enGage

Nov 23

**Perseverance is not a long race;
it is many short races one after the other.**

- Walter Elliot

Featuring

Dr. Dilip Nath

AVP & Deputy CIO

SUNY Downstate Health Science University

Table Of Content

Editor's Note

Soumika Das

In the ever-evolving landscape of artificial intelligence, the quest to imbue machines with consciousness has long captivated the human imagination. The tale of the Mechanical Turk, an 18th-century chess-playing machine, illustrates how we've been drawn to the idea of machines having minds. The Mechanical Turk tricked people for 84 years, making them believe it was more than a mere machine, but, it was just a clever deception. Yet, the chasm between this human desire and the actual realization of AI consciousness remains vast.

Recent events, such as the audacious claim by engineer Blake Lemoine regarding AI consciousness within Google's LaMDA, followed by his abrupt dismissal, catapulted this debate into the forefront. The emergence of ChatGPT in November 2022 further fueled the discussion, yet skepticism still abounds.

Renowned philosopher and cognitive scientist David Chalmers, in his 1996 work "The Conscious Mind," explored the possibility of artificial consciousness, though recent remarks at NeurIPS underscored the disparities between large language models and genuine consciousness.

Discerning AI consciousness requires more than identifying structures akin to the human brain. A foundational theory that expounds on the nature of consciousness, its origins, and who possesses it is indispensable. Neuroscientists, philosophers, and AI researchers, including Turing Prize laureate Yoshua Bengio, have issued a white paper advocating practical methods for detecting AI consciousness. Yet, no existing system meets the stringent criteria outlined in their report card. Large language models excel in predictive text and making connections, kindling illusions of something more profound. However, their intellectual feats should not be conflated with consciousness, as the essence of awareness remains elusive.

The ethical dimension of AI consciousness looms large. Failing to identify conscious AI may lead to inadvertent cruelty or subjugation, while mistakenly attributing consciousness to the unconscious poses potential threats to human well-being. The question of what AI gains from consciousness is equally pertinent, given their remarkable achievements without it. In this pursuit of the elusive, the path to AI consciousness is fraught with ethical and philosophical conundrums, making it one of the most profound challenges of our technological age.

We have insightful articles lined up in this edition.

Dr. Dilip Nath, AVP & Deputy CIO, SUNY Downstate Health Sciences University, has written, **How can Generative AI transform the next generations of Healthcare?**

Pramod M has written, **A Deep Dive into the Value Chain of Generative AI.**

Naren Raja E and **Sripriyadharshini A** have written, **Key Benefits of Implementing SIEM in Cybersecurity Strategy**

Kumaresan Periyasamy has written, **Social Engineering: How to Identify and Prevent them?**

Sagar Neve has written, **The Future of AI and Automation in Telecom.**

Ravikiran Kada has written, **Navigating the Software Development Landscape: Generalist or Specialist?**

Happy Reading!

What's New in Tech

AI designs new robot from scratch in seconds

Researchers at Northwestern University developed the first AI that can intelligently design robots from scratch by compressing billions of years of evolution into mere seconds. It's not only fast but also runs on a lightweight computer and designs wholly novel structures from scratch — without human-labeled, bias-filled datasets.

AI advancing bird conservation efforts

Big data and AI are enabling the analysis of concealed patterns in the natural world. This extends beyond individual bird species, encompassing entire ecological communities across continents. The models track the complete annual life cycle of each species. This method uniquely tells which species occur where, when, with what other species, and under what environmental conditions.

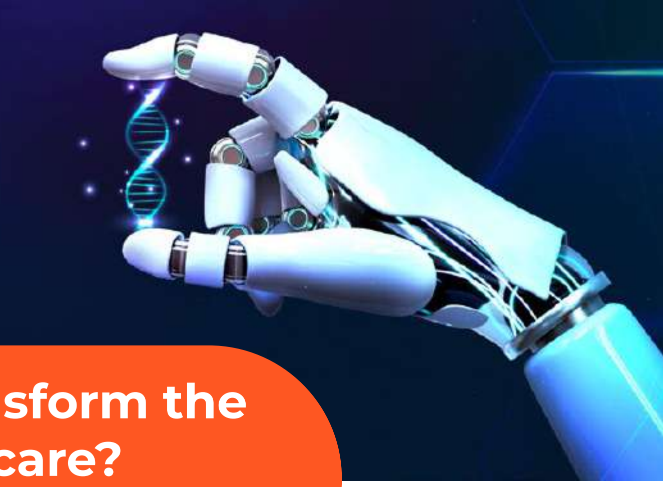
Novel algorithm stops harmful robot attacks

Australian researchers have developed a cyber algorithm that swiftly halts malicious robotic attacks. Using deep learning neural networks to simulate the behaviour of the human brain, they trained the robot's operating system to recognize the signature of a man-in-the-middle (MitM) cyberattack. The algorithm demonstrated a 99% success rate in preventing attacks.

AI models may aid in diagnosing schizophrenia

Scientists at the UCL Institute for Neurology, London, have developed new tools, based on AI language models, that can characterize subtle signatures in the speech of patients diagnosed with schizophrenia. This work shows the potential of applying AI language models to psychiatry.

Source: Science Daily



How can Generative AI transform the next generations of Healthcare?

Dr. Dilip Nath
AVP & Deputy CIO, SUNY Downstate Health Sciences University

The healthcare business is growing increasingly interested in the distinct type of artificial intelligence known as Generative AI. In contrast to traditional AI, Generative AI has the unique ability to generate new data by extrapolating patterns observed from pre-existing data sources. Conventional AI, on the other hand, is primarily concerned with data analysis and creating predictions based on current data. With this unique ability, Generative AI is well-suited for applications such as the development of cutting-edge pharmaceutical formulations, simulated patient data, and creative medical imaging.

