Developing secure text chatting application using ChatGPT-based chatbot

Humesh Reddy Venkatapuram
humeshrv@nmsu.edu
Computer Science Department
New Mexico State University

Pratyay Kumar
pratyay@nmsu.edu
Computer Science Department
New Mexico State University

***Abstract*—This paper examines the critical security considerations for chat applications and chatbot systems, focusing on data encryption and secure communication protocols in network communications. As these platforms become increasingly integrated into our digital lives, protecting user data and ensuring system security are paramount. By adopting a comprehensive approach that encompasses both server-side and client-side components, this paper presents strategies for mitigating security risks and safeguarding sensitive information. Specifically, it discusses the implementation of encryption and secure communication protocols in a SwiftUI-based client-side application, leveraging Apple's cryptographic libraries for robust encryption techniques. Further research is suggested to explore end-to-end encryption solutions and enhance authentication systems to build more resilient chat applications and chatbot systems.**

***Index Terms*—network security, chatting application, chatbot, chatGPT**

I. Introduction

A chatbot is a software application that establishes real-time text-based communication between an artificial intelligence-based chatting bot and an individual. These applications have become indispensable to modern communication, revolutionizing how people interact with technology by assisting various domains and becoming valuable tools for businesses, medical, educational fields, etc. It has become a versatile, user-friendly tool that enhances our everyday lives by automating tasks, providing information, and offering support when needed.

Recent development in Artificial intelligence (AI) has led to significant progress in developing chatbots and chat applications, enabling more natural, context-aware, and emotionally perceptive user interactions. Evolving natural language processing has influenced chatbots to conduct conversations like humans in real-time. One such famous AI-based model is ChatGPT [1], released by Open-AI in November 2022. It has gained recognition for its exceptional ability to engage in human-like conversation, offering users an interactive experience by leveraging natural language processing and machine learning technologies.

ChatGPT has its roots in the field of NLP, an area of AI focused on enabling machines to understand and generate human language [2] [3] [4]. The model is based on OpenAI's GPT architecture, which consists of several layers of transformer blocks that process the input text and generate output text. The model is pre-trained on a vast corpus of text data, enabling it to generate contextually relevant responses to various queries. The model is then fine-tuned using supervised learning techniques on a specific task, ensuring that the model generates high-quality, accurate, informative responses.

ChatGPT has been applied in various domains, including customer service, healthcare, education, and entertainment. Its ability to generate contextually relevant responses and engage users in a human-like conversation has made it an invaluable tool for businesses seeking personalized customer support and educational institutions seeking to enhance student learning experiences.

In conclusion, Chatbots have become indispensable to modern communication, providing valuable tools for various domains. ChatGPT, an AI-based model released by OpenAI, has gained recognition for its exceptional ability to engage in human-like conversation, offering users an interactive experience by leveraging natural language processing and machine learning technologies. The model has the potential to revolutionize how we interact with technology, providing personalized assistance and support when needed.

This paper aims to present a secure chatbot application based on ChatGPT, which provides a reliable and versatile solution for various domains. Our application ensures the privacy and integrity of user data by implementing encryption and secure authentication methods, making it a safe and secure platform for communication. Moreover, our application is user-friendly, reliable, and highly customizable, making it an ideal tool for businesses, healthcare, education, and entertainment. Our ChatGPT-based application leverages natural language processing and machine learning technologies to engage users in human-like conversation, providing personalized assistance and support when needed. Our application's versatility and reliability make it an invaluable tool for various domains, providing users with an interactive and seamless communication experience. This paper presents a practical and reliable ChatGPT-based secure chatbot application, offering new opportunities to enhance modern communication channels and improve user experiences.

II. Related Work

1) "Chatbot for E-Learning: A Case of Study" [5]

The paper presents a case study where a chatbot is developed and integrated into an e-learning platform to enhance students' learning experience. The authors discuss

the design and implementation of the chatbot, highlighting its functionalities, including providing personalized course recommendations, answering student queries, and facilitating interactive learning activities. The paper also evaluates the chatbot's effectiveness in user satisfaction and learning outcomes. The case study results demonstrate the potential of chatbots in e-learning environments to engage and support learners, providing them with timely and relevant assistance. The study contributes to the understanding of how chatbots can be leveraged to improve the effectiveness and efficiency of e-learning platforms.

