NTNU
Kunnskap for en bedre verden

CybAlliance WP3 Report Joint Supervision, and Guest Tutorials Report 2023

Author:
Lama Amro
Vasileios Gkioulos

November 2023

Executive Summary

The progress and achievements of Work Package WP3 are summarized in this report, which includes the Joint Supervision (T3.2) and the Guest Lectures and Tutorials (T3.3) components. The successful completion of this year's deliverables was made possible by the dedicated efforts put into arranging guest lectures and facilitating international collaboration for co-supervision, all of which have had a positive influence on education.

Contents

1 Introduction

The main objective of Work Package WP3 is to strengthen and make a significant contribution to the field of cyber security and privacy education, with a particular focus on healthcare systems. This report provides a comprehensive overview of the progress and achievements we have made over the past year, emphasizing the dedicated efforts and contributions of our team.

Four tasks have been assigned to Work Package WP3. T3.1 is dedicated to the task of arranging and overseeing two summer schools. No summer school was scheduled for 2023, but it will be in 2024.

T3.2, Join Supervision; **T3.3, Guest Lectures and Tutorials**, and **T3.4, Course Material**, which will be explained in detail in a separate report.

This report focuses on the planning and achievements of the second and third tasks T3.2 and T3.3, in addition to future plans to make sure we achieve the project's objectives. The sections below outline our accomplishments and future objectives.

2 Work Package WP.3.2: Join Supervision

2.1 Overview

This task's goal is to discuss opportunities for joint supervision of Bachelor's, Master's, and Ph.D. students. NR does not offer Master's, or Ph.D. degrees, and OUS has Master's, and Ph.D. but mostly on special healthcare services. However, the vision of CybAlliance is focused on the security and privacy of healthcare. Therefore, NR and OUS will be actively involved in the co-supervision activities by suggesting topics at GUF, UCCS, IMT, and NTNU. The rest of the partners are expected to conduct two joint supervisions of the thesis in any of the mentioned levels.
The work of this task started with each partner providing a list of thesis topics. This list of topics was available for everyone to give all partners the chance to show their interest in any of them. The topics and the suggested partners are as follows:

2.1.1 NR

NR proposed the following topics for co-supervision activities at NTNU.:

- **AI-based Anomaly Detection for 5G-Enabled IoT**
  Thesis abstract: The acceptance of 5G technology depends on its security. 5G introduces new dynamics in terms of network softwarization, network function virtualization (NFV), dynamic network slicing, SDN, and Service customization [3]. While these provide the required functionalities to ensure 5G principles in terms of dynamic configuration, flexibility, scalability, and elasticity [3], they introduce increased attack space [2]causing additional security challenges and complexities in some cases [1], [4]. Therefore, security services must be adapted to meet the resource-constrained nature of the IoT and new 5G dynamics. Thus, there is a need to develop an adaptive anomaly detection approach for security-related data collection, analytics and prediction of incidents and provision of response and mitigation measures autonomously to systematically understand, characterize, quantify, and manage cybersecurity in 5G-enabled IoT. It will apply closed-loop AI techniques in a privacy-preserving manner and adapt to security changes and contexts in the 5G-IoT dynamics and characteristics.
  Thesis objectives:
  - To study related literature review and prepare a short report
  - To test the AI based adaptive anomaly detection for 5G-enabled IoT
  - To compare and benchmark with already developed technique(s)
- **Digital Twin for Cybersecurity in the Healthcare Sector**
  Thesis abstract: Digital Twin offers significant advantages to cybersecurity experts, empowering them to predict risks without entering the

physical world, and to simulate and test cyber-attacks that would otherwise be infeasible to do in the real-time physical environment [[8], [5], and [7]. Therefore, novel and automated methodologies for enhancing cybersecurity in IoT-based healthcare using DT technology. In [6], we have developed a DT-based cybersecurity framework for IoT based healthcare applications which includes contextual computing and simulation technologies for healthcare to forecast and mitigate security threats in real-time. In this master thesis, some of components of the framework will be implemented and tested.
Thesis objectives:

- To study related literature review and prepare a short report
- To implement and test the selected components of the framework in [6]
- To prepare a report based on the results from implementation and testing

2.1.2 UCCS

UCCS proposed the following topics:

- **Cyber Risk Management**
  Thesis objective : To investigate a systematic framework for managing cyber risks to healthcare infrastructures and systems.