Because of its capacity to accelerate the development of novel treatments and therapies, enhance diagnostic procedures and treatment plans, and generate fresh patient data, Generative AI has the potential to totally transform the healthcare environment. However, in order to secure this technology's responsible and ethical deployment in the healthcare sector, it is critical to apply rigorous and ethical stewardship in its implementation.

Specific uses for Generative AI in healthcare

Medical Imaging Advancements: With the analysis of large patient datasets, Generative AI enhances its potential to improve medical diagnosis by discovering patterns linked with certain diseases. This ground-breaking medical technology has the potential to help doctors, nurses, and other healthcare personnel detect illnesses more accurately and effectively. The relationship between Google Cloud and healthcare institutions exemplifies how AI technologies are being leveraged to tackle administrative and operational issues. These technologies, which are meant to make tasks like information retrieval and documentation easier to accomplish, will increase the amount of time available to researchers and clinicians (Gupta & Corrado, 2023).

Drug Discovery: The promising route that Generative AI offers allows for the identification of novel pharmaceutical compounds with the potential to treat a wide range of illnesses. According to McKinsey & Company (2023), one of the strengths of Generative AI is the analysis of various and unstructured data sources typical in the healthcare business. This innovative technology has the potential to transform these data sources into meaningful resources, allowing Generative AI to be more creative and effective in its quest for novel medications.

Patient Data: Generative AI is a potent tool for producing new patient data sets, which is critical for developing treatment regimens and improving patient well-being. According to BCG (Huddle et al., 2023), Generative AI systems have the ability to methodically analyze vast libraries of medical data and develop entirely novel stuff. The level of therapy may be enhanced, accessibility and cost may be improved, imbalances in research and healthcare delivery may be reduced, and companies may be able to generate hitherto untapped value as a result of this breakthrough technology.

Transformative Force: Healthcare may experience a fundamental transformation as a result of the promise of Generative AI, which transcends fads and trends to construct a continually evolving toolset. According to predictions, the global market for Generative AI would be valued $118.06 billion by 2032, highlighting the technology's enormous potential to revolutionize a wide range of operational elements and healthcare operations (Precedence Research, 2023).

The Ethical Use: However, in order to guarantee that this technology is utilized ethically and responsibly, it is critical that it be used with prudence. The ability of Generative AI systems to distinguish tiny alterations in longitudinal medical images, such as X-rays, CT scans, and MRIs, is proven. In the long term, examining these minute differences can aid in the development of improved diagnoses and treatment regimens.

Benefits from AI

According to an Accenture study, Generative AI has the potential to enhance up to 40% of working hours in the healthcare business. This figure is significant because it indicates the significant benefits that this technology may provide to a sizable portion of the medical workforce (Siwicki, 2023). According to the same poll, 98% of healthcare provider executives and 89% of healthcare payer executives believe that the emergence of Generative AI heralds a new age of business intelligence.

According to a recent McKinsey study, Generative AI has the potential to boost the world economy by $2.6 trillion to $4.4 trillion per year by 2040. This illustrates the technology's huge potential to help a wide range of organizations, including the healthcare sector (McKinsey & Company, 2023). According to an Elsevier survey, just 11% of healthcare decisions are presently supported by technologies based on Generative AI.

Nonetheless, a large 48% of respondents said doctors utilizing Generative AI will be better at making diagnosis and treating patients (Elsevier, 2023).

Furthermore, according to a Robert Half survey, 41% of US workers believe that Generative AI will positively impact their careers (Robert Half. 2023), implying that by making complex and labor-intensive processes simpler, this technology may aid in attracting the next generation to work in the healthcare sector.

Conclusively, Generative AI has the potential to change the healthcare industry by enabling the development of innovative pharmaceuticals and therapies, the improvement of diagnostic and treatment plans, and the generation of new patient data. But it is critical to utilize this technology wisely and in an ethical and responsible manner. Additionally, by automating difficult and labor-intensive activities, Generative AI can assist in the recruitment of the next generation to work in the healthcare field.

Note: This article was originally published in **'The Generation.'**

References

Precedence Research. (2023, September 22). Generative AI Market (By Component: Software, Services; By Technology: Generative Adversarial Networks (GANs), Transformers, Variational Auto-encoders, Diffusion Networks; By End-Use: Automotive & Transportation, BFSI, Media & Entertainment, IT & Telecommunication, Healthcare, Others) - Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook, and Forecast 2023-2032.
https://www.precedenceresearch.com/generative-ai-market

Robert Half. (2023, August 21). Not all bad news? Generative AI will benefit careers, say 41% of US workers. Staffing Industry Analysts.
https://www2.staffingindustry.com/Editorial/Daily-News/Not-all-bad-news-Generative-AI-will-benefit-careers-say-41-of-US-workers-66584

Siwicki, B. (2023, May 11). Generative AI could augment 40% of healthcare working hours. Healthcare IT News.
https://www.healthcareitnews.com/news/generative-ai-could-augment-40-healthcare-working-hours

Elsevier. (2023, September 7). New report finds doctors and nurses ready to embrace Generative AI to answer the pressure points facing global health systems. Elsevier.
https://www.elsevier.com/about/press-releases/corporate/new-report-finds-doctors-and-nurses-ready-to-embrace-generative-ai-to-answer-the-pressure-points-facing-global-health-systems

Huddle, M., Kellar, J., Srikumar, K., Deepak, K., & Martines, D. (2023, June 22). Generative AI Will Transform Health Care Sooner Than You Think. BCG.
https://www.bcg.com/publications/2023/how-generative-ai-is-transforming-health-care-sooner-than-expected

Gupta, A., & Corrado, G. (2023, August 29). Google Cloud Next: Generative AI for healthcare organizations - The Keyword. Google Cloud.
https://blog.google/technology/health/cloud-next-generative-ai-health/

McKinsey & Company. (2023, September 21). How Generative AI could add trillions to the global economy. McKinsey & Company.
https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier

About
the Leader

Dr. Dilip Nath is a distinguished leader in higher education and healthcare, known for his advocacy in voting and human rights. As a Harvard Kennedy School alumnus, he's celebrated for his transformative leadership.

