Critical Analysis of Mobile VPN Security

Deep Nandre
MSc Cyber Security
Manchester Metropolitan University
Manchester, United Kingdom
23685656@stu.mmu.ac.uk

Harsimran Kaur
MSc Cyber Security
Manchester Metropolitan University
Manchester, United Kingdom
23713280@stu.mmu.ac.uk

Vivek Kumar
MSc Cyber Security
Manchester Metropolitan University
Manchester, United Kingdom
23685510@stu.mmu.ac.uk

Navneet Kaur
MSc Cyber Security
Manchester Metropolitan University
Manchester, United Kingdom
23692403@stu.mmu.ac.uk

Vipasha Chaudhary
MSc Cyber Security
Manchester Metropolitan University
Manchester, United Kingdom
23645136@stu.mmu.ac.uk

***Abstract* — This survey study provides a thorough examination of the security of mobile virtual private networks (VPNs), utilising findings from four technical research. This study examines the function of mobile VPNs in guaranteeing secure and uninterrupted communication in dynamic settings, focusing on their structure, effectiveness, and security characteristics. The article discusses the progress made in mobile VPN technology, with a specific emphasis on solutions that effectively combine security and uninterrupted connectivity. It also explores the obstacles associated with this technology, including susceptibility to attacks, scalability concerns, and the intricacies of safeguarding mobile communications. Additionally, it assesses alternative open-source mobile VPN options, analysing their functionality and appropriateness for specific applications. This synthesis seeks to provide academics, developers, and users with an overview of the present status of mobile VPN security, its possible weaknesses, and future strategies for improving the dependability of these crucial tools in an increasingly interconnected world.**

Keywords— Virtual Private Network (VPN), Internet Protocol Security (IPSec), Internet Key Exchange version 2 (IKEv2), Layer 2 Tunnelling Protocol (L2TP), Secure Sockets Layer (SSL), Host Identity Protocol (HIP), Network Emulator (NEmu), Optimised Network Engineering Tool (OPNET).

I. Introduction

In modern society, Virtual Private Networks (VPNs) have become indispensable, as they provide secure communication pathways over untrusted networks such as the Internet. Originally developed for corporate use, VPNs were designed to enable secure remote access to internal networks and connect geographically separated company locations. Over time, VPNs have undergone significant advancements. With the rise of mobile technologies and widespread internet access, a new category of VPNs, called mobile VPNs, has emerged. These technologies not only create secure tunnels, but they also ensure that sessions remain uninterrupted even when there are changes in location or connection failures, which is important in our dynamic and mobile-focused workplace.[4]

The increasing number and expansion of mobile VPNs exemplify the challenges and aspirations of protecting data in a globalised environment characterised by remote work, global interconnectedness, and heightened worries about online privacy. Research and advancements in mobile VPNs primarily aim to enhance their efficiency and reliability, while addressing the challenges associated with maintaining security in dynamic mobile environments. [1][2][3] These findings highlight the growing challenge of balancing robust security measures with the necessary flexibility for efficient mobile communications.

This paper provides a comprehensive analysis of the latest research and advancements in the field of mobile VPN security. The article discusses various mobile VPN systems, their security measures, and the challenges they face, including DoS and replay attacks, scalability concerns, and vulnerabilities in decentralised P2P networks [4]. The article also examines how various mobile VPN systems address these challenges, such as enhancing session key renegotiation procedures and implementing robust authentication approaches.

The survey is structured methodically, commencing with a comprehensive examination of mobile VPNs and their evolution from conventional VPN technology. Subsequently, it delves into specific mobile VPN alternatives, scrutinising their functionality, efficiency, and security attributes. The survey examines many aspects of mobile VPNs, comparing various systems and evaluating their strengths and weaknesses in practical scenarios. The paper provides a comprehensive review of the current state of mobile VPN security and presents insights into future directions and potential areas for further research and development.