- **Privacy-Preserving Data Sharing and Computing**
  Thesis objective : To design and develop a system that can be used by stakeholders to share healthcare data in a privacy-preserving fashion.
  If we can identify competent students who have an interest in pursuing their Thesis/Dissertation research in these topics, with the due amount of funding support, this can lead to not only high-quality publications but also results that could be employed in the real world.

2.1.3 GUF

GUF proposed the following topics:

- **IoT Devices in Smart Homes: A Qualitative Analysis on Security Concerns.**
  Here, health data can be a part of smart home data (smart fitness devices, or smart speakers that process spoken health-related information).
  Thesis objective : Analysis of security concerns in relation to these devices. What concerns are there? Which factors and antecedents influence them? How can such concerns be mitigated using hardware and software solutions?

- **Intelligence anomaly detection in 6G networks**
  The 6G networks will serve as the foundational infrastructure for a smart

and intelligent healthcare system, facilitating the seamless sharing of data among entities and enabling teleoperation, among other functionalities. The integration of smart health applications has the potential to connect and provide benefits to citizens across various verticals. **Thesis objective** : Identify explicit threats that may arise in 6G networks and conduct a comprehensive analysis of security and privacy concerns associated with 6G networks across infrastructure, platforms, applications, apps, and new technologies within our scope. Explore the nature of these concerns, investigate the influencing factors and antecedents, and propose strategies for mitigation using both hardware and software solutions. Additionally, explore intelligent methods for anomaly detection in order to enhance overall network security.

- **Privacy vs. Utility: Synthetic Text Data Generation with ChatGPT for Efficient Privacy-Preserving Training of NLP Models**
  Thesis objective : Study whether ChatGPT or other LLMs can be used to generate synthetic data that can be used instead of personal data. This approach could theoretically also be used and replicated using patient data in the healthcare context.

- **Secure Privacy Sensitive Information (PSI) detection using Secure Multiparty Computation (SMPC)** and **Secure Privacy Sensitive Information (PSI) detection using Homomorphic Encryption (HE)**
  Thesis objective: To develop a method to identify privacy-sensitive information (PSI) using SMPC or HE. Both approaches can also be applied, or tested, for health data, which is defined as special category data under personal data in the GDPR. The goal here is to first identify this data automatically in texts and then anonymize it.

- **A privacy threat analysis of children's data: What is happening and what can parents do?**
  An Exploration of Privacy Nudges in the Realm of Parenting Deceptive Design in Children's Apps: An Automated Analysis of User Reviews.

2.1.4 IMT

IMT proposed the following topics:

- **Cyber Range Virtualization**

- **Generation of Healthcare Topologies**

After a discussion between NTNU and IMT, a decision was made to conduct a joint supervision for two master students with the previously mentioned topics, and with the possibility of hosting them in NTNU Norway later in the process. **Alexandre Grimaldi** and **Julien Ribiollet** are both second-year

master's students at télécom sudParis, and the duration of their theses is 225 hours. Their theses objectives and abstract can be summarized as follows: As cyber incidents increase in number and disruption, cybersecurity competencies represent a need more than ever. In this context, Cyber Range platforms have been proven as an effective tool to train both professional and common users in such competencies. This study presents a comparative analysis of eight Cyber Range platforms, discussing the needed evolution toward next-generation cyber range platforms. The comparative analysis focuses on key aspects such as application domains, methods of experimentation, infrastructure technologies, and topology generation, among others. This study also aims to provide insights into the capabilities and features offered by different Cyber Range platforms and, specifically, network topology generation tools, allowing for informed decision-making when selecting the most suitable solution for specific training and experimentation needs. Additionally, the study considers how the ethical and well-thought use of artificial Intelligence (AI) could enhance the automation processes of Cyber Ranges, whether it acts in scenario randomization or topology generation.

2.2 Future Plan

We will continue to request additional thesis topics and streamline collaboration among partners to accomplish the task's objective. Admittedly, this task has advanced below expectations, with the key reason being that processes and institutional procedures related to student supervision have to be aligned between the partners. We will continue this effort, aiming to improve the outcome of the task in 2024.