2) "Chatbots: History, technology, and applications" [6]

The paper traces the evolution of chatbots from early rule-based systems to modern AI-powered chatbots. It explores the technological foundations of chatbots, such as natural language processing, machine learning, and dialogue management. Additionally, the paper discusses the diverse range of applications where chatbots are being deployed, including marketing, customer support, education, healthcare, cultural heritage, and entertainment. It highlights the potential benefits of chatbots in improving user experience, efficiency, and accessibility in these domains. The paper is a comprehensive introduction to chatbots, offering insights into their development, functionality, and practical use cases.

3) "MANDY: Towards a Smart Primary Care Chatbot Application" [7]

The paper addresses the growing need for accessible and efficient healthcare services and explores how chatbots can be leveraged to support primary care. MANDY utilizes natural language processing and machine learning techniques to provide users with personalized healthcare recommendations, symptom assessments, and medical information. The paper discusses the development and implementation of MANDY, highlighting its functionalities, user interaction design, and integration with existing healthcare systems. The evaluation and results of user satisfaction and system performance are also presented. Overall, the paper presents MANDY as a promising approach to enhancing primary care services through intelligent chatbot technology.

4) "A critical review of state-of-the-art chatbot designs and applications" [8]

The paper critically evaluates various aspects of chatbot technology, including natural language processing techniques, dialogue management strategies, and user experience considerations. It examines the strengths and weaknesses of different chatbot architectures and approaches, highlighting their effectiveness in real-world applications across various domains. The paper also discusses challenges and future research directions in improving chatbot designs to enhance user engagement, conversational quality, and overall performance.

5) "Future directions for chatbot research: an interdisciplinary research agenda" [9]

The paper emphasizes the need for interdisciplinary collaboration and highlights the importance of considering various perspectives, including social sciences, computer science, design, and ethics. The authors propose an interdisciplinary research agenda encompassing user experience, trust, transparency, personalization, ethical considerations, and the integration of emerging technologies like AI and machine learning. The paper aims to guide researchers and practitioners in exploring new avenues for chatbot research and development to create more effective, trustworthy, and user-centered chatbot systems.

6) "Chatbot Development for Educational Institute" [10]

This research paper tells that chatbot is a software designed to facilitate natural language conversations between users and computers or systems. It interacts with users, simulating human-like conversations while operating as a computer program. The chatbot application described in the context aims to assist students with college admission processes. By providing information and answering queries about admissions, the chatbot reduces the workload on the admission department. It allows students or parents to access relevant information conveniently from anywhere with an internet connection. This system streamlines the admission process and improves efficiency by automating responses to common queries, thus benefiting both students and the department.

7) "A Review on Implementation Issues of Rule-based Chatbot Systems" [11]

It examines various aspects such as knowledge representation, rule management, user intent recognition, and dialogue flow management. They discuss the limitations of rule-based approaches, including scalability issues, lack of adaptability, and difficulties in handling ambiguous user queries. The paper concludes by highlighting the need for more advanced techniques, such as machine learning and natural language processing, to overcome the limitations of rule-based chatbots and enhance their performance and user experience.

8) "An Overview of Chatbot Technology" [12]

The paper discusses the motivations behind using chatbots and their usefulness in various fields such as marketing, support systems, education, healthcare, cultural heritage, and entertainment. It highlights the impact of social stereotypes on chatbot design and presents a classification of chatbots based on different criteria. The authors have talked about

Rule-based chatbots, which utilize expert-created rules for topic-based response selection, lacking robustness to errors. In contrast, advanced chatbots consider multi-turn conversation context for more human-like response selection. The paper also covers the general architecture of modern chatbots and mentions the main platforms for their creation. Overall, the authors express optimism about the prospects of chatbots and emphasize the need for further in-depth research in the field.

The aforementioned literature provides a comprehensive overview of the current utilization of chatbot applications across a wide range of domains, examining the extensive body of research work and in-depth surveys on existing chatbot systems. These applications have been employed in numerous fields, including but not limited to customer service, healthcare, education, entertainment, and finance, demonstrating their versatility and adaptability. The review highlights the innovative approaches developed to enhance the capabilities of chatbots, as well as the potential challenges and limitations accompanying their implementation. By analyzing the practical applications and theoretical underpinnings of chatbot technology, this literature is a valuable resource for researchers, practitioners, and stakeholders interested in understanding the landscape of chatbot systems and their potential to revolutionize various aspects of our lives.

