ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

AI in Cybersecurity and User Interface Design beyond Chatbots

Shriyash Shete

Zscaler, Inc. Bloomington, IN, USA

ABSTRACT

This paper examines the integration of Artificial Intelligence (AI) in cybersecurity, highlighting how AI is revolutionizing cloud security for enterprises amidst increasing cyber threats. It defines key concepts including AI, Machine Learning, Large Language Models, Natural Language Processing, and Generative AI, and explores their applications in cybersecurity. Focused on enhancing the efficiency and efficacy of cybersecurity solutions, the paper delves into AI-driven technologies like Text-to-Visualization, Breach Analytics, and Multi-modal Data Protection. It also discusses the impact of AI on user experience (UX) design, advocating for user-centric, intuitive interfaces in cybersecurity tools. The paper concludes by emphasizing the importance of ethical considerations in AI deployment and the crucial role of UX designers in shaping the future of AI-enhanced cybersecurity solutions.delves into AI-driven technologies like Text-to-Visualization, Breach Analytics, and Multi-modal Data Protection. It also discusses the impact of AI on user experience (UX) design, advocating for user-centric, intuitive interfaces in cybersecurity tools. The paper concludes by emphasizing the importance of ethical considerations in AI deployment and the crucial role of UX designers in shaping the future of AI-enhanced cybersecurity solutions.

***Corresponding author**

Shriyash Shete, Zscaler, Inc. Bloomington, IN, USA.

Received: December 04, 2023; **Accepted:** December 13, 2023; **Published:** December 21, 2023

Keywords: Artificial Intelligence, Cybersecurity, User Experience Design, AI-Driven Security Solutions

Introduction

Cybersecurity is defined as a set of processes and methodologies to protect computer systems, networks and data from digital attacks, unauthorized access and damage. It is a crucial aspect of modern society as it protects individuals, organizations and governments from cyber-attacks and cybercrime. As more and more of our daily lives are conducted online, the need for robust cybersecurity measures becomes increasingly important [1].

Cybersecurity has rapidly evolved and frequently made headlines in the past decade due to the increasing number of threats and the continual efforts of cybercriminals to out-pace law enforcement. While the fundamental reasons behind cyberattacks have largely stayed the same over the years, the methods used by cybercriminals have grown more advanced. Conventional cybersecurity methods are now often insufficient in identifying and countering new types of cyberattacks. However, developments in cryptography and Artificial Intelligence (AI) offer hope, presenting new ways for cybersecurity professionals to combat the constantly changing tactics of adversaries [2].

In this paper, we present an overview of the cybersecurity threat landscape and discuss the various facets of Artificial Intelligence technology that could be foundational for next-gen security solutions. We discuss the enterprise user needs by identifying the goals, challenges, and pain points of the target persona of cybersecurity professionals and describe applications of AI that can assist them in achieving their goals. Finally, we present some key use cases in the cybersecurity community that can leverage AI technology and how they can be visualized through an interface design based on a user-centered approach.

Background

Before we dive deep into the implications of AI in cybersecurity and user experience design, it's imperative to understand the basic definitions and differences in the technological terms:

Artificial Intelligence

"Artificial Intelligence" (AI) refers to systems that can replicate human intelligence and cognitive processes. Science fiction has often presented a dramatic view of AI, showing advanced machines with human-like thinking capabilities. However, the reality is that current technology is far from achieving such advanced AI, known as artificial general intelligence [2].

Presently, the focus is more on artificial narrow intelligence, or weak AI, which is designed to perform specific tasks. Within this domain, there are two main types: rule-based AI, where machines operate based on set rules, and example-based AI, where they learn from examples [3,4].

AI manifests in various forms including machine learning, computer vision, natural language processing, and robotics. It's increasingly common to use "AI" to denote machines that imitate human cognitive functions like learning and problem-solving. A comprehensive definition of AI would be the field dedicated to creating systems that emulate human intelligence and thought processes, encompassing a wide range of applications and technologies [5].

Machine Learning

Machine learning (ML), a branch of artificial intelligence (AI), focuses on enabling AI systems to perform tasks without explicit programming. Essentially, it involves teaching machines to learn autonomously.