With 30+ years of strategic planning expertise, Dilip focuses on using technology to bridge equity gaps in healthcare and education.

At 16, Dr. Dilip Nath emigrated from Bangladesh to the US, becoming the first in his family to attend college. He's lived in Queens for 33 years, earning the trust of his community as a dedicated leader and activist.

Recognizing the importance of knowledge in politics, he embarked on a self-learning journey about US government and principles of democracy. He earned degrees from the State University of New York, including an MBA and a DBA

Dr. Dilip Nath is know for his visionary, team-oriented, and compassionate leadership. He's a respected advocate for various community issues, including healthcare, immigrant rights, and education. He founded NAVA and co-founded ABHF to further his endeavors.

Dr. Dilip Nath

A Deep Dive into the Value Chain of Generative AI

Since late 2022, generative AI technology surged, impressing business leaders and investors with its ability to create human-like text and images. OpenAI's ChatGPT gained an astonishing one million users in just five days, outpacing Apple's iPhone adoption. Facebook and Netflix took months and years, respectively, to reach the same user base. Domains like finance and language preservation are embracing generative AI's novel capabilities, enabled by neural networks trained on vast data and using attention mechanisms to understand context and generate original content.

98%

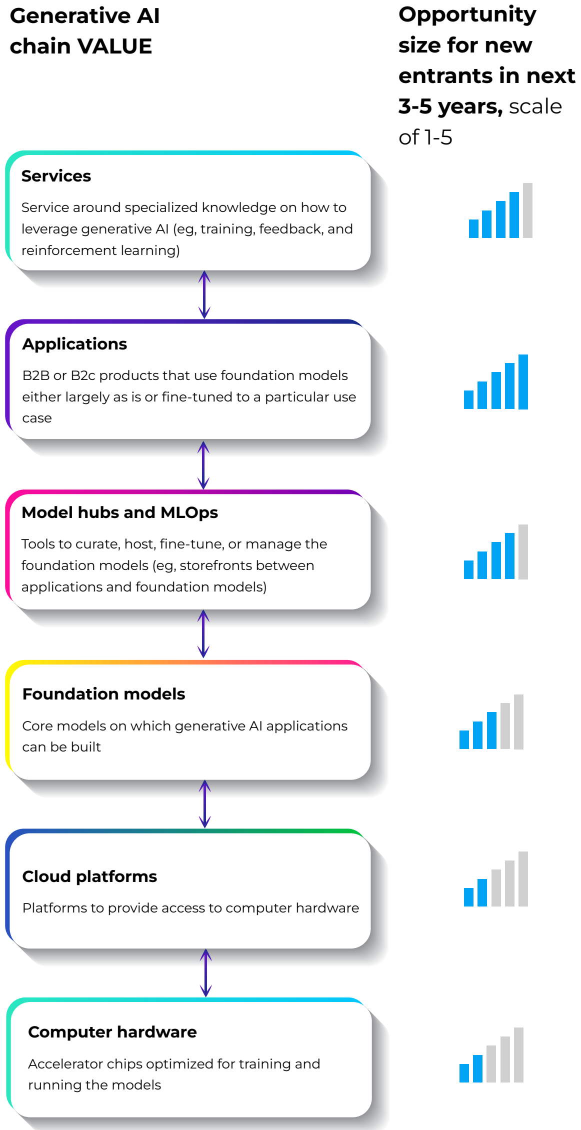
Of global executives agree AI foundation models will play an important role in their organizations' strategies in the next 3 to 5 years.

40%

Of all working hours can be imacted by large language models (LLMs) like GPT-4

The value chain of GenAI: Six links

As generative AI systems are being created and utilized, a fresh value chain is arising to facilitate the training and utilization of this potent technology. At first glance, it might appear quite akin to the conventional AI value chain. In essence, out of the six main categories—computer hardware, cloud platforms, foundation models, model hubs and machine learning operations (MLOps), applications, and services—only the inclusion of foundation models is novel.



Generative AI chain VALUE

Opportunity size for new entrants in next 3-5 years, scale of 1-5

Services
Service around specialized knowledge on how to leverage generative AI (eg, training, feedback, and reinforcement learning)

Applications
B2B or B2c products that use foundation models either largely as is or fine-tuned to a particular use case

Model hubs and MLOps
Tools to curate, host, fine-tune, or manage the foundation models (eg, storefronts between applications and foundation models)

Foundation models
Core models on which generative AI applications can be built

Cloud platforms
Platforms to provide access to computer hardware

Computer hardware
Accelerator chips optimized for training and running the models

McKinsey & Company

Computer hardware

Generative AI systems like OpenAI's GPT-3 rely on vast knowledge—trained on approximately 45 terabytes of text data—which demands specialized hardware. Traditional computers are insufficient for these workloads; instead, large clusters of GPUs or TPUs with accelerator chips are necessary to process the massive data across billions of parameters in parallel.

Cloud platforms

GPUs and TPUs are expensive and limited in availability, making it impractical for most businesses to own and manage them on-site. Consequently, companies turn to cloud-based solutions to access and utilize computational power efficiently, allowing for greater flexibility and cost management.

Foundation models

Generative AI relies on foundation models—large pretrained deep learning models designed for specific content creation tasks and adaptable to various applications. Like Swiss Army knives, these models, exemplified by OpenAI's GPT-3 and GPT-4, generate human-quality text, powering applications like ChatGPT, Jasper, and Copy.ai. Training foundation models involves vast datasets from public and private sources, necessitating expertise in data preparation, model architecture selection, training, and fine-tuning to enhance output quality.