The existing chatbot applications use traditional rule-based chatbots that follow predefined rules, scripts, or decision trees to interact with users. While these chatbots can effectively handle specific tasks and scenarios, they possess limitations, such as Flexibility, Scalability, Language Understanding, Personalized response, Handling Ambiguity, etc.

To our knowledge, no existing chat application leverages cutting-edge Chat-GPT-based chatbot technology. This realization motivated us to develop a chat application incorporating Chat-GPT and implementing various network security aspects. The aim is to create a comprehensive, secure, singular chat application that stands out in the current market.

III. Methodology

This section will discuss the conversational chatbot we build using Swift-UI and Chat-GPT.

First, we have employed the OpenAiSwift library [13] with the Suift-UI [14] incorporating the cutting-edge chat-GPT to facilitate natural and interactive conversations with users. This model is seamlessly integrated with responsive and user-friendly IOS mobile applications, providing an unparalleled user experience. To ensure the highest level of security, we have implemented network security measures to safeguard the exchange of information between the user and the ChatGPT/OpenAI-based chatbot.

The methodology encompasses several stages and additional details:

1) **Secure communication:** Ensuring the security and privacy of user data is a crucial concern. To achieve this, we have implemented various security measures in the ChatGPT/OpenAI backend to protect user information during transmission. One of the key measures we have put in place is message encryption using a secure HTTP header of messages exchanged between the user interface and our backend. This encryption mechanism ensures that any sensitive data sent by the user and the response received from the chatbot are both encrypted and secure, preventing unauthorized access to the user's private information. In addition to encryption, we employ secure authentication methods to ensure that only authorized users can access the chatbot. This adds an additional layer of security to our platform, ensuring user data is protected from potential security breaches.
2) **Obtaining context-aware responses:** Chatbot applications, leveraging the sophisticated natural language understanding and generation capabilities of models like ChatGPT, have transformed the landscape of human-computer interactions by facilitating more engaging and human-like conversational experiences. These advanced models, built on large-scale pre-trained neural networks, effectively process and generate contextually appropriate responses by analyzing user inputs, detecting underlying meaning and intent, and utilizing their vast knowledge base to provide accurate and relevant information. Consequently, this has led to a broad range of practical applications for chatbots, including customer service, healthcare, e-commerce, and virtual assistants. Integrating advanced machine learning algorithms with pre-trained models allows chatbots to adapt and respond to diverse user inputs, fostering meaningful interactions and personalized experiences.
3) **Response refinement:** The responses generated by the ChatGPT model are subject to further refinement to align with the application's unique requirements, ensuring that the conversational output maintains coherence, relevance, and adherence to the desired conversational style. By implementing post-processing techniques, developers can enhance the chatbot's performance, customizing and tailoring its responses to better suit user preferences, predefined use cases, and specific scenarios. Additionally, these techniques can filter sensitive content and ensure compliance with various regulations, further improving the user experience and promoting trust in the application. To optimize the user experience and strike a balance between delivering concise, relevant information and providing comprehensive answers that address user needs and concerns, the chatbot application limits ChatGPT-generated responses to 500 words. This limitation ensures that the chatbot remains an efficient communication tool while covering most user queries in a chat-based environment. By combining the robust natural language understanding and generation capabilities of ChatGPT with an adaptive, contextually-aware response generation system and effective post-processing techniques, chatbot applications can cater to the diverse needs of users, creating engaging and personalized conversational experiences that closely re-

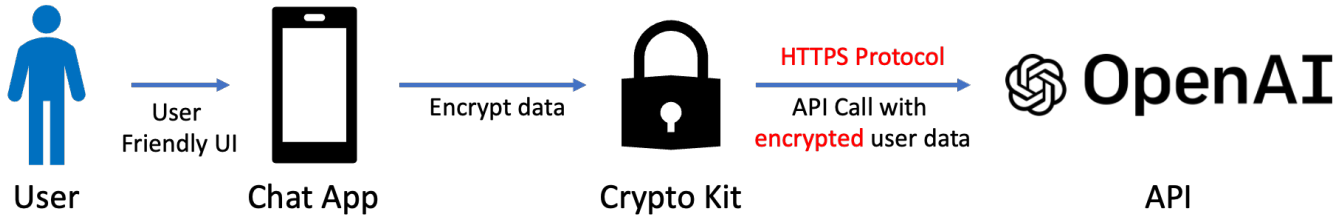

Fig. 1: Work flow

semble human interaction while maintaining the focus on delivering pertinent information and addressing user queries effectively.