II. Understanding Mobile VPNs: Technical Foundations and Security Insights

Virtual Private Networks (VPNs) have become an essential component of secure internet access in our fast changing digital landscape. Originally, virtual private networks (VPNs) primarily served the needs of businesses by offering a secure connection for remote access to corporate networks and linking offices worldwide. Currently, they have broadened their scope by providing individuals with the capability to encrypt their internet traffic, thereby bolstering privacy and security, particularly when utilising public networks. This trend signifies our increasing dependence on digital data and the necessity to safeguard it against intrusive individuals and unauthorised entry. [1]

VPNs primarily operate by encrypting data flows and employing diverse tunnelling mechanisms. This guarantees the confidentiality, integrity, and availability of our sensitive information. An illustrious illustration, the Internet Protocol Security (IPSec) Virtual Private Networks (VPNs), are

celebrated for their resilient encryption and capacity to thwart attacks such as eavesdropping or replay attacks. When used with Internet Key Exchange (IKEv2), they facilitate reciprocal authentication between users and VPN servers, establishing a secure communication pathway [2].

The VPN industry is characterised by a wide range of tunnelling protocols, each tailored to address unique security and operational requirements. Layer 2 Tunnelling Protocol (L2TP) and Secure Socket Layer (SSL) VPNs are used for different purposes. L2TP is commonly used for remote employee access, whereas SSL VPNs are often used for browser-based solutions. The incorporation of sophisticated authentication techniques, such as digital certificates, pre-shared keys, and encrypted nonces, has strengthened the security of VPNs, guaranteeing that only authorised users are granted access [1].

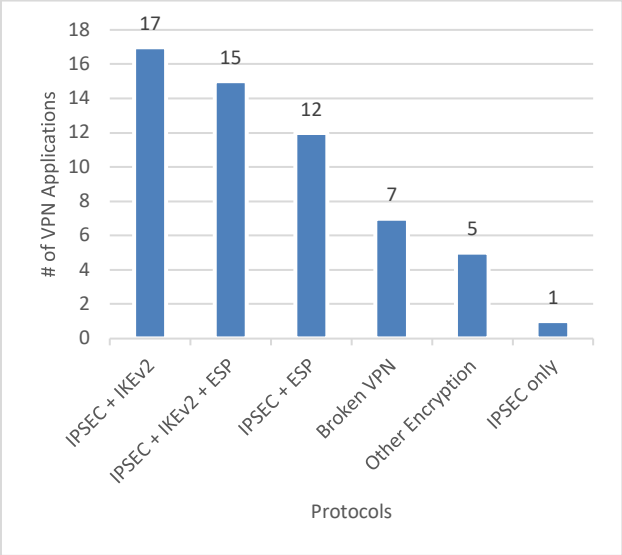

Figure 1: Chart of Encryption Protocols in Use [1]

Within the domain of mobile environments, conventional VPNs frequently have difficulties in sustaining connectivity in the face of shifting locations or disruptions in the network. In response to this issue, a novel category of mobile VPNs has arisen, which are highly skilled at not only establishing secure connections, but also guaranteeing uninterrupted sessions even in the presence of such interruptions. These mobile VPNs utilise advanced technology such as N2N and Host Identity Protocol (HIP) based systems, each specifically developed to address the distinct difficulties of mobility and security in various situations. They achieve the maintenance of secure communication without the necessity of re-establishing security keys for each session, thus improving efficiency and user satisfaction in mobile environments [4].

The subsequent sections of this paper are structured in the following manner. Section 2 offers a thorough examination of conventional VPN technologies, elucidating their fundamental principles and original objectives. Section 3 explores the progress made in mobile VPN systems, focusing on the developing technologies that provide safe and uninterrupted access in dynamic contexts. Section 4 examines the different security obstacles and remedies that are intrinsic to mobile VPNs, with a specific emphasis on how they tackle vulnerabilities like DoS and replay attacks. Section 5 delves into the pragmatic uses and evaluations of various mobile VPN systems. Section 6 provides a conclusion to our survey, presenting insights regarding the future of VPN technologies and their role in a world that is becoming more interconnected.