3 Work Package WP.3.3: Guest Lectures and Tutorials

3.1 Overview

This task's goal is to organize guest lectures and tutorials for students on Critical Infrastructure Security, Information Security, Dynamic Risk Management, and Privacy-Preserving. Each partner is expected to host lectures and give lectures to a hosting partner. The following is an overview of the lecture that has been done for this task:

- On August 7th, NR hosted Ann-Kristin Lieberknecht from GUF to give a lecture with the **title**: "Supporting Parents in Managing Online Privacy Risks: Learnings from Media Educators" and **Abstract**: Children's digital footprints become visible at a very early age, often with information being gathered even before their birth. Although parents express concerns about their children's personal data, studies have shown that parents themselves often share this data, are not aware of certain privacy risks,

or lack knowledge on how to mitigate them. This presentation provides insights from a qualitative, exploratory study among media educators in Germany. The purpose of the study is to identify current knowledge, obstacles, and techniques for engaging parents in privacy education, as well as to analyse the needs of parents and media educators for support. **Ann-Kristin Lieberknecht** is a doctoral candidate at Goethe University Frankfurt, specializing in online privacy and its impact on families. She has studied and gained valuable experiences at the Dresden University of Technology, École de Management Strasbourg, and Goethe University Frankfurt, from which she obtained her master's degree in information management and marketing Analytics. Her passion for data protection has led her to pursue a doctoral degree to deepen her knowledge of the field. Her research focuses specifically on assisting parents in navigating and mitigating the potential risks associated with online privacy for their children. Through her work, she aims to create a safer digital environment for families and children.

- On November 7th, NR hosted Dr.Vasileios Gkioulos from NTNU to give a lecture with the **title**: Enhancing cyber-security preparedness through training and awareness - A framework for healthcare and beyond, and **Abstract**: Several security breaches occur because of negligence or lack of awareness of the personnel within an organization, and attackers often structure malicious actions by exploiting one or more human factor weaknesses. Enhancing cyber hygiene through training and awareness, besides the integration of technical countermeasures, can not only reduce organizational vulnerabilities but also improve their capacity to identify and respond to ongoing attacks. The lecture on Enhancing cyber security preparedness through training and awareness provided insights to the participants on the importance of structured cybersecurity awareness programs, as well as of best practices for their execution, and indicators as success criteria. The material, not only is reusable across the delivered courses but can also raise awareness of the significance of undertaking such programs. **Dr.Vasileios Gkioulos** is an Associate Professor in secure systems engineering at NTNU and the product portfolio manager for OT security at Telenor Norway. He is a member of the NTNU-Critical Infrastructure Security and Resilience group and of the leader group for the Centre for Research-based Innovation - Norwegian Centre for Cybersecurity in Critical Sectors (SFI-NORCICS). Vasileios has a background in electronics engineering and communication systems, with a particular focus on cybersecurity across both domains. His main research interests are within the areas of critical infrastructure security and cyber-physical systems security, with a particular focus on secure systems engineering. Furthermore, he focuses on security awareness, education, and training, primarily on critical infrastructure personnel, but also the society at large.
- On November 9th, NTNU hosted Dr. Nesrine Kaaniche from IMT to give a lecture with the **title**: Data-Driven Healthcare: Striking the Balance

Between Innovation, Regulation, and Privacy, and **abstract**: Data-driven healthcare has the potential to revolutionize the way we diagnose, treat, and prevent diseases. However, the widespread use of healthcare data also raises concerns about privacy and security, particularly in the context of artificial intelligence (AI). Striking a balance between innovation, regulation, and privacy is essential for ensuring that the benefits of data-driven healthcare are accessible to all while protecting the privacy of individuals. **Dr. Nesrine Kaaniche** is an assistant professor in cybersecurity at Télécom SudParis, Institut Polytechnique de Paris, and an affiliate member of the interdisciplinary chair Values and Policies of Personal Information of Institute Mines Télécom, France. Previously, she was a lecturer in cybersecurity at the Department of Computer Science, the University of Sheffield, UK, and an International Fellow at SRI International, San Francisco, CA, USA. Her major research interests include privacy-enhancing technologies, applied cryptography for distributed systems, and decentralized architectures, i.e., IoT, fog, and clouds.