4) **Performance optimization:** The chatbot application is designed to optimize response times and minimize latency, ensuring real-time responsiveness and smooth user interactions. By leveraging the capabilities of Apple's SwiftUI framework, the application benefits from its efficient rendering engine, which automatically optimizes the user interface updates and minimizes resource consumption. Furthermore, SwiftUI's declarative syntax allows for concise and easily maintainable code, leading to more efficient algorithms and faster response times. Combined with the inherent performance benefits of Swift as a programming language, this results in a highly responsive and user-friendly chatbot application that maintains seamless communication and interaction with users.

The Swift UI framework enables the creation of visually appealing, accessible, and user-friendly interfaces, ensuring consistency and functionality across various platforms. The OpenAI robust and efficient networking framework facilitates secure connections between the Swift UI-based interface and the ChatGPT backend.

A. Client side security concerning network

Client-side security is a crucial aspect of chatbot applications, as it ensures the protection of user data and maintains privacy. Various client-side security measures can be implemented in chatbot applications to safeguard against potential threats and vulnerabilities. The following we have addressed in our project:

1) **Data Encryption:** Our chatbot application employs Apple's CryptoKit framework to enhance client-side data security through robust encryption techniques. By leveraging symmetric encryption algorithms, such as AES-GCM, the application ensures the confidentiality and integrity of user data. CryptoKit's user-friendly APIs make it easy to implement encryption, decryption, and secure key management processes. The seamless integration of this powerful framework with SwiftUI provides an efficient and secure communication channel between the client and server without compromising the user experience. This comprehensive approach to data security plays a crucial role in maintaining the trust and privacy of users interacting with the chatbot application, making it suitable for handling sensitive information and complex queries.
2) **Secure Communication:** In this project, we have established a secure communication channel using the HTTPS protocol, which encrypts data transmitted between the client and server. This added layer of security prevents unauthorized access and data interception by malicious third parties. In the provided code, the OpenAISwift client communicates with the server through an HTTPS connection, ensuring the user's encrypted data remains protected during transmission; combining the client-side encryption provided by CryptoKit with the secure communication offered by HTTPS results in a robust security infrastructure for the chatbot application, further safeguarding user data and enhancing overall trust in the system.

The chatbot application's client-side security has been significantly enhanced by incorporating data encryption using Apple's CryptoKit framework and establishing secure communication through the HTTPS protocol. These measures protect user data and preserve privacy during chatbot interactions. The seamless integration of encryption, decryption, and key management processes, along with the use of secure communication channels, demonstrates trust and security for the user. As a result, the chatbot application is better equipped to handle sensitive information and complex queries, providing users with a safe and enjoyable conversational experience.

B. Working

The proposed secure chat application workflow, as shown in the figure 1 involves four main components: User, Chat App, Crypto Kit, and API. This workflow ensures user messages are encrypted and securely transmitted to the OpenAI server using the HTTPS protocol.

1) The process begins with the user accessing the user-friendly chat application on their device. The user interface is designed to provide an intuitive and straightforward experience, allowing users to easily compose and send messages within the chat platform. As shown in 2 you can see, the UI is very simple and easy to use.
2) Once the user composes their message, the chat application acts as the intermediary between the user and the encryption process. The primary responsibility of