To understand this, consider human learning processes. Humans aren't born with advanced knowledge; instead, we start with a basic understanding of our surroundings and gradually acquire knowledge. This learning occurs through sensory experiences, interactions with our environment, teachings from others, pattern recognition, and extensive trial and error.

Similarly, AI systems initially lack knowledge. Through machine learning, these systems are equipped to learn and adapt to their environment, mirroring the way humans learn and evolve in understanding [2,3,4,5].

Large Language Model

Large Language Models (LLMs) are advanced computer programs designed to understand and create human language. They work by using large neural networks, which are sets of algorithms modeled after the human brain, to process text. These models are trained on huge amounts of written material, like books and articles, which helps them learn how language works, including grammar, context, and even subtleties like humor and sarcasm.

LLMs can do impressive things with language. They can write coherent text, answer questions, translate languages, and more, all by analyzing the context of the words and sentences they're given. However, they're not perfect and can sometimes replicate biases found in their training data. They're powerful tools for interacting with and generating language but need careful handling to address ethical concerns like privacy and misinformation [5, 6].

Natural Language Processing

NLP, or Natural Language Processing, is a technology that helps computers understand, interpret, and respond to human language in a valuable way. It's like teaching a computer to understand and speak our language. Imagine you're typing a question into a search engine or talking to a voice-activated assistant like Siri or Alexa; NLP is what helps these systems understand your words and respond appropriately.

NLP combines computer science and linguistics (the study of language) to break down and analyze human language. It works on tasks like translating languages, converting speech to text (like when you dictate a message to your phone), or picking out important information from large documents. The goal is to make interactions between computers and humans feel natural and easy, almost like talking to another person [5,6].

Generative AI

Generative AI refers to a branch of artificial intelligence that is concerned with the creation of novel content, encompassing various mediums such as text, imagery, music, and video. This technology operates by employing complex algorithms to synthesize new outputs that are derivative of, yet distinct from, the data it has been trained on.

In essence, generative AI functions as a digital creator, utilizing its extensive training in existing content to produce original works. For instance, when tasked with composing a narrative, generating an image, or creating a musical composition, generative AI analyzes and emulates patterns, styles, and structures inherent in its training data to produce new, unique creations. This capability differentiates it from other AI models, which primarily focus on the interpretation, analysis, or categorization of data. Generative AI stands out for its ability to engage in creative processes, offering innovative contributions that extend beyond the scope of mere data processing [3].

In summary, while all these terms are interrelated and fall under the broad umbrella of AI, they each have a specific focus: AI is the general field, ML is about learning from data, LLMs are about language processing at a large scale, NLP is about understanding and interacting with human language, and Generative AI is about creating new, original content [4,5,7].

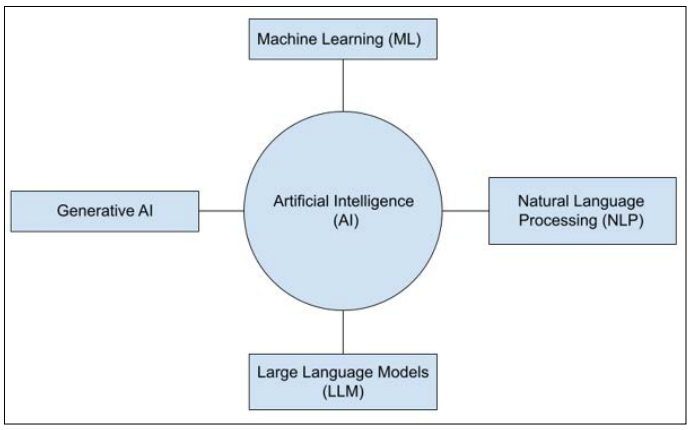

Figure 1: Applications of Artificial Intelligence

User Research

Any technology would be useful if it is applied to solve human problems. The user-centric approach to design involves understanding business and user needs. For this study, we interviewed 5 CISOs and 4 security analysts and articulated their goals, needs and challenges:

Cybersecurity professionals have the executive role of Chief Information Security Officer (CISO) who needs faster analysis of data to make informed decisions. CISOs are expected to interpret data represented in the form of dashboard visualizations and present findings to the board team for more budget or to the security operations team for faster remediation and secured posture.