- On November 28th, NR hosted Dr. Roufaida Laidi from OUS to give a lecture with the **title**: Federated Learning in Healthcare: Privacy, Challenges, and the Future of Decentralized Machine Learning, and **abstract**: In the rapidly evolving landscape of machine learning (ML) and healthcare, traditional centralized models of data training are being challenged by emerging paradigms. This presentation delves into one such paradigm shift: Federated Learning (FL). Rooted in the principle of decentralized training, FL offers a promising avenue for collaborative model training across multiple devices or nodes without the need for raw data centralization. In an era marked by escalating data privacy concerns, tightening regulations, and the critical need for personalized healthcare solutions, FL provides an innovative solution to respect user privacy while harnessing the collective intelligence of distributed data sources in healthcare environments. **Dr. Roufaida Laidi**, Ph.D. is a postdoctoral researcher at NTNU in Trondheim, Norway, with a keen focus on the confluence of the Internet of Things (IoT) and Deep Learning. She completed her Ph.D. at ESI in Algeria in 2022 and has engaged in research collaborations in Germany and Norway. Her significant projects encompass innovative smart building solutions leveraging AI and IoT and federated learning on medical data, with contributions to prominent journals like ACM Transactions and IEEE Transactions as an author and reviewer.

- On November 29th, UCCS invited Prof. Maryline Laurent from IMT, to give a lecture with the **title**: Positioning privacy issues vs cyber security, and **abstract**: The lecture is clarifying what is privacy with regard to security, as privacy is often confused with data confidentiality whereas privacy extends far beyond that. The comparison will be performed in terms of properties, attacks, and threat models. After this clarification, the lecture pursues the main results of our analysis related to digital identity management across several countries in the world. **Maryline Laurent**

works as a Full Professor at Télécom SudParis, Institut Polytechnique de Paris, France. She leads the RST department (Telecommunication Networks and services) of Télécom SudParis, and she is co-founder of the chair of Institut Mines-Télécom "Values and Policies of Personal Information". She is a representative of France in the technical committee about security and privacy in the International Federation for Information Processing. She is a member of the editorial board of two leading journals (ranked Q1, Scopus) in the field of cybersecurity: IEEE Transactions on Information Forensics and Security (TIFS) and the International Journal of Information Security (IJIS). She is the area editor of the Annals of Telecommunication journal. She is the editor of several books including "Digital Identity Management" (2015). She was the TPC chair of the 18th International Conference on Availability, Reliability, and Security (ARES 2023). She also recently chaired the international conference PSD (Privacy in Statistical Databases) in 2022. She conducts research in the fields of cybersecurity and privacy. She is particularly interested in privacy-enhancing technologies (PETs) and has a keen interest in digital identity management. She is currently contributing to two national projects (PEPR Tracia on health and ANR TRUST), and several European projects including the PRIMA MoreMedDiet project.

- On December 4th, Dr. Vasileios Gkioulos got invited again by GUF, to give a lecture with the **title**: Security Awareness in Healthcare and Critical Infrastructures.

- On December 13th, NTNU invited Dr, Sandeep Pirbhulal from NR, to give a lecture with the **title**: Cybersecurity and Resilience for Healthcare Infrastructure: Challenges and Opportunities, and **abstract**: In recent times, healthcare infrastructure is considered as one of the crucial assets for several nations and governments. e-healthcare has received much attention concerning its cybersecurity and resilience. Due to the applicability of the broad spectrum of digital information and communication technologies, modern healthcare aims to offer more efficient medical services. In the e-healthcare domain, it is significant to demonstrate medical information storage components and services, to identify cybersecurity challenges and requirements, and to examine the impact of the availability and security of healthcare data and services in society. This talk includes a) exploring the security issues, potential threats, and resilience trends, and security requirements in healthcare systems, b) addressing healthcare standards, regulations, and governing bodies involved and their responsibilities, c) illustrating the potential threats and risks for healthcare, and to get an overview of the performance metric for health care security, and d) to discuss future directions and opportunities of cybersecurity and resilience in healthcare infrastructures.
  The lecture is highlighting healthcare security and resilience challenges, opportunities, and tentative solutions. This talk will potentially discuss some opportunities for WP3 (especially Task 3.4) by highlighting the kind