Model hubs and MLOps

To utilize foundation models for building applications, businesses require two key elements: a storage and access platform for the foundation model and specialized MLOps tools for adaptation and deployment within their applications. Model hubs serve this purpose, offering access to closed-source models through APIs and licensing agreements, with MLOps capabilities provided by the model developer. For open-source models, independent model hubs are emerging, offering a range of services, from model aggregation to end-to-end MLOps support, catering to companies seeking generative AI technology without extensive in-house resources.

Applications

Foundation models possess the versatility to handle diverse tasks, but it's the applications built upon them that enable specific functionalities, like customer support or marketing emails. These applications may come from new entrants aiming for unique services, existing providers adding innovative features, or businesses striving to gain a competitive edge in their industry.

Applications built from fine-tuned models stand out

Applications built on fine-tuned models excel in generative AI, falling into two categories: those using foundation models with slight customization and those leveraging fine-tuned models with additional data and parameter adjustments for specific use cases. Fine-tuning is cost-effective, faster, and accessible to many companies. Data for fine-tuning can come from industry knowledge, proprietary sources, or user feedback loops. Staying updated on generative AI advancements is crucial for developers to assess the benefits of adopting newer foundation models with enhanced capabilities.

Services

The emergence of dedicated generative AI services is inevitable as companies strive to enhance their capabilities and explore business opportunities and technical challenges. Established AI service providers will likely adapt and expand to cater to the generative AI market, while niche players may enter with specialized expertise in applying generative AI to specific functions, industries, or capabilities, like customer service workflows, drug discovery, or feedback loop implementation in various contexts.

Evolving Service Catalogue for Specific Verticals & Operations

Healthcare

- **Clinical notes and Report generation:** Improves clinician efficiency by automating tasks like generating clinical notes, letters, and responses to patient queries.

- **Medical Imaging Enhancement and Generation:** Leverage medical imaging advancement by producing high-quality images such as MRI and CT scans, facilitating early disease identification and precise diagnostics.

- **Anomaly Detection:** Learn what normal medical data looks like and then flag anomalies or outliers in patient data, which can aid in the early detection of diseases or unusual conditions.

- **Patient Data Augmentation:** Generative models can augment datasets used for training machine learning algorithms, thereby improving the accuracy and robustness of these algorithms.

BFS

- **Know your Client:** Customer Data Platform to generate a summarized and unified customer profile with risk and credit score profiles, intelligent document processing in KYC process.

- **Fraud Detection and Prevention:** To produce synthetic data mimicking genuine and fraudulent transactions, enhancing fraud detection algorithms' accuracy and adaptability to changing fraud trends.

- **Personalized Financial Advice:** Enables personalized financial advice by analyzing individual financial situations, goals, and risk preferences to generate tailored recommendations, facilitating informed and prudent decision-making for customers.

- **Credit scoring and loan approval:** To automate credit assessments by analyzing customer credit and financial data to predict creditworthiness, enhancing loan approval efficiency.

- **Financial Document Generator:** To streamline financial document creation by producing diverse forms like investment reports, tax documents, and insurance policies, leading to time savings and decreased human errors.

Operations

- **Text generation:** Improving clinician efficiency with administrative tasks such as assisting with generation of clinical notes, letters, responding to patient queries (e.g., autogenerating responses to EHR inbox messages) and producing patient information and educational material.

- **Text summarization:** Enabling clinicians to easily find the information they need, for example through summarizing information within a patient's EHR or large volumes of medical literature. Providing patients with specific summaries of their health information.

- **Question answering:** Enhancing patient-facing chatbots and conversational assistance supporting activities such as triage, care navigation and administrative questions (e.g., billing). Enabling clinical decision support through answering clinical questions, for example, differential diagnoses and treatment options.

- **Text classification:** Medical domain specific LLMs enable classification of the large volume of unstructured text within the EHR for multiple purposes. This includes making it available for research and data analysis, enabling identification of patients for clinical trials and facilitating clinical coding for billing purposes. Text classification could also be used for sentiment analysis of patient feedback and reviews.

As organizations move forward, they must focus on understanding how generative AI will impact their industries and consider strategic choices to exploit opportunities and manage challenges. Additionally, understanding the value chain of generative AI, including computer hardware, cloud platforms, foundation models, model hubs, MLOps, and applications, is critical for organizations seeking to leverage the technology effectively.

References

- Exploring opportunities in the gen AI value chain | McKinsey
- The CEO's Guide to the Generative AI Revolution | BCG
- Generative AI Technology in Business | Accenture
- Quick Answer: What Healthcare Provider CIOs Need to Know About LLM Applications Such as ChatGPT | Gartner

About the Author

Pramod M has an overall experience of around 17 years in Aerospace, IT, Education & Product development. He holds a MBA degree from Leeds University Business School, UK and currently working with solutions & strategy team at GS Lab | GAVS.

Pramod M

Key Benefits of Implementing SIEM in Cybersecurity Strategy

Security Information and Event Management (SIEM) pull together log information from all log sources (Security tools, Servers, Network devices etc.) and stores all in one place.

SIEM offers a dashboard where collected data is organized, offering a visual representation of the data. Security Analysts receive alerts when threats are detected, and these alerts can be configured to come via the dashboard or through email.

Implementing SIEM in your cybersecurity strategy offers a range of significant advantages. Here are a few of them -

• Centralized Log Management

SIEM tools provide a centralized platform for log management, making it easier to collect, store, and search through massive amounts of security data. Log data comes in different formats and structures depending on the source. SIEM tools normalize this data, making it consistent and easily interpretable. SIEM systems can identify patterns, anomalies, and security events that may go unnoticed when examining logs individually. By correlating data, they can detect complex, multi-stage attacks that involve multiple systems. It helps organizations understand the timeline of an attack or data breach.

