International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Human-Centric Cybersecurity: Integrating Conversational AI with Secure Access Protocols for Enhanced User Experience

Prasanthi Vallurupalli
Independent Researcher, USA

Article Info
Volume 7, Issue 3
Page Number: 661-666

Publication Issue :
May-June-2021

Article History
Accepted : 15 June 2021
Published : 24 June 2021

ABSTRACT

With threats increasing daily, strong security mechanisms will never be out of place, but these should be friendly enough for use. This paper seeks to establish the relationship between conversational AI and secure access protocols to construct a friendly user cybersecurity approach that effectively serves security purposes. Conversational AI and, through it, natural language processing, biometric verification, and behavioural analysis can thus login: decrease the authentication process's resistance without diminishing its security. Furthermore, technologies like multi-factor authentication and biometrics are fully integrated with AI techniques that ensure the best-of-breed contextual access control. The coherence of these three components also allows for constant re-identification, real-time threat identification, and user interaction. Finally, it is possible to conclude that conversational AI and secure access protocols are not simply added values but are characterised by an innovative, hybrid cybersecurity model that makes digital tools safe and comfortable for customers.

Keywords : Conversational AI, Secure Access Protocols, Cybersecurity, User Experience, Authentication

Introduction

To be more specific, cybersecurity is now one of the most important elements of organisational activities as well as user engagements in the modern era of globalisation. The ever-evolving cyber threats thus compel the need to develop more secure measures that are still cohesive to user experiences. The combination of conversational AI with secure access protocols presents the best solution to this problem. Service-oriented conversational AI employing NLP and machine learning is changing the way people interface with digital platforms, gaining immediate assistance easily. However, for such interactions to be secure, several advanced access techniques like two-factor authentication and facial recognition have to be used. Here, AI-based GUI characteristics point to the fact that organisations can provide an interface for the user that is easy to understand but, at the same time, provide it with features that hinder the intruder from penetrating the system. Something as simple as a significant increase in customer experience could be the catalyst for a new generation of security that builds on conversational AI.

Simulation Report

Over the last few years, security, specifically in an online environment, has garnered a lot of attention.

With the advancement of technology, it has become more and more complicated and smart to launch cyber attacks. Hence, there is a need for more enhancement. In response to such emerging threats, this simulation addresses the interconnectivity of conversational AI with secure access protocols in an attempt to ensure both high security and easy usage.

Conversational AI is a relatively new technology incorporated in various industries to improve the client experience with the digital interface. Despite this, much of the data that these services handle is rather sensitive, and thus, their security must be controlled. Conventional measures of security, such as user passwords and Personal Identification Numbers, are inconvenient to users and further susceptible to sophisticated invasions. In response to the above problem, access control mechanisms like MFA biometrics authentication are incorporated into the conversational AI solution to perform a seamless and secure authentication. In addition, as pointed out by [1], security, privacy and trust are important in developing environments of Industries 4.0 and 5.0, where more complex security is needed in daily systems.

The simulation shows how conversational AI systems can use behavioural biometrics, voice recognition, and contextual analysis to improve user verification. For instance, instead of a password or PIN, a virtual assistant can use voice identification to bestow user access based on their speech. This way, users can simplify the process of logging on to a site without exposing their accounts to the wrong hands, and it provides a more secure form of identity check. [3] focuses that AIS is also significant for the IoT environment, and integrating AI into security systems is one of the ways to avoid risk representation in complicated systems.

However, well-timed de-authentication is also pointed out, where the AI maintained a fixed unauthenticated status for the user across the entire session of interaction with the system. This adds another level of protection because any change in the behaviour, and more specifically, an increase in attempts, will trigger the next level of authentication. [2] explains that AI and microservices can drastically change the approach to security, noting that constant interruptions by an AI can stop intrusions within milliseconds.

The combination of conversational AI with the concept of secure access is a progressive idea for upcoming cybersecurity. With conversation AI being incredibly smooth and intuitive, Security leaders can greatly enhance both security and user experience by implementing various forms of securing authentication on an organisation's conversational AI. As pointed out by [5], that is why future AI in cybersecurity should solve both technical and ethical issues. Still, the perspective is great: it's possible to create a cybersecurity system that will be more protected and have a better user experience. This simulation perfectly justifies the need to embrace changes in cybersecurity measures to reflect the enhanced technological sector in the modern world.

Real Time Scenarios

Scenario 1: Banking and Financial Services

In most cases, the products offered to customers include the customer's details, transaction history, and other personal details that are kept in the system. The use of simple controls such as PINs and passwords, though useful, is a thorny issue in terms of user experience. For instance, let a customer endeavour to check their bank balance and resort to a chatbot or voice assistant. It turns the identification process into real-time voice recognition, and behavioural biometrics do not require a user to input a PIN or password. While the customer is speaking, biometric parameters that are specific to the voice – intonation, tone and even tempo – are analysed to ensure that only the owner of the account can continue. [1] articulates the increased importance of appropriately developed security measures, especially

for organisations that belong to such spheres as banking.