Goals

- Protect the organization's critical assets from adversaries and breaches
- Strengthen the security posture of the company by leveraging advanced insights
- Convey results and impact to board members for buy-in

Needs

- Monitor the security posture of the company holistically and analyze a large amount of data as efficiently as possible
- Prioritize the actions to mitigate the risk
- To be able to slice and dice large volumes of data to make sense of it

Challenges

- Current dashboards and tools don't allow customized analytics based on natural language
- Applying many filters manually and drilling down into pages to find out the exact anomaly
- Time-consuming to go through multiple tools, spread- sheets, slide decks and correlate fragmented data

In essence, modern security teams are confronted with numerous obstacles, including advanced cyberattacks, increasing points of vulnerability, a surge in data volume, and escalating complexity of

infrastructures. These challenges impede their capability to protect data, oversee user access, and promptly identify and address security threats. Consequently, there's a growing demand for revolutionary solutions powered by AI, designed to enhance the efficiency of analysts. These solutions aim to speed up threat identification, hasten response times, and secure user identities and data, all while ensuring that cybersecurity teams remain informed and in control [5].

AI Applications in Cybersecurity

We identified the following general themes that can leverage AI capabilities to assist cybersecurity professionals in working more efficiently and intelligently:

Text-to-Visualization

Popular Generative AI tools like Chat GPT and mid-journey utilize Text-to-text and text-to-image interactions. AI has tremendous potential to empower cybersecurity executives by providing big data analysis at their fingertips. CISOs mentioned that they are used to view dashboard widgets with graphs, charts and various forms of complex data visualizations. Inspired by the mid-journey tool, I envision a text-to- chart use case evolving for more analytical users in which CISOs could type or voice input a query-"show me a pie chart for top 5 Facebook users in the last 7 days" and use Natural Language Processing, the filters will be applied on massive data sets of logs for the last 7 days and interface will show an output with a pie chart within a few seconds. For visibility, we can show filters applied to the dataset so that the user can quickly verify the logic if needed and check if the output matches the expectations or not. It can then preserve the query in the history section for easier recall. We can also show suggestions with commonly used queries similar to popular interfaces [3,6].

Breach Analytics and Prediction

Another interesting example of how a CISO can leverage AI is to predict the likelihood of breaches in the environment. A Breach Analytics dashboard can populate a grid of past breaches and users impacted and protected at each stage of the kill-chains so that a CISO can quickly drill down into the particular breach, and stage and study the anomalous activity at the user level to devise a preventive mitigation plan and perform necessary action preemptively to avoid the risk of a similar threat in the future [6].

Data Auto-Classification

Data breach is probably the most expensive wound organizations face. Data security tools can utilize AI to assist security professionals with auto-classification of the sensitive data into pre-defined categories. Automated filtering of sensitive data would help analysts and executives with a high-level picture of where the data resides, who is using it and what are they doing with it to identify suspicious activity, configure policy, and prevent data loss [6].

Multi-Modal Data Protection

Another application of AI for data protection is leveraging not just text but also image, video and code analytics capabilities in defining policies. An administrator should be able to define criteria for multi-modal data protection. This will be powerful and expand the capabilities of data Security [6].

Natural Language-Based Querying

Large log tables with billions of data records are difficult and tedious to analyze by applying manual filters one by one. Even writing a RegX query can be challenging for some users. Natural language-based querying can solve this problem by delivering results with efficiency and accuracy. Users can either type the query or they can input it by voice-to-text interaction. Moreover, some patterns could be identified in the filtered information with the help of machine learning [5,6].

Help Assistant

AI-based assistants are very common in customer support UIs. Cybersecurity products can replicate similar patterns for live support to CISOs and their teams within the security product interface. Based on natural language, a chatbot can answer questions related to usability and product documentation that can improve the overall user experience of the product [6,8].

LLM Based Reports

Massive cybersecurity maturity reports and regulatory compliance reports can be generated with the help of Large Language Models. It can be delivered as a periodic report for executives to help them present the findings in board meetings. This report can summarize top security priorities for the customers and their holistic risk posture. The reports can be in pdf or slides format for ease of use [6].

Implications in User Experience Design

Chatbot is not the solution to every use case. Designers should understand the information flow and intent when it comes to designing user-centered interfaces for AI systems. Based on the research and the above potential AI in cybersecurity use cases we derived two broader UI patterns for interface designers.