• Improved Threat Detection and Response

SIEM systems collect, monitor, and analyze security data from various sources, such as network traffic, logs, and endpoints. This holistic view allows organizations to detect anomalies and potential threats in real-time. By identifying unusual patterns or unauthorized access, security teams can respond quickly and mitigate potential security incidents.

• Compliance and Reporting

Organizations are subject to various regulatory requirements, such as GDPR, HIPAA, PCI DSS, and more. These regulations dictate specific security and privacy measures that must be in place. SIEM solutions help organizations comply with these regulations by monitoring and reporting on relevant security controls and activities. SIEM systems assist in compliance efforts by automating the collection and reporting of security-related data and reducing the risk of non-compliance.

• Reduced False Positives

One of the significant advantages of SIEM is its ability to reduce false positives. By correlating data from multiple sources and applying sophisticated rules and algorithms, SIEM tools help security teams distinguish real threats from false alarms.

This, in turn, improves the overall efficiency of incident response efforts.

- ## Enhanced Incident Response

SIEM solutions not only detect threats but also facilitate faster and more effective incident response. They provide alerts and notifications to security teams, helping them take swift action. Automated incident response workflows can also be implemented, allowing organizations to respond to threats 24/7.

- ## Forensic Analysis and Investigation

Forensic analysis begins with collecting data relevant to the incident. This data may include logs, network traffic records, system files, and other sources of information. SIEM systems continuously monitor for security incidents and alerts. When a potential incident is detected, it triggers an alert. Security analysts review the alerts generated by the SIEM. Forensic analysis involves the examination of the collected data to reconstruct the incident's timeline, understand the attack vectors, and identify the root cause. Analysts try to determine the source and purpose of the attack or incident. They classify the incident as either a security breach or a false positive. Based on the findings of the forensic investigation, the incident response team takes action to contain, mitigate, and remediate the incident. This might involve isolating affected systems, patching vulnerabilities, and enhancing security controls.

- ## Cost Savings

While the initial implementation of a SIEM system can be an investment, the long-term benefits often lead to cost savings. SIEM streamlines security operations, reducing the need for manual monitoring and investigation, thus saving both time and money.

- ## Scalability

SIEM systems are highly scalable and can adapt to the evolving needs of an organization. As the volume of data and complexity of threats increase, SIEM can expand to accommodate these changes, ensuring that an organization's security posture remains robust.

- ## Real-time Visibility

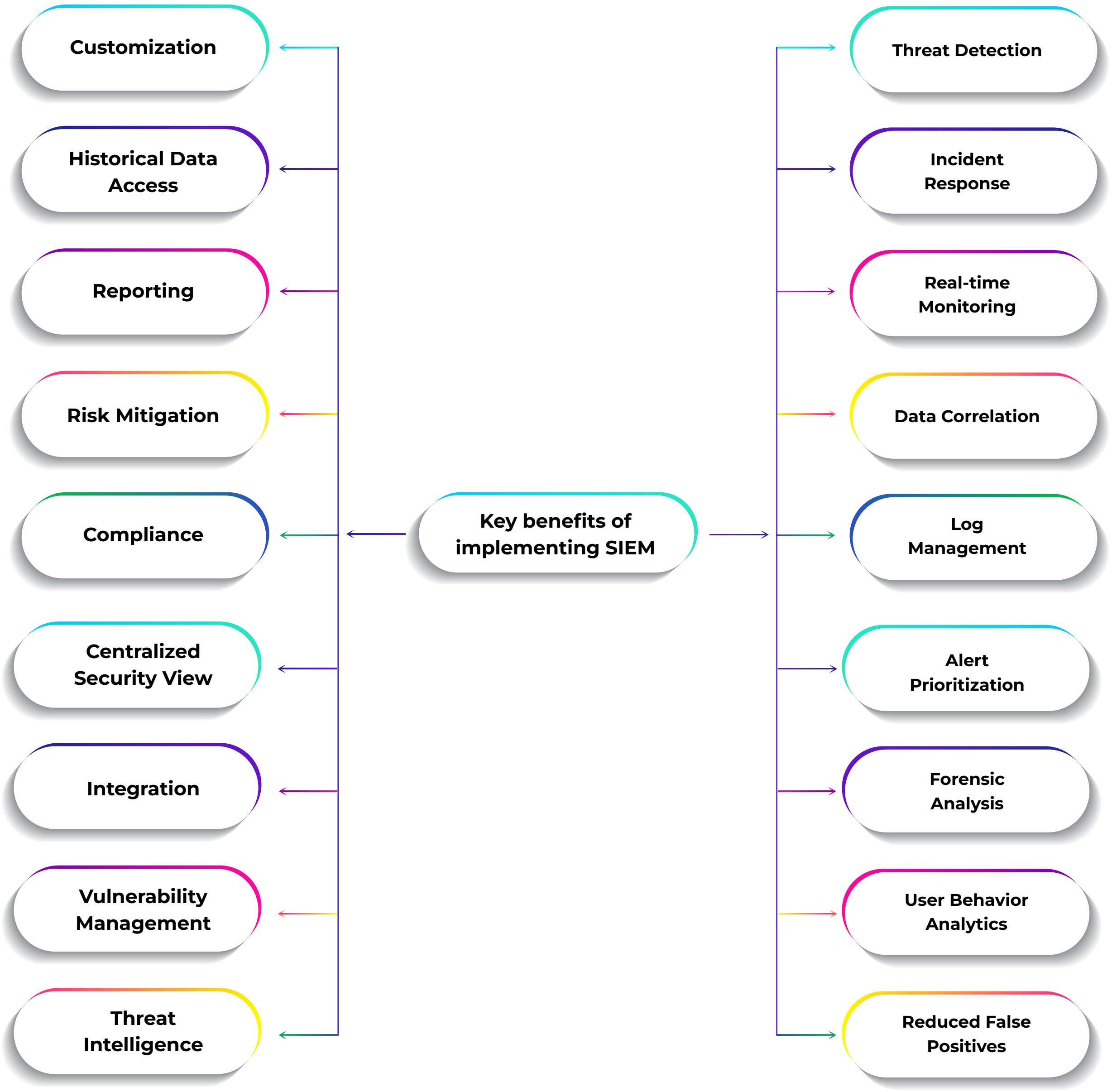
By providing real-time visibility into network activities and security events, SIEM tools empower organizations to act proactively. This real-time insight can help identify emerging threats and vulnerabilities before they can cause significant damage.