III. An Investigation of the Spectrum: A Comparative Analysis of Feature-Based Classifications for Mobile VPNs

A. Security and Privacy in Mobile VPN Applications

The paper examines the technical principles and inherent limits of mobile VPN software for iOS devices. It indicates that numerous applications jeopardise user security by communicating data using insecure HTTP protocols, resulting in vulnerabilities like DNS leakage and the disclosure of sensitive personal information. The presence of these problems highlights the absence of strong encryption and secure tunnelling protocols, which are essential for preserving user privacy and ensuring the integrity of data in mobile networking contexts. The study's emphasis on iOS apps, however informative, restricts its reach, indicating the necessity for more extensive research including many platforms to achieve a more holistic comprehension of mobile VPN security. This research is crucial for security professionals to comprehend the prevailing security vulnerabilities in mobile VPN applications and for knowledgeable consumers to make informed choices regarding VPN usage. [1]

The primary focus of this paper is to protect mobile VPNs from bandwidth flooding attacks. The study presents a strategy that combines a probabilistic model with the Access Token Embedded Encapsulating Security Payload (ATE-ESP) technique. This technique is formulated to differentiate genuine VPN traffic from malicious data, so effectively reducing the likelihood of such assaults. The probabilistic model evaluates traffic patterns to detect irregularities, which may indicate potential insider threats. Meanwhile, the ATE-ESP approach, deployed at the ISP's edge, aids in the identification and filtration of faked packets, a common attribute of outsider assaults. Nevertheless, the methods are not devoid of difficulties. The probabilistic model's dependence on consistent user behaviour can be a constraint, as user patterns can fluctuate. The ATE-ESP technique, however efficacious, may introduce intricacy to the VPN architecture, thus impacting its scalability and adaptability. The entire strategy is crucial for security professionals to protect VPNs from advanced assaults, and it emphasises the significance of strong security features in VPN services for knowledgeable users. [2]

This paper primarily aims to improve the security of mobile VPN applications by implementing a sophisticated two-factor authentication scheme. This method cleverly utilises graphical passwords, which are generated from activity samples and sports pitch photos, and incorporates a coordinate selection process. Although the utilisation of a dual-layered technique greatly enhances security by protecting against typical assaults such as shoulder surfing and smear attacks, it also adds complexity to the authentication process. The requirement for users to memorise and precisely choose graphical passwords and coordinates could be a usability obstacle, especially for individuals who are infrequent users or have difficulty with memory retention. This novel method signifies a crucial progression in mobile VPN security, while also emphasising the persistent difficulty of striking a balance between strong security and user-friendly functionality. [3]

The research conducted in this paper evaluates different mobile VPN solutions by considering their operational processes and acknowledging their limits. The article examines the methods by which these VPNs ensure secure connections in mobile settings, with a specific emphasis on evaluating the efficacy of various solutions in managing changes in location and disruptions in network connectivity. Although these solutions demonstrate the ability to adjust and withstand security challenges while on the move, they also expose intricate aspects and possible difficulties in expanding their capabilities. The findings of this study are essential for security experts, who must comprehend the intricacies of implementing mobile VPNs, as well as knowledgeable individuals, who will acquire a more comprehensive understanding of the security and dependability of the VPNs they may utilise in their everyday activities. The combination of technical expertise and ease of understanding makes the paper a significant asset in the realm of mobile VPN security. [4]

B. Improving the efficiency and expandability of mobile VPNs

The paper thoroughly examines how mobile VPNs perform in different network situations. It emphasises the crucial equilibrium between strong security measures, such as sophisticated encryption and tunnelling techniques, and the necessity of speedy data transfer. An optimal VPN performance requires a delicate equilibrium, which guarantees both data integrity and anonymity, while maintaining high speed and connectivity. The study also discusses the flexibility of mobile VPNs, emphasising their ability to smoothly adapt to changing network circumstances and various user needs. The conversation highlights the need to create VPN systems that provide not only strong security and efficiency, but also exceptional scalability and flexibility. The ability to scale is especially crucial in mobile environments where users constantly switch between several networks and require consistent and dependable VPN service. The paper provides essential insights into these aspects, which are of great importance to network managers and VPN developers that seek to improve the user experience while maintaining high levels of security and performance. [1]

