adverse consequences in the event of system failures or unexpected behavior. Ethical considerations should be integrated into the design phase of AI systems to proactively identify and address potential ethical dilemmas, rather than relying solely on post hoc measures.

Human-Centric Design – AI systems should prioritize the well-being and needs of users, aiming to enhance human capabilities and decision-making rather than replacing or compromising them. In critical applications, such as healthcare and autonomous vehicles, AI should include mechanisms for human oversight to ensure responsible decision-making and accountability.

DeepFakes: The Good, The Bad and the AI

Deepfakes, those videos where a computer-generated face replaces the original, are both fascinating and potentially troubling.

The Good – Benefits of Deepfake Technology

Cost-Effective Video Campaigns: Deepfake technology has the potential to significantly lower the cost of creating engaging video campaigns, providing a more budget-friendly avenue for marketers.

Enhanced Omnichannel Campaigns: Marketers can leverage deepfake technology to create more impactful omnichannel campaigns, delivering a consistent and compelling message across various platforms.

Hyper-Personalization: Deepfakes enable the creation of hyper-personalized content, offering customers a unique and tailored experience that goes beyond traditional marketing approaches.

The Bad – Threats Posed by Deepfakes

False Statements and Announcements: Deepfake manipulation can lead to the creation of videos featuring individuals making false statements or announcements. This poses a significant risk, especially when it involves high-profile figures or corporate leaders.

Blackmail and Reputation Damage: Cyber attackers could use deepfakes to blackmail companies by threatening to release fabricated videos to the media or on social platforms. This has the potential to damage reputations and create chaos.

What You Can Do With Google Slides

If presentations are part of your job description, Google Slides is a free program that's included with Google Drive. With hundreds of different fonts and templates to choose from, you can create presentations that look professional and personalized. Add animation and embedded video to add even more unique content to your slides. When complete, you'll be able to access your presentation from wherever you are and through any device, including your PC, tablet, or phone. You can also share Google Slides with anyone, giving them rights to view, edit, or comment.

Google Slides also works with PowerPoint. Open and edit PowerPoint presentations using the app or Chrome extension. Then convert the files to Google Slides – and you can also convert Google Slides to PowerPoint, eliminating the need to worry about different file formats.

Insert Content Into Microsoft OneNote

Most of aren't taking advantage of Microsoft's OneNote when it comes to smart content. Use the Insert tab on the ribbon to insert content to make OneNote the flexible app it's meant to be:

- Add file attachments that can be opened directly in OneNote.
- Attach or capture recorded audio and video from meetings.
- Include and attach spreadsheets and tables to detailed notes.
- Add time and date stamps to organize information when sharing OneNote with other team members.
- Add and organize your tasks by assigning tags to each item on your to-do list.
- Customize the look of OneNote pages with page color, size, and layout.

What is 2FA?

Two-factor authentication (2FA for short) is a system in which you must verify your identity in two separate ways to access an account. Sound confusing? It's not. Here's an example:

After enabling 2FA on a Gmail account, you have to enter your password each time you log in. Then you are asked to enter a six-digit code that you pull from your phone, a jump-drive-sized key fob or a program on your computer.

Only then do you have access to your account. That way, if someone steals your password, they still can't

get in. If you aren't currently using two-factor authentication with your most sensitive data and systems, look into whether it might be an option.

The extra 15 seconds it takes to pull up that second code is short compared to the time you'd spend dealing with a hacked account.



Take the NeoLore Cyber Security Survey

Has your company done a Cyber Security Maturity Assessment within the last year? Do you have an IT security policy in place? Do you know if you've been hacked or are leaking data?

If your answer was "no" or "I'm not sure" to any of those questions, your company may be at risk for a devastating cyberattack.

Get the NeoLore Networks Cyber Security eBook for Free!

It Features

- Information on the various threats to your business
 - NIST Security Framework
 - CIS Controls
 - Basic Controls
- And More!