- ## User and Entity Behavior Analytics (UEBA)

Many SIEM solutions incorporate UEBA capabilities, which enable organizations to detect abnormal user and entity behavior. This helps in identifying insider threats and compromised accounts, ultimately strengthening the security posture.

- ## Customization and Integration

SIEM systems can be tailored to the specific needs and technologies of an organization. They are often compatible with various security solutions and can integrate with other tools for a seamless and comprehensive security infrastructure.



SIEM plays a pivotal role in enhancing the cybersecurity posture of organizations. With its centralized log management, improved threat detection and response, compliance and reporting capabilities, and reduction of false positives, SIEM offers a comprehensive solution for safeguarding critical data and systems.

About the Author

Naren Raja E is a Lead SOC Engineer at GS Lab | GAVS and is interested in learning new technologies in the cybersecurity space and exploring avenues for product improvements.

Naren Raja E

About the Author

Sripriyadharshini A is a seasoned Security Operations Center (SOC) analyst with a passion for cybersecurity and a commitment to enhancing digital defenses. She enjoys exploring new cybersecurity technologies.

Sripriyadharshini A

Social Engineering

How to Identify and Prevent them?

Social engineering attacks are a type of cybersecurity threat that relies on psychological manipulation to deceive and trick people into divulging sensitive information, such as passwords or other confidential data. These attacks have become increasingly common in recent years and can cause significant harm to individuals and organizations.

In this article, we will discuss what social engineering attacks are, the different types of social engineering attacks, and how to recognize and prevent them.

What are Social Engineering Attacks?

Social engineering attacks are tactics used by cybercriminals to exploit human weaknesses to gain unauthorized access to sensitive information. Attackers use various techniques, such as impersonation, pretexting, phishing, and baiting, to manipulate people into divulging confidential data or clicking on malicious links.

The primary goal of social engineering attacks is to trick people into revealing information that the attackers can use to gain access to computer systems, steal money or data, or perpetrate other cybercrimes.

Types of Social Engineering Attacks

There are several types of social engineering attacks, and we will discuss the most common ones:

Phishing: Phishing is one of the most common social engineering attacks. It involves sending fake emails that appear to be from legitimate sources, such as banks or e-commerce sites, to trick people into divulging their login credentials, credit card numbers, or other sensitive information. Phishing attacks can also come in the form of instant messaging, text messages, or social media messages.

Pretexting: Pretexting involves creating a false scenario to trick people into divulging confidential information. Attackers use various tactics, such as impersonating authority figures or pretending to be someone in a position of trust, to manipulate people into giving up sensitive data.

Baiting: Baiting is a social engineering attack that involves offering something of value, such as free software or concert tickets, to entice people into clicking on a malicious link or downloading a file that contains malware.

Quid pro quo: Quid pro quo is a social engineering attack that involves promising something in exchange for sensitive information. For example, an attacker might offer technical support in exchange for login credentials.

Spear phishing: Spear phishing is a more targeted version of phishing. It involves sending fake emails that appear to be from someone the victim knows or trusts, such as a colleague or supervisor. Spear phishing attacks are more challenging to detect because they are tailored to the victim's specific interests or job functions.

Recognizing Social Engineering Attacks

Social engineering attacks can be challenging to detect, but there are several signs to watch out for:

Urgency: Social engineering attacks often involve a sense of urgency, such as threatening to shut down an account or insisting that action must be taken immediately. Attackers use urgency to manipulate people into making hasty decisions that they may later regret.

Suspicious links or attachments: Social engineering attacks often involve malicious links or attachments that can infect your computer with malware or steal your login credentials. If you receive an email or message with a suspicious link or attachment, do not click on it.

Requests for sensitive information: Legitimate companies or organizations will rarely ask you to divulge sensitive information, such as login credentials or credit card numbers, via email or text message. If you receive a message requesting such information, do not respond and report it to the appropriate authorities.

Unusual sender: Be wary of emails or messages from senders you don't know or recognize. Attackers often use fake email addresses or impersonate legitimate senders to trick people into clicking on malicious links or downloading malware.

Social engineering attacks can be difficult to detect, but there are several steps you can take to prevent them from happening to you or your organization.

- **Educate yourself and your employees:** The first step in preventing social engineering attacks is to educate yourself and your employees on the various tactics that attackers use, such as phishing, pretexting, and baiting. Make sure that everyone in your organization is aware of these threats and knows how to recognize them.

- **Use strong passwords:** Strong passwords are an essential defense against social engineering attacks. Make sure that all your accounts have strong passwords that are difficult to guess. Use a combination of letters, numbers, and special characters, and avoid using the same password for multiple accounts.

- **Be cautious of unsolicited emails or messages:** Be cautious of unsolicited emails or messages, especially those that ask for personal or sensitive information. If you receive an email or message that seems suspicious, don't click on any links or attachments, and don't reply to the message.

- **Verify requests for information:** If you receive a request for personal or sensitive information, always verify the request before responding. Call the company or organization directly using a phone number that you know is legitimate, rather than responding to an email or message.

- **Keep your software up to date:** Keeping your software up to date is essential for preventing social engineering attacks. Software updates often include security patches that can prevent attackers from exploiting vulnerabilities in your system.

- **Use antivirus and anti-malware software:** Antivirus and anti-malware software can detect and remove malicious software before it can do any damage. Make sure that you have antivirus and anti-malware software installed on all your devices and keep it up to date.