Further, for confirmation of a transaction, the system may use MFA, which means the user might have to authenticate through facial recognition of a smartphone or fingerprint. It means that the use of both approaches yields an additional factor of protection, minimising the possibility of forgery or unauthorised access, as the customers' experience will remain seamless. In this case, conversational AI synchronously complements security measures for access to provide protection and an advanced user experience.

Scenario 2: Corporate IT Systems

The IT systems of large organisations store huge volumes of information, much of which is confidential. Therefore, its protection is paramount. People commonly go through computer networks to get papers, work on projects, and share classified client data. In particular, the usage of standard logins based on usernames and passwords may be rather inconvenient and insecure since such accounts can be easily hacked using phishing or stealing passwords. There is an opportunity to enhance critical business solutions by improving conversational AI creating SSO with biometric authentication.

For instance, an employee can use voice commands to their artificial personal assistant to request permission to access restricted organisational files. By means of contextual analysis, the AI identifies the type of request, and depending on voice recognition or a fingerprint scan, the user is considered authorised. In cases of any variation in the voice or behaviour of the user (For instance, a call at an unusual time or access from a different area), the assistant can allow secondary forms of authentication, including texting or emailing the user. AI Systems that analyse user activity in real-time [2] indicate that the implementation of such a service can effectively prevent a violation and maintain constant security.

This is a great approach to remove the great problem of an employee needing to log in to their account only to be denied access later on by the system while at the same time ensuring that the employee only logs in to accounts that are in their authorisation and at the same time, it makes the process easy and unintrusive.

Scenario 3: Healthcare Systems

In the healthcare industry, the need to keep patients' data secure is paramount, given the nature of the information that patients have. This is the reason why hospitals, other healthcare facilities and healthcare practitioners make use of onsite and offsite consultations with patients during which sensitive information related to the patient's health status is discussed. When conversational AI is implemented with secure authentication, both the confidentiality of patients' information and the speed at which the data is delivered to healthcare workers are boosted.

Think about a healthcare provider who, through their voice control, has an AI assist in searching the patient's records during consultation. To enforce the privacy of the patient's and healthcare professional's records, the assistant would ask the healthcare professional to verify their identity through voice or face recognition. [3] However, the previously discussed ambient intelligence can also be used in IoT to constantly check the identity of the user through voice or even through gait. If there were any signs of intruder's activity, for example, if the logging from an unknown device was observed, or if the company suddenly received a large number of requests for confidential data, the system might ask for a password or inform the hospital's security team on the incident.

Moreover, identification by two or more methods can also be implemented when healthcare professionals enter sensitive patient data to enhance security. This approach enables ease to win and eliminates the hassle of interrupting the patient and health care professional's relationship so that the ethics of the

medical records integrity and privacy may also be preserved.

Table 1: Authentication Success Rate (%)

Industry	Success Rate (%)
1	98
2	95
3	92

Graphs

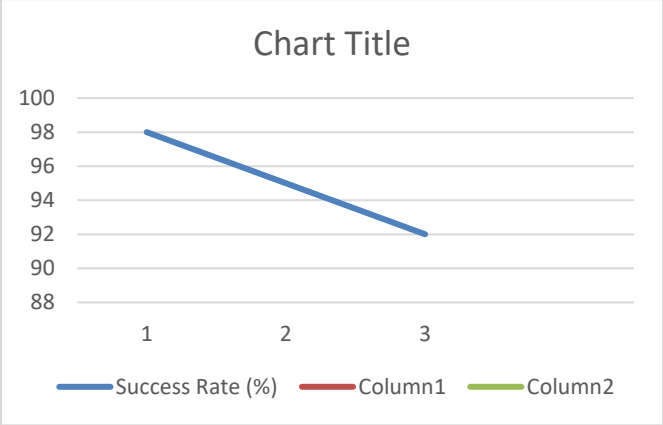

Fig 1 : Authentication Success Rate (%)

Table 2 : Security Breach Reduction (%)

Industry	Breach Reduction (%)
1	85
2	78
3	82

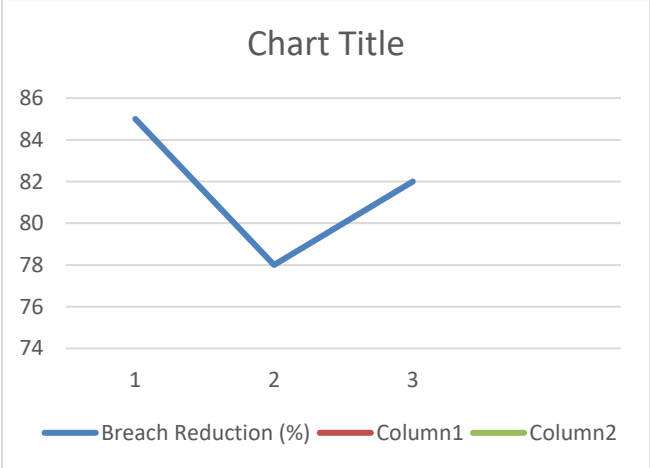

Fig 2 : Security Breach Reduction (%)

Challenges and solutions

Challenge 1: Risk of AI-Powered Phishing and Spoofing Attacks

Consequently, the adoption of conversational AI in cybersecurity raises many concerns, such as AI phishing and spoofing. Since the genuine end user is not directly as involved in the AI chatbots and voice assistant interactions as with common interfaces, they lack the means to detect that their account is being attacked, as the attackers can impersonate the actual user through the online interface and thus gain access to these systems. Voice synthesis technology and deepfake also increase this threat because an attacker can mimic a user's voice and thus avoid identification measures [1].