These could be classified into two categories:

System-Generated UI

These can include AI-powered, innovative, preset widgets, visualizations, charts, reports, recommendations and insights curated for users without relying on their inputs. Instead, traditional AI in the background can analyze user behaviors and preferences to provide insights through Adaptive User Interfaces (AUIs) [9]. In this case, users can have a personalized experience but with limited control.

User-Input-Based UI

This category includes AI assistants, chatbots and natural language-based querying that take multimodal user inputs to generate customized output. This experience can evoke the sense of real-time assistance however it still puts the onus on the user to switch their context, draft a good prompt and figure out how to use the generated response in their work.

Future of AI, Cybersecurity and UX

As we advance into the future, the integration of AI in cybersecurity is set to deepen, bringing transformative changes. Predictive analytics and AI's ability to proactively identify and mitigate potential threats will significantly enhance cybersecurity measures. This shift towards anticipatory defense mechanisms will be complemented by AI's proficiency in ensuring compliance with evolving data privacy and cyber regulations, streamlining governance processes.

User experience (UX) in cybersecurity is poised for a paradigm shift, with an increased emphasis on personalization and user-centric designs. AI-driven interfaces will adapt to individual user behaviors, offering tailored insights and recommendations, thereby making interactions more intuitive and efficient [10]. The integration of multimodal interfaces, including voice and

gesture-based controls, will further simplify user interactions with complex security systems.

Moreover, ethical considerations in AI deployment, such as bias mitigation and privacy concerns, will become paramount. The balance between technological advancement and ethical responsibility will be crucial. As AI systems gain more autonomy in identifying and responding to cybersecurity threats, the role of continuous learning and adaptation will be key in ensuring the effectiveness and relevance of security measures in an ever-evolving digital landscape.

Conclusion

In summary, this paper has highlighted the transformative impact of Artificial Intelligence (AI) on cybersecurity, emphasizing the shift towards more intuitive, efficient, and AI- driven security systems. As cybersecurity challenges grow more complex, AI technologies like Machine Learning, Large Language Models, Natural Language Processing, and Generative AI are crucial in enhancing system capabilities and user experience. The future direction for UX designers in this field is clear: focus on creating user-centric interfaces that are not only technologically advanced but also easy to navigate and responsive to the specific needs of cybersecurity professionals.

Looking ahead, UX designers are poised to play a pivotal role in shaping the interaction between AI and cybersecurity. They are tasked with designing interfaces that seamlessly integrate AI's complex functionalities into user-friendly experiences, ensuring that cybersecurity solutions are accessible and effective for all users, regardless of their technical expertise. As AI continues to evolve, staying attuned to ethical considerations, user feedback, and emerging trends will be essential for UX designers in crafting the next generation of cybersecurity tools.

References

1. Shanthi RR, Sasi NK, Gouthaman P (2023) A New Era of Cyber- security: The Influence of Artificial Intelligence 2023 International Conference on Networking and Communications (ICNWC), Chennai, India 1-4.
2. Zeadally S, Adi E, Baig Z, Khan IA (2020) Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE Access 8: 23817-23837.
3. Artificial Intelligence (2023) IBM Design for AI https://www.ibm.com/design/ai/basics/ai.
4. Ansari M, Dash B, Sharma P, Yathiraju N (2022) The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. Int J Adv Res Comput 11.
5. Muppidi S, Fisher L, Parham G (2022) AI and automation for Cybersecurity. IBM https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-cybersecurity.
6. Zscaler Blog (2023) Zscaler https://www.zscaler.com/blogs.
7. Transforming Businesses with Artificial Intelligence (2023) Cisco https://www.cisco.com/c/dam/en/us/solutions/collateral/digital- transformation/ai-whitepaper.pdf.
8. Patel J (2023) How We're Making AI Pervasive in the Cisco Security Cloud. Cisco https://blogs.cisco.com/news/how-were-making-ai-pervasive-in-the-cisco-security-cloud.
9. Zimmerman J, Oh C, Yildirim N, Kass A, Tung T, et al. (2021) UX designers pushing AI in the enterprise: a case for adaptive UIs. Interactions 28: 72-77.
10. Hofstetter M, Riedl R, Gees T, Koumpis A, Schaberreiter T (2020) Applications of AI in cybersecurity. 2020 Second International Conference on Transdisciplinary AI (TransAI), Irvine, CA, USA 138-141.