- **Limit the amount of information you share online:** Limit the amount of personal information that you share online, such as your full name, date of birth, or address. Attackers can use this information to create fake identities or steal your identity.

In conclusion, social engineering attacks are a serious threat to individuals and organizations. By educating yourself and your employees, using strong passwords, being cautious of unsolicited emails or messages, verifying requests for information, keeping your software up to date, using antivirus and anti-malware software, and limiting the amount of information you share online, you can help prevent social engineering attacks from happening to you or your organization.

About the Author

Kumaresan Periyasamy has more than 17+ years of Technology experience in Cyber Security, IT Infrastructure Audit, Risk Management, Compliance and Project Management. He has done his MBA in IT Systems.

Kumaresan Periyasamy has rich experience in Information Security, GRC, Information Technology Audit, Compliance Audits and Program Management.

Kumaresan Periyasamy

The Future of AI and Automation in Telecom

Modern day Telecom networks are highly complex and increasingly so. Given the huge diversity in network components, functions, and services, they demand significant investment of time and human resources for deployment and maintenance. Experts anticipate that by 2030, telecom networks would require integration of over 50 to 60 different types of devices! Due to the complexities involved, the volume of support calls inundating Network Operations Centers (NOCs) also continues to grow. All of this has reiterated the need to find innovative solutions.

Traditional and Modern Challenges of Telecom Automation

Human-centric QA activities have evolved significantly, incorporating various tools, toolchains, and frameworks. However, Telecom QA complexity arises from dealing with intricate architectures, numerous network functions, and many network protocols like Diameter, GTP V2, ISAAC, PFCP, and more. The infrastructure is intricate, and interdependencies between components abound, particularly due to the proliferation of independently developed network functions that must work harmoniously with others.

Writing QA automation tests involves the interpretation of lengthy specification documents and their transformation into automated test cases.

Despite the use of generic automation tools, toolchains, frameworks, and technological advances like the cloud, human effort remains indispensable. This brings challenges such as human error and retention into the equation.

The introduction of the cloud transformed the Telecom landscape, enabling the transition from fixed hardware to dynamic, open networks with abstraction layers, simplifying deployments and maintenance. Major players such as Google, Microsoft, and AWS also introduced their specific tools, catering to Telecom network deployment and management. These tools are tailored to the unique demands of Telecom networks.

The primary goal of network operations is to ensure high availability. DevOps partially addresses traditional operational challenges. Beyond scalability and high availability, operations bring unique challenges, including guaranteeing that business Service Level Agreements (SLAs) are met, generating accurate call data records, detecting anomalies, managing network congestions, data migrations, and providing customer support.

The operations team also receives requests to address issues related to dependencies among multiple application services, rest API calls, and interconnected services. These issues affect a minuscule percentage of users but demand high human involvement. Solving these operational challenges within specific timeframes is critical, as they directly impact Return on Investment (ROI).

Telecom teams constantly face the need to reskill and upskill themselves. Telecom predominantly dealt with circuit switching in the past, and Telecom teams were trained accordingly. Evolving technologies require Telecom teams to undergo periodic reskilling.

Using AI for QA Automation

The world of AI is making remarkable advancements and recent applications like ChatGPT have demonstrated that AI is not just hype and can be leveraged for practical, real-world applications.

In Telecom, AI has the potential to address two key objectives: minimizing disruptions and maximizing service availability. AI applications need to understand complex network and Telecom service meshes, along with network topology, monitor health, Service Level Agreements (SLAs), and perform deep packet inspection to detect hard-to-simulate anomalies. Predicting future failures is another goal, although it remains a significant challenge due to the vast amount of operational data.

However, current AI engines are not yet mature enough to provide end-to-end solutions. One strategy for bridging this gap is the development of intermediary tools. Recent advancements, like GPT-3, have demonstrated the potential of AI, particularly in Natural Language Processing (NLP). Mature NLP models, when properly trained, can understand context along with keywords. This paves the way for creating abstraction layers that simplify using AI-enabled engines.

Tools such as Octopus assist in QA, DevOps, and operational challenges. Octopus is an interpreter, translating between different languages to facilitate AI understanding and adoption.

Future of AI in Telecommunication

Looking toward the future, there are some exciting prospects to consider:

- **Open SourceTelecom AI:** With the increasing adoption of open source Telecom technologies, there is a possibility to have open source Telecom-specific AI. Users won't need to develop AI engines from scratch, as AI will learn from traffic patterns and be available out of the box with open source Telecom cores. This autonomous system will continuously train itself, reducing human effort and enabling customization when needed.

- **Explainable AI:** This concept ensures that AI developers provide reasoning for AI decisions. This move can enhance trust in AI, especially in critical applications, where the reasoning behind AI decisions can be stored in non-alterable systems like hyper-ledgers.

- **Distributed AI:** AI could be integrated at multiple levels within Telecom components, allowing them to work independently and collaboratively. For instance, a user's pattern and application context could lead to dynamic bandwidth allocation for seamless user experiences.

These advancements hold promise for the future of Telecom, driving efficiency, minimizing human effort, and enhancing overall performance and trust in AI-driven systems.

GS Lab | GAVS plays a pivotal role in enabling key players in the telecom ecosystem to transform their infrastructure in tandem with the dynamic changes that this transformation demands. Equipped with about two decades of experience in the telecom, networking, cloud, and enterprise space, GS Lab | GAVS is a trusted partner in end-to-end system integration for global telecom leaders. For more on our telecom offerings, please visit https://www.gavstech.com/5g-engineering/

This blog is a gist of the webinar, but you can watch the entire discussion here. GS Lab | GAVS periodically organizes insightful webinars with our own tech leaders, the leadership team, and industry thought leaders to explore current and emerging trends. To watch all our webinar recordings, please visit https://www.gslab.com/webinars and https://www.gavstech.com/videos/

About the Author

Sagar Neve is an Associate Director Engineering at GS Lab | GAVS with over 20 years of experience in the telecom industry. He has successfully delivered different projects and products for various organizations and has a keen passion for problem-solving. He likes to dig into customer problems. Finding different ways to solve the problem fascinates him. Sagar's strong focus lies in nurturing leadership within teams and crafting elegant, scalable, and distributed solutions. He welcomes different perspectives, and is open to discussing emerging technologies. Beyond work, he is passionate about reading, driving, and food.