Technical Paper 2 focuses on the critical issue of network performance when dealing with security concerns such as bandwidth flooding. The paper's novel methodology, which combines a probabilistic model and the ATE-ESP technique, seeks to protect VPN bandwidth from unauthorised utilisation. Implementing this method is crucial for preserving network performance, particularly when facing the risk of bandwidth abuse, which can significantly impair VPN effectiveness and user satisfaction. Nevertheless, the utilisation of these sophisticated methods can present difficulties in network scalability. The efficacy of the probabilistic model in identifying atypical traffic patterns relies on the consistency of user activity, which may not always be uniform. In addition, the ATE-ESP approach, while effective in removing unauthorised traffic, introduces additional complexity to the current VPN architecture. This has the potential to impede the flexibility of VPN services in accommodating various network conditions and user requirements. Therefore, although these strategies greatly improve VPN performance and security, they also emphasise the requirement for well-rounded solutions that can quickly scale without excessively complicating the network architecture. [2]

Technical Paper 3 takes a comprehensive approach to analysing two-factor authentication and its impact on VPN performance. The paper's approach employs a two-step authentication process that combines graphical components with coordinate selection to enhance security. Nevertheless, this complex procedure could potentially have a discernible influence on the overall efficiency and expandability of the VPN service. The duration required for users to authenticate using this method, particularly in situations when prompt access is crucial, may be a potential disadvantage. Moreover, the computational demands for generating and validating these visual components could impose an extra burden on the VPN infrastructure. Although this strategy certainly improves security standards, the difficulty is in optimising these processes to prevent them from hindering the operation of the VPN, especially in situations with a large number of users or in networks with limited capacity. [3]

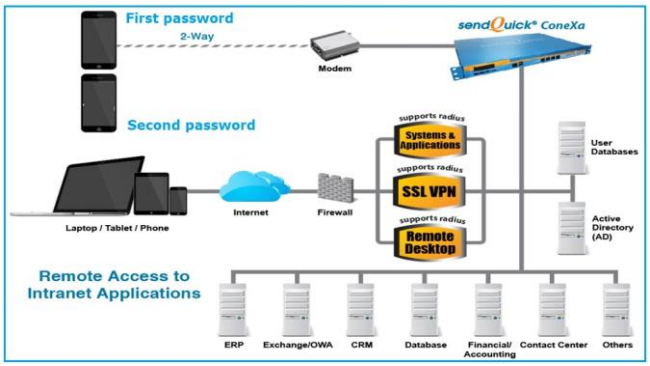

Figure 2: Illustrate two-factor authentication [3]

The research in this one provides a comprehensive analysis of the operational effectiveness of mobile VPN solutions. The investigation centres on the capacity of these systems to effectively manage the ever-changing nature of mobile networking, specifically their capability to uphold safe and consistent connections amongst network alterations and user movement. The study provides a thorough analysis of several VPN systems, emphasising their effectiveness in maintaining continuous service and identifying potential limitations in terms of scalability and complexity. This feature is especially vital for network administrators and IT professionals who must strike a balance between the requirements of strong security and the necessity for a scalable and effective network infrastructure. This analysis offers customers valuable information on the dependability and efficiency of their mobile VPNs. It is crucial for individuals who heavily rely on VPNs for business or personal purposes in mobile-focused environments. [4]

C. Mobile VPNs: Enhancing User Experience and Interface

The study highlights the crucial importance of user-centric design in the effectiveness of mobile VPN applications. This emphasises the concept that the technological security aspects of an application, although crucial, are but one aspect

of the whole equation. The application's user interface and overall design are equally crucial as they greatly impact the way users engage with the security features. An intuitive design that streamlines secure processes can result in enhanced and more uniform acceptance of security protocols among users. This strategy can significantly enhance the network's overall security stance. The study proposes a fundamental change in the development of VPNs, shifting the focus from exclusively technological security measures to also prioritising user involvement and streamlining the user experience. By attaining this equilibrium, VPN developers can guarantee that their programmes are both safe and user-friendly, catering to a wider audience that includes individuals with limited technical expertise. The comprehensive approach to VPN design is essential in a time when ensuring digital security is of utmost significance to all users. [1]