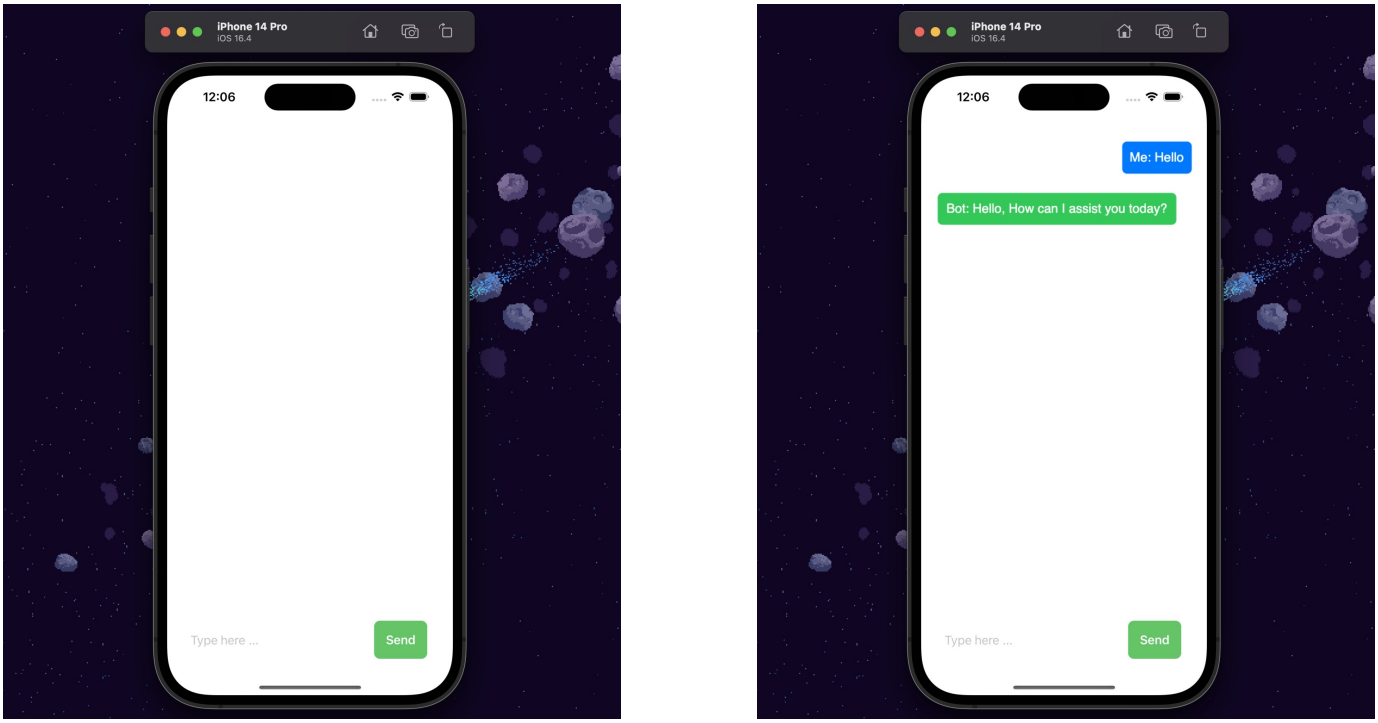

Fig. 2: Chat Application Demonstration

the chat app is to facilitate the process of message encryption and secure transmission.

3) After the user submits their message, it is passed to the Crypto Kit, which encrypts the message content. Crypto Kit [15] is a cryptographic library provided by Apple that offers various encryption and decryption techniques. In this workflow, the chat application utilizes Crypto Kit to encrypt the user's message using an appropriate encryption algorithm, such as AES (Advanced Encryption Standard). This process ensures that the message content is unreadable and secure, even if it were to be intercepted during transmission.
4) With the message encrypted, the chat application proceeds to transmit the encrypted message to the OpenAI server using a secure API. This transmission is done through the HTTPS protocol, which extends the HTTP protocol with added security features. HTTPS ensures that the data transmitted between the client (chat application) and the server (OpenAI) is confidential and has not been tampered with during transmission.

Upon receiving the encrypted message packets, the OpenAI server decrypts the message using its corresponding decryption algorithm and processes the message accordingly. The server then sends an encrypted response back to our chat application, which is then decrypted and displayed on the user interface.

IV. Conclusion

In conclusion, the rapid integration of chat applications and chatbot systems into our digital lives has made it increasingly important to prioritize user data protection and system security. By adopting a comprehensive approach encompassing server-side and client-side components, we have discussed the implementation of encryption and secure communication protocols in a SwiftUI-based client-side application.

In light of the presented features comparison in Table I, our Chatbot offers significant advantages over basic chatbots regarding natural language understanding, scalability, scope, and adaptability. By leveraging advanced Chat-GPT-based technology, our chatbot can understand context and intent better than traditional keyword-based approaches. This allows it to provide more accurate and relevant responses, even when faced with complex or ambiguous user queries.

Moreover, the multi-level inheritance hierarchy and the ability of the chatbot to self-improve over time contribute to a highly scalable and adaptable solution. This translates to a chatbot that can efficiently handle various topics and evolve alongside the ever-changing needs of users, organizations, and the market landscape.

Additionally, our chatbot excels in entity extraction and multilingual capabilities, enhancing its ability to provide personalized and contextually relevant interactions. Furthermore, by incorporating user authentication and robust privacy and security measures, our chatbot ensures that user data remains secure throughout the communication.