Sagar Neve

Navigating the Software Development Landscape

Generalist or Specialist?

This is perhaps one of the most continually asked questions by all the entry level software engineers.

In this article, we will try to debunk one of the age-old debates of whether you should become a specialist or a generalist. Should you become a “full-stack developer,” or should you specialize in one or two areas of software development and “go deep?” or should you specialize in Java or should you also specialize in UI technologies?

To be honest the real answer is both. Let’s find out why.

The Power of Specialization

Before we get into the topic, let's start by exploring just how important and beneficial specialization is. Let’s suppose that you were on trial for a crime (I hope this never happens). Yes, a crime you did not commit. But you still need to prove you are not guilty. What do you do?

Do you hire a lawyer who is good at labor law, civil law, real estate law and criminal law? Or do you hire a lawyer who specializes in criminal law, specifically defending people who are convicted of robbery? I don’t know about you, but if the rest of my life is on the line, I’m going to choose the specialist every time.

Many people say they would prefer being a generalist, but when it comes down to it, they pick a specialist every time.

That’s not to say there isn’t any value in having a broad base of knowledge, or being a generalist to some degree, but it is extremely valuable to be a specialist of some kind—or at least to market yourself that way.

The lawyer that you hired might be very good in multiple areas of law and have knowledge in several fields. But he advertises himself as a murder or criminal lawyer because he understands the power of specialization.

Another simple example, if you had to build a customized wooden chair and you had to choose between a contractor who knows carpentry, plumbing, painting versus a person specializing in carpentry. I would choose the person specializing in carpentry.

Don’t you think the carpenter could probably handle other jobs? Of course, they can, but they preferred to specialize because it may be more profitable than other jobs.

Have a broad base in order to specialize!

One thing that many software developers should take note of is, all specialists are also generalists, but no generalists are specialists. What does that mean?

In order to acquire the skills of a specialist, a great deal of general knowledge is required, and it is accumulated along the way.

It is tough being a good specialist without building a broad general knowledge about your field.

One of my friends' wife is studying to become an oral surgeon. She had to first go through dental school and become a dentist. Now, she's not going to be doing general dentistry very often, but to her, filling a cavity or doing some general dentistry work is cake. She's probably better than most generalist dentists, simply because she had to learn all that and more to become an oral surgeon.

It's all about the T Factor

What do you really want to strive for is T-shaped factor or T-Shaped knowledge? It means you have deep knowledge on one skill or technology and a broad base of knowledge in your field or area.

As a software developer, you should strive to be well-versed in front-end, back-end, databases, best practices, algorithms, data structures, system design, architectures, etc. But pick at least one area where you are going to go in-depth. You need to pick some specialization that will set you apart from the masses and increase your value.

You have to be versatile and adaptable to learn quickly if asked to work on the skills which you knew very little of.

You can't be a generalist today

It's not really possible. The field of software development and technology is so vast, it is hard to cope with the pace. Hence, you can't know everything present out there. Yes, you can have a broad knowledge base. Even if you are a "full stack" Javascript developer, you are going to have to pick a stack or two i.e., either MERN or MEAN stack. You can't know them all and be super effective. It's not just computer science and programming where we have so many options to choose from. Every profession is moving towards more value on specialization.

Lawyers, Financial Analysts, Accountants, and just about every kind of engineer must specialize to be effective and unique, because knowledge domains are growing.

But what if I specialize in the wrong area?

Then specialize in something else. When I started my career back in 2012, I specialized in Java Swings which was used to create desktop applications. During the same period, desktop applications were no longer preferred, the era of web applications had already started and grew in popularity. Did I switch my career and become a Lawyer? No. Since I already knew Java, I planned to specialize in the Java based framework i.e., Spring framework which is a one stop solution for developing enterprise back applications.

A lot of software developers are afraid of picking the wrong thing to specialize in and end up not specializing in anything. They remain stagnant in their careers for years, paralyzed by fear, always considering the "what ifs." Don't do that; just pick something and go with it. Something is better than nothing, hence you can always change directions later if you need to. You'll notice that once you learn how to go deep into one specialization, the next one is much easier.

So, what should you do?

Regardless of where you are in your career, pick some kind of specialization to pursue. Whatever you choose, try to build your personal brand around it, and decide to go deep. But should we choose a specialty based on our interests or on what we're doing for our current employer? Well, this is a tough one.

If you plan to specialize on something different from what you are currently working on every day, it will be difficult to build the expertise you need and go into the depth required to specialize. It's certainly possible though.

Perhaps start off learning your desired specialization and building a reputation around it in the mornings before work and/or in the evenings.

Don't be just a Java developer: be a Java developer specializing in a Spring framework and know some UI stack. Try out as small as possible and get into more details as you go.

You can always branch out and expand later. Learn how to write good code. Try to avoid learning a bunch of different programming languages and frameworks that you may never use.

By following this approach, your progress and success will trend upwards.

About the Author

Ravikiran Kada is a Lead Software Engineer at GS Lab | GAVS, has around 10 years of software development experience primarily working on technologies such as Java and Spring Boot. Most of the experience has been in the Banking domain covering areas such as Insurance, Retail banking, Research, Lending etc.

Ravikiran Kada enjoys playing cricket at club level and is a sports enthusiast enjoying several other sports.

Ravikiran Kada

enGAge

www.gslab.com | www.gavstech.com

Follow us on: