MINISTERUL EDUCAŢIEI, CULTURII ŞI CERCETĂRII

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef de departament:
Fiodorov Ion dr., conf. univ.

„___” ____ *2024*

SISTEM AUTOMAT DE AVERTIZARE PENTRU UTILIZATORII VULNERABILI ÎN MEDIUL DIGITAL
AUTOMATED WARNING SYSTEM FOR VULNERABLE USERS IN THE DIGITAL ENVIRONMENT

Teză de master

Student: _____ **Ciocanu Carolina, IS-221**

Coordonator: _____ **Mariana Catruc, lector univ.**

Chişinău, 2024

REZUMAT

Lucrarea prezintă un proiect complex axat pe îmbunătățirea securității utilizatorilor în mediul digital prin implementarea unui sistem automatizat de avertizare. În primul capitol, s-a efectuat o analiză detaliată a domeniului securității în interacțiunile digitale. S-au identificat amenințările frecvente și vulnerabilitățile existente, evidențiind necesitatea unei soluții inovatoare și eficiente.

În al doilea capitol, s-a realizat o evaluare a soluțiilor bazate pe inteligența artificială pentru a spori securitatea utilizatorilor. S-au analizat diverse tehnologii AI, precum analiza comportamentală, detecția de anomalii și învățarea automată, pentru a identifica cele mai potrivite metode de prevenire a atacurilor și îmbunătățirea detecției acestora.

În cel de-al treilea capitol, s-a detaliat procesul de proiectare și implementare a sistemului automatizat de avertizare. S-au conturat cerințele funcționale și tehnice, iar apoi s-a trecut la dezvoltarea și implementarea efectivă a soluției. Integrarea inteligenței artificiale în arhitectura sistemului a fost esențială pentru atingerea obiectivelor propuse.

Astfel, prin aceste etape fundamentale, proiectul a vizat crearea unui sistem coerent și eficient, capabil să ofere avertizări rapide și precise în cazul unor potențiale amenințări la adresa securității utilizatorilor în mediul digital. Implementarea acestui sistem reprezintă o măsură proactivă pentru contracararea amenințărilor cibernetice și îmbunătățirea experienței utilizatorilor în interacțiunile lor online.

Capitolul 1: Analiza domeniului securității în interacțiunile digitale. Aprofundarea în complexitatea securității interacțiunii digitale, explorarea amenințărilor și contramăsurilor.

Capitolul 2: Evaluarea soluțiilor AI pentru îmbunătățirea securității utilizatorilor. Evaluarea eficacității soluțiilor AI în îmbunătățirea securității utilizatorilor și atenuarea riscurilor cibernetice.

Capitolul 3: Proiectarea și implementarea sistemului. Principii directoare și considerații practice în proiectarea și implementarea sistemelor de securitate robuste.

ABSTRACT

This paper presents a comprehensive project focused on enhancing user security in the digital environment through the implementation of an automated warning system. In the first chapter, a detailed analysis of the security domain in digital interactions was conducted. Common threats and existing vulnerabilities were identified, emphasizing the need for an innovative and effective solution.

In the second chapter, an evaluation of artificial intelligence (AI) solutions was carried out to augment user security. Various AI technologies, such as behavioral analysis, anomaly detection, and machine learning, were examined to identify the most suitable methods for preventing attacks and improving detection capabilities.

The third chapter outlined the design and implementation process of the automated warning system. Functional and technical requirements were defined, followed by the actual development and implementation of the solution. The integration of artificial intelligence into the system architecture was crucial to achieving the proposed objectives.

Through these fundamental stages, the project aimed to create a coherent and efficient system capable of providing rapid and accurate warnings in the event of potential threats to user security in the digital environment. The implementation of this system represents a proactive measure to counteract cyber threats and enhance the user experience in their online interactions.

Chapter 1: Analysis of the field of security in digital interactions. Delving into the intricacies of digital interaction security, exploring threats and countermeasures.

Chapter 2: Evaluation of AI solutions to improve user security. Assessing the effectiveness of AI solutions in enhancing user security and mitigating cyber risks.

Chapter 3: System design and implementation. Guiding principles and practical considerations in the design and implementation of robust security systems.

Contents:

Introduction 5

1 Analysis of the field of security in digital interactions 7

1.1 Evaluation of the security of digital interaction 7

1.2 Analysis of users' security needs 9

1.3 Assessing user perceptions for AI Integration in daily digital interactions 13

2 Evaluation of AI solutions to improve user security 16

2.1 Exploring AI solutions 21

2.2 Study of existing analog solutions 22

2.3 Analysis of Natural Language Processing 28

3 System design and implementation 39

3.1 System Design 41

3.2 Functional and nonfunctional requirements 42

3.3 Vader sentiment analysis 44

3.4 System Implementation in the chats 48

Conclusions 51

Bibliography 52

Annexes 53

Annexe 1. Vader Sentiment implementation in Chat 53

Annexe 2 – Email warning Code 54

Anexe 3 – User Interface 55

Anexe 4 – Firebase storage 57

Anexe 5 – Chat page code with vader implementation 58

Introduction

In our contemporary interconnected world, the ubiquity of digital interactions has seamlessly woven into the fabric of our daily lives. As users increasingly engage in online transactions, participate in social media activities, utilize cloud-based services, and collaborate remotely, the paramount concern that looms large is the security of these digital interactions. While these advancements bring unprecedented convenience, they also usher in a landscape fraught with challenges, including cybersecurity threats, privacy breaches, and vulnerabilities in data protection.

The urgency to safeguard users in the realm of digital interactions is underscored by the evolving nature of threats. Cybercriminals and malicious actors continually adapt, employing new tactics that pose escalating risks to both individuals and organizations. Addressing these challenges proactively becomes imperative to uphold the privacy, integrity, and availability of digital interactions. In response to this imperative, the integration of artificial intelligence (AI) has emerged as a potent strategy. AI-driven solutions possess the capability to fortify user security by identifying anomalies, thwarting fraud, and mitigating risks in real-time. By harnessing the power of machine learning, natural language processing, and predictive analytics, AI stands poised to revolutionize the protective measures surrounding digital interactions.

The enhancement of user security through AI-driven solutions is a multifaceted undertaking. This encompasses the (Martin 2003) of sophisticated algorithms capable of predicting and thwarting cyberattacks, the creation of intelligent authentication mechanisms ensuring access only to authorized individuals, and the pervasive integration of AI across all dimensions of our digital interactions to provide continuous vigilance and protection.

This thesis represents a comprehensive exploration of the domain of user security in digital interactions, with a specific focus on leveraging AI-driven solutions to bolster security measures. The objective is to conduct an in-depth analysis of the current digital security landscape, assess existing AI-powered solutions through a comparative lens, and synthesize data to propose actionable recommendations for cultivating a more secure digital future. Furthermore, as the digital landscape evolves, the complexity of potential security threats grows exponentially. This necessitates not only a proactive stance against current challenges but also an anticipatory approach to future risks. The synergy between AI and cybersecurity becomes paramount in developing adaptive defenses that can learn and evolve alongside emerging threats. This thesis delves into the nuances of this evolving landscape, exploring the dynamic interplay between AI innovations and the ever-changing tactics of those seeking to compromise digital security. By shedding light on these intricate dynamics, the aim is to contribute valuable insights to the

ongoing discourse on securing digital interactions, fostering a resilient environment that can withstand the challenges of tomorrow's digital frontier.

Bibliography

1. Anderson, R., & Moore, T. 2009. *Information Security Economics—and Beyond.* Springer.
2. Gamma, E., Helm, R., Johnson, R., & Vlissides, J. 1994. *Design Patterns: Elements of Reusable Object-Oriented Software.* Addison-Wesley.
3. Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. 2016. *Deep Learning.* MIT Press.
4. Liao, Q. V., Knijnenburg, B. P., & Kobsa, A. 2017. "Privacy as a Service: An Interaction-Centric Framework for Privacy Practices in Web Services." *Journal of the Association for Information Science and Technology* 68.
5. Martin, R. C. 2003. *Agile Software Development: Principles, Patterns, and Practices.* Prentice Hall.
6. Moqadam, Amir-Hossein. 2023. "Artificial Intelligence (AI) Models Can Play a Crucial Role." *Artificial Intelligence (AI) Models Can Play a Crucial Role.*, 7 April.
7. Nilesh. 2023. "How is AI Helping to Make the Internet Safer." *medium.com.*
8. Russell, S., & Norvig, P. 2010. *Artificial Intelligence: A Modern Approach.* Prentice Hall.
9. Schneier, B. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* W. W. Norton & Company.
10. Sci., Front. Comput. 2023. "Sec. Human-Media Interaction - Volume 5." *Frontiers.*
11. Sommerville, I. 2011. *"Software Engineering.* Addison-Wesley.
12. Team, Embroker. 2023. *Global Trends and Threats Report 2023.* PhD Thesis, Embroker.