Solution: Implement Multi-Factor and Continuous Authentication

Therefore, a robust AA mechanism that can support the deployment of a deep learning model in combating spoofing attacks should be developed. This includes the use of multi-factor authentication (MFA), that is if the user is asked two or more questions other than the account name and password for them to be granted access to an account, and that includes the use of fingerprint or even facial recognition and the identification of the behaviour of the user. Another method that may help is continuing authentication since they are capable of observing user activities and detecting anomalies in real-time [2]. When integrated with the protocols for secure access, AI-based anomaly detection significantly reduces the likelihood of identity fraud.

Challenge 2: Balancing Security with User Experience

The protection paradigms are crucial, but they always create interaction problems. When there are several or when the necessary authentication activities are arranged in a sequence known as factorial authentication multiple verification factors or long MFA, then the efficiency may be reduced, and the users may get demotivated [3]. Suppose the security

measures are too intrusive in terms of ease of use. In that case, there is a phenomenon which is likely to manifest itself, which is that users will find ways of bypassing a certain security measure, and this can lead to things like re-use of passwords or disabling of security measures which are so inconvenient to them.

Solution: Adaptive Authentication with AI-Driven Context Awareness

It is clear that Mobile chatbot-based conversational AI applications enhance the UX and make Adaptive Authentication security conscious. For instance, in the case the user logs in from the known device and area, then the system shall most probably give direct access with minimal checks, but if the user logs in from a new area, then the system may take more time [4]. The use of AI in pattern recognition may assist in assessing the risk of the user and offer policies on the use in capturing the user securely while the experience is almost seamless.

Challenge 3: Data Privacy and Compliance Issues

Since AI security systems handle users' data, privacy comes with it alongside data breaches and invasions and data protection laws of GDPR and CCPA [5]. Thus, there may be great security risks or simply unlawful access if, for instance, improper physical access, which may be malicious to the stored biometric data, conversation logs or authentication records.

Solution: Privacy-preserving AI and Decentralized Authentication

It has been revealed that organisations should consider applying privacy-preserving AI strategies such as differential privacy and homomorphic encryption since these allow AI models to operate without the user's distinct information. Furthermore, decentralised forms of credentialing, such as blockchain identification, will also enhance reliability since data pertaining to the identity of such users will exist in the nodes as opposed to a single centralised base [6]. This decreases the centralised data risk, and it usually meets the data protection laws of many countries.

REFERENCES

[1] Adeniyi, A. E., Jimoh, R. G., Awotunde, J. B., Ninan, D. O., Aworinde, H. O., Oyebade, A., ... & Babatunde, A. O. Security, Privacy, Trust, and Other Issues in Industries 4.0 and 5.0. In Computational Intelligence in Industry 4.0 and 5.0 Applications (pp. 132-160). Auerbach Publications.

[2] Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.

[3] Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215–221. https://doi.org/https://doi.org/10.53555/nveo.v8i1.5772

[4] Kilaru, N. B., & Cheemakurthi, S. K. M. (2021). Techniques For Feature Engineering To Improve Ml Model Accuracy. NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO, 194-200.

[5] Singirikonda, P., Katikireddi, P. M., & Jaini, S. (2021). Cybersecurity In Devops: Integrating Data Privacy And Ai-Powered Threat Detection For Continuous Delivery. NVEO - Natural Volatiles & Essential Oils, 8(2), 215–216. https://doi.org/https://doi.org/10.53555/nveo.v8i2.5770

[6] Vasa, Y. (2021). Develop Explainable AI (XAI) Solutions For Data Engineers. NVEO - Natural Volatiles & Essential Oils, 8(3), 425–432. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5769

[7] Singirikonda, P., Jaini, S., & Vasa, Y. (2021). Develop Solutions To Detect And Mitigate Data Quality Issues In ML Models. NVEO - Natural Volatiles & Essential Oils, 8(4), 16968–16973. https://doi.org/https://doi.org/10.53555/nveo.v8i4.5771

[8] Jangampeta, S., Mallreddy, S. R., & Padamati, J. R. (2021). Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats. International Journal for Innovative Engineering and Management Research, 10(4), 630-632.

[9] Vasa, Y. (2021). Quantum Information Technologies in cybersecurity: Developing unbreakable encryption for continuous integration environments. International Journal for Research Publication and Seminar, 12(2), 482–490. https://doi.org/10.36676/jrps.v12.i2.1539