In future developments, incorporating end-to-end encryption into this chat application could be a valuable addition, significantly enhancing the network security aspects of the communication platform. By ensuring that the messages exchanged between users are encrypted from the sender's device to the recipient's device, end-to-end encryption adds an extra layer

TABLE I: Features over other chatbots

Features	**Basic Chatbot**	**Our Chatbot**
Natural language understanding	Key-word based tech	Yes
Multi-Level inheritance hierarchy	If/Then statement	Yes
Unlimited scalability	Limited improvement capacity	Yes
Broad Scope	Narrow Scope	Yes
Self-improving over time	No	Yes
Entity Extraction	No	Yes
User authentication	No	Yes
Multilingual	No	Yes
Privacy & Security	No	Yes

of protection against potential data breaches or interception. This increased security measure would protect users' privacy and sensitive information more effectively and contribute to building greater user trust in the chat application.

REFERENCES

[1] Robert W McGee. Is chat gpt biased against conservatives? an empirical study. *An Empirical Study (February 15, 2023)*, 2023.

[2] Chenfei Wu, Shengming Yin, Weizhen Qi, Xiaodong Wang, Zecheng Tang, and Nan Duan. Visual chatgpt: Talking, drawing and editing with visual foundation models. *arXiv preprint arXiv:2303.04671*, 2023.

[3] Yejin Bang, Samuel Cahyawijaya, Nayeon Lee, Wenliang Dai, Dan Su, Bryan Wilie, Holy Lovenia, Ziwei Ji, Tiezheng Yu, Willy Chung, et al. A multitask, multilingual, multimodal evaluation of chatgpt on reasoning, hallucination, and interactivity. *arXiv preprint arXiv:2302.04023*, 2023.

[4] Som Biswas. Chatgpt and the future of medical writing, 2023.

[5] Francesco Colace, Massimo De Santo, Marco Lombardi, Francesco Pascale, Antonio Pietrosanto, and Saverio Lemma. Chatbot for e-learning: A case of study. *International Journal of Mechanical Engineering and Robotics Research*, 7(5):528–533, 2018.

[6] Eleni Adamopoulou and Lefteris Moussiades. Chatbots: History, technology, and applications. *Machine Learning with Applications*, 2:100006, 2020.

[7] Lin Ni, Chenhao Lu, Niu Liu, and Jiamou Liu. Mandy: Towards a smart primary care chatbot application. In *Knowledge and Systems Sciences: 18th International Symposium, KSS 2017, Bangkok, Thailand, November 17–19, 2017, Proceedings 18*, pages 38–52. Springer, 2017.

[8] Bei Luo, Raymond YK Lau, Chunping Li, and Yain-Whar Si. A critical review of state-of-the-art chatbot designs and applications. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 12(1):e1434, 2022.

[9] Asbjørn Følstad, Theo Araujo, Effie Lai-Chong Law, Petter Bae Brandtzaeg, Symeon Papadopoulos, Lea Reis, Marcos Baez, Guy Laban, Patrick McAllister, Carolin Ischen, et al. Future directions for chatbot research: an interdisciplinary research agenda. *Computing*, 103(12):2915–2942, 2021.

[10] Kshitija Shingte, Anuja Chaudhari, Aditee Patil, Anushree Chaudhari, and Sharmishta Desai. Chatbot development for educational institute. *Available at SSRN 3861241*, 2021.

[11] Sandeep A Thorat and Vishakha Jadhav. A review on implementation issues of rule-based chatbot systems. In *Proceedings of the international conference on innovative computing & communications (ICICC)*, 2020.

[12] Eleni Adamopoulou and Lefteris Moussiades. An overview of chatbot technology. In *Artificial Intelligence Applications and Innovations: 16th IFIP WG 12.5 International Conference, AIAI 2020, Neos Marmaras, Greece, June 5–7, 2020, Proceedings, Part II 16*, pages 373–383. Springer, 2020.

[13] Adam Rush. Openaiswift. https://github.com/adamrushy/OpenAISwift, 2021. GitHub repository.

[14] Apple Inc. Swiftui. https://developer.apple.com/xcode/swiftui/, n.d. Retrieved May 9, 2023.

[15] Apple Inc. CryptoKit. https://developer.apple.com/documentation/cryptokit, n.d. Accessed May 10, 2023.