The study provides a detailed and subtle analysis of VPN security as seen from the user's point of view. The use of advanced security measures, specifically the ATE-ESP approach, plays a crucial role in establishing user confidence in VPN services, particularly at a time when cybersecurity threats are growing more complex. Nevertheless, prioritising high-level security entails certain compromises in terms of user experience. The intricate nature brought about by these sophisticated security measures may not perfectly correspond with the anticipated simplicity and straightforwardness of interfaces sought by numerous VPN users. This contrast emphasises the crucial equilibrium that must be achieved in VPN design, where advanced security measures must be incorporated with user-friendly interfaces. By achieving this equilibrium, VPN providers can guarantee not just the technical resilience of their services but also their availability and attractiveness to a wider user demographic, who may lack extensive technical expertise but share the same level of worry over their online security and privacy. [2]

Technical Paper 3 presents a study that demonstrates a significant advancement in enhancing the appeal and interactivity of security measures. Integrating graphical components into the authentication process not only improves security but also adds a touch of personalisation and increases user engagement. This approach, which may specifically attract customers who want visually stimulating and interactive security measures, has the capability to change the perception of VPN security from a boring duty to an exciting experience. Nevertheless, this advancement is not devoid of its obstacles. The intricacy and originality of the system may appear intimidating or burdensome for certain users, especially those who favour direct and expedient access methods. The difference in user preferences highlights the significance of developing VPN systems that accommodate a wide range of users, striking a balance between advanced security capabilities and the requirement for simplicity and user-friendliness. The article emphasises the importance of ongoing innovation in VPN design, with a specific focus on developing solutions that are both technically strong and attractive to a wide range of users. [3]

The article provides a thorough examination of the design principles of mobile VPN systems, emphasising their user-centric approach. This study examines the user experience of handling VPN connections while on the go, focusing on how different solutions meet the requirement for smooth and user-friendly interfaces. This study emphasises the significance of creating VPNs that include both technological resilience and user-friendly accessibility for the general population. The emphasis on user-centric design is essential in the current digital environment, as the usability of security measures often dictates their widespread acceptance and efficacy. The paper offers essential recommendations for developers and providers who want to design mobile VPN solutions that cater to a varied user base, ranging from tech-savvy professionals to everyday consumers seeking secure and convenient online experiences. It focuses on the user experience component of mobile VPNs. [4]

IV. RESEARCH CHALLENGES

This section is a compilation of significant research inquiries that are vital to the security landscape of mobile virtual networks (VPNs). To improve the strength and durability of these systems, it is necessary to thoroughly investigate the challenges mentioned in the technical articles. [1] to [4]. This investigation will help in synthesising valuable insights.

A. Enhancement of Two-Factor Authentication

The rise of mobile virtual private networks (VPNs) underscores the need to enhance user authentication processes, particularly through the use of Two-Factor Authentication (2FA). Developing enhanced two-factor authentication (2FA) techniques that seamlessly integrate with mobile virtual private network (VPN) applications on both iOS and Android platforms poses significant challenges. The inherent constraints of mobile devices, such as their limited screen size and unreliable internet connection, pose specific challenges in the development of 2FA methods that effectively balance security and user-friendliness. Addressing these challenges will pave the way for a mobile VPN ecosystem that is more secure and user-friendly.

B. Defence Mechanism Against Both Internal and External Bandwidth Flooding

The utmost priority should be placed on safeguarding the availability and integrity of VPN services from both external and internal attacks involving the overwhelming of bandwidth. The study purpose is to create sophisticated security mechanisms capable of differentiating between malicious flooding efforts and legal traffic. It is crucial to investigate adaptive strategies that can dynamically adjust to evolving attack vectors. Striking a balance between the need for robust defence and the efficacy of VPN services is a challenging undertaking that requires meticulous investigation.