of course material that can be considered for developing education courses on securing real-time healthcare services. Also, this talk may elaborate on what can be potential proposal ideas in this domain as contributions to WP4 (innovation activities). **Dr. Sandeep Pirbhula**l is currently working as a Senior Research Scientist at the Norwegian Computing Center, Norway (since 2021). His current research focuses on cybersecurity and resilience, critical infrastructure protection, tele-healthcare, risk management, privacy and security for WSNs, 5G, and Internet of Things. He has published over 80 scientific articles (including peer-reviewed journals and international conferences) comprising IEEE Transactions, Elsevier's JCR Q1 other high-impact factor venues. Dr. Pirbhulal has extensive management experience in national and international research projects. He was the Principal Investigator/Team Lead of the project entitled, "Parallel Structure-based Biometric Authentication Mechanism for Secure Transmission of Sensitive Clinical Information", China Postdoctoral Science Foundation (2018-2019). He is the Project Leader of the International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance), funded by the Research Council of Norway (2023-2028). Dr. Pirbhulal has reviewed more than 150 papers in reputed peer-reviewed journals such as IEEE Access, IEEE JBHI, IEEE Transactions etc. He is an editorial board member of Springer International Journal of Information Security (since 2022), and Signals Journal (since 2020). For, three years (2019-2021), he was the Organizing Chair of the Workshop on Decentralized Technologies and Applications for IoT (D'IoT) in conjunction with the IEEE Vehicular Technology Conference (VTC). He is also the co-organizing chair of SecASure 2022 and 2023, SecIndustry 2023, SUNRISE 2023, and CANTATA 2023. He also serves as a TPC member of several conferences, seminars, and workshops at the national and international levels.

- On December 13th, another lecture was planned, GUF invited Dr. Shouhuai Xu from UCCS to give a lecture with the **title**: Cybersecurity Metrics, and **abstract**: Pursuing quantitative cybersecurity metrics is a fundamental but notoriously hard problem. It is no doubt one pillar of the emerging Science of Cybersecurity. In this talk, I will describe the Security, Agility, Resilience, and Risk (SARR) framework for tackling this fundamental problem. The framework is driven by the assumptions that are made when abstracting systems which are broadly defined to include infrastructures and enterprise networks (i.e., when creating system models), when abstracting attacks (i.e., when creating threat models), and when abstracting defenses (i.e., when creating defense models). I will describe how these assumptions are naturally tied to, among other things, security, agility, resilience, and risk attributes in the presence of attacks. While the problem is largely unexplored, I will review some recent results as initial steps toward ultimately tackling the problem and discuss a range of open problems for future research. In relation to the CybAl-

liance project, one important future work is to conduct a case study by applying the framework to define a systematic set of metrics to quantify the cybersecurity of healthcare infrastructures. **Dr. Shouhuai Xu** is the Gallogly Chair Professor in Cybersecurity, Department of Computer Science, University of Colorado Colorado Springs (UCCS). He introduced a systematic approach, dubbed Cybersecurity Dynamics, to modeling and quantifying cybersecurity from a holistic perspective. This approach has three major research thrusts: cybersecurity metrics, cybersecurity data analytics, and cybersecurity first-principle modeling (for seeking cybersecurity laws). His research has won several awards, including the 2019 worldwide adversarial malware classification challenge organized by the MIT Lincoln Lab. He co-initiated the International Conference on Science of Cyber Security (SciSec) and is serving as its Steering Committee Chair. He has served as Program Committee co-chair for several international conferences. He is/was an Associate Editor of IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), IEEE Transactions on Information Forensics and Security (IEEE T-IFS), and IEEE Transactions on Network Science and Engineering (IEEE TNSE).

Two additional talks that took place as a part of CYbAlliance work package WP.2, also, had contributions to WP3. These talks were done at SUNRISE 2023: 1st Workshop on SecUre aNd Resilient digItal tranSformation of healthcarE co-located with the 35th Norwegian ICT Conference for Research and Education (NIKT 2023) on 30th November 2023 at the University of Stavanger, Norway.