C. Upgrades to the HTTP Protocol for Mobile VPNs

Due to the utilisation of HTTP protocols in mobile VPNs, there exist vulnerabilities that can be exploited by astute adversaries. The primary study concerns pertain to the examination of improved and fortified techniques specifically tailored for mobile situations. It is imperative to tackle concerns with protocol overhead, compatibility, and speed optimisation. To construct resilient mobile VPN networks, it is essential to have a comprehensive

understanding of the consequences associated with transitioning from HTTP to more fortified alternatives.

D. Mitigation of DNS Leakage

Mobile VPNs continue to be a significant concern due to DNS leaks, as they jeopardise user privacy and undercut the claimed anonymity of these services. Developing dependable techniques to mitigate DNS leaks on iOS and Android platforms is a research obstacle. Crucial areas requiring thorough investigation involve analysing the intricacies of mobile DNS resolution, exploring state-of-the-art encryption methods, and assessing the impact of different network conditions on DNS leak vulnerability.

V. EVALUATION TOOLS

This section presents the evaluation tools utilised to analyse the security elements of mobile virtual networks (VPNs). An exhaustive analysis is required to fully comprehend and evaluate the efficacy of security techniques suggested in the literature under investigation. To evaluate the effectiveness of different research initiatives in the field, we utilise the following instruments for analysis and assessment.

A. Wireshark

Wireshark is an essential tool in our assessment methodology as it provides comprehensive analysis of network traffic at the packet level. This open-source packet analyser can be used to examine data flows and detect security weaknesses and vulnerabilities in mobile VPN implementations. By gathering and examining network packets, Wireshark aids in conducting a comprehensive evaluation of the security and privacy features of iOS VPN applications [1] and suggests effective security measures by detecting abnormal patterns and possible risks. [2]

B. Network Emulator for Mobile Universe (NEmu)

NEmu is a useful assessment tool for evaluating the practical consequences of suggested security patches on iOS and Android devices. NEmu is a network emulator that replicates different network circumstances to aid in simulating mobile environments. Through the utilisation of NEmu, we assess the robustness and flexibility of VPN schemes in different scenarios, providing insights into their practicality and adaptability. [2]

C. Optimised Network Engineering Tools (OPNET)

OPNET, also known as Optimised Network Engineering Tools, introduces an additional layer of intricacy to our assessment process. OPNET facilitates the evaluation of the network's overall effectiveness by analysing the influence of security measures on performance. OPNET is essential for protecting VPNs against bandwidth flooding attacks due to its ability to mimic network scenarios comprehensively. This enables us to assess the effectiveness of suggested remedies in reducing both internal and external risks. [3]

D. Additional Considerations

Our evaluation toolset mostly consists of Wireshark, NEmu, and OPNET. However, we continuously seek for new tools and ways to enhance our evaluation process. In accordance with established industry standards, we acknowledge the ever-changing nature of the sector and are open to the possibility of including additional instruments to enhance the reliability of our assessments. By integrating new tools, we ensure that our assessments remain current and relevant as the mobile VPN security landscape evolves.

In general, the several evaluation instruments used in this investigation provide an adaptable technique for examining the security and privacy implications of mobile virtual networks. When combined, these resources assist with offering a more thorough understanding of the positive and negative aspects of several safety procedures that are dealt with in the literature review.

VI. CONCLUSION

This overview provides a comprehensive examination of the current state of mobile VPN security, including its history, underlying technology, and categorizations. The analysis focuses on identifying vulnerabilities in four technical articles, examining the phenomenon of bandwidth floods, exploring various authentication approaches, and evaluating the operational effectiveness of these articles. The focus on iOS and the inclusion of Android displays a commitment to achieving a thorough comprehension.

Research problems highlight the need for ongoing investigation in areas such as two-factor authentication, protection against bandwidth flooding, improvements to the HTTP protocol, and mitigation of DNS leakage. Assessment tools such as Wireshark, NEmu, and OPNET offer real-time analysis combined with established standards in the field.

The objective of this poll is to furnish security specialists and well-informed users with valuable insights. Practitioners benefit from exploiting security vulnerabilities, developing innovative defences, and addressing