- The first talk was done by Dr Sanjay Mishra, from the Institute for Energy Technology (IFE), Halden, Norway, with the **title**: Healthcare 4.0: Data Analytics, Digital Transformation and Cyber Security Perspective.
  Dr. Sanjay Misra, a Sr. member of IEEE and ACM Distinguished Lecturer, is a Senior Scientist at the Institute of Energy Technology(IFE), Halden, Norway. Before joining IFE, he was associated with the Computer Science and Communication department of Østfold University College, Halden, Norway. He holds a Ph.D. in Information & Knowledge Engg (Software Engg) from the University of Alcala, Spain & M.Tech.(Software Engg) from MLN National Institute of Tech, India. His expertise is in the area of Applied Informatics (Cyber Security, Health Informatics, Software Engineering Applications, and Intelligent systems using AI and computational techniques) and has been published (- around 150 JCR/SCIE) in top journals like Computers and Security, Information Processing and Management, Engineering Applications of Artificial Intelligence, Expert Systems, and Applications, etc. He has been amongst the top 2% of scientists in the world (published by Stanford University) for the last three consecutive years, ranked no 2 in the whole of Africa in computer science (as per Elsevier: Scival analysis during 2017-2022) and also got several awards for outstanding publications (2014 IET Software Premium Award (UK)), TUBITAK-Turkish Higher Education, and Atilim University). He

is Editor in Chief of Int J of Human Capital & Inf Technology Professionals(IGI), IT Personnel and Project Management(IGI), and editor in various SCIE journals(Nature: Scientific Report((Impact Factor: 4.996), Elsevier: Alex. Engineering((Impact Factor: 6.626, Q1 7/92)), edited several special issues and 80 books from Springer(65 LNCSs, 4 LNEEs, 3 LNNSs, 3 CCISs) , 10 IEEE proceedings and several books. He delivered more than 100 keynotes and invited talks and public lectures at reputed conferences and institutes (he traveled to more than 60 countries).

- The second talk was done by Dr. Pantaleone Nespoli,from Institut Mines-Télécom (IMT), France. The **title** of the talk was: Methodology for Automating Attacking Agents in Cyber Range Training Platforms.
  Dr. Pantaleone Nespoli is a postdoctoral researcher working together with the Department of Information and Communication Engineering at the University of Murcia, Spain, and the SCN team of the SAMOVAR laboratory at Institut Polytechnique de Paris. His research is focused on cybersecurity and cyber defense training, with a particular interest in the detection and response to intrusions, and disinformation in social networks.

3.2 Future Plan

As future work for this task, we will plan more lectures, and encourage all partners to propose more topics, that might interest others. We will try to plan more lectures to be a part of the courses for students.

4 Conclusion

The work on WP3.2 and WP3.3 has resulted in great additions to the academic repositories among the partners and opened the doors for future collaboration, which resulted in giving the chance for students to travel and visit other universities.

References

[1] Amir Afaq et al. “Machine learning for 5G security: Architecture, recent advances, and challenges”. In: *Ad Hoc Networks* 123 (2021), p. 102667.

[2] 2. ENISA. *NFV Security in 5G - Challenges and Best Practices*. https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices. Feb. 2022.

[3] Hamed Hellaoui, Mouloud Koudil, and Abdelmadjid Bouabdallah. “Energy efficiency in security of 5G-based IoT: An end-to-end adaptive approach”. In: *IEEE Internet of Things Journal* 7.7 (2020), pp. 6589–6602.

[4] Rasheed Hussain et al. “On the adequacy of 5G security for vehicular ad hoc networks”. In: *IEEE Communications Standards Magazine* 5.1 (2021), pp. 32–39.

[5] Saurabh Mittal et al. “Digital twin modeling, co-simulation and cyber use-case inclusion methodology for IoT systems”. In: *2019 Winter Simulation Conference (WSC)*. IEEE. 2019, pp. 2653–2664.

[6] Sandeep Pirbhulal, Habtamu Abie, and Ankur Shukla. “Towards a novel framework for reinforcing cybersecurity using digital twins in IoT-based healthcare applications”. In: *2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)*. IEEE. 2022, pp. 1–5.

[7] Sandeep Pirbhulal et al. “A Cognitive Digital Twin Architecture for Cybersecurity in IoT-Based Smart Homes”. In: *International Conference on Sensing Technology*. Springer. 2022, pp. 63–70.

[8] Jun Zhang et al. “Cyber resilience in healthcare digital twin on lung cancer”. In: *IEEE Access* 8 (2020), pp. 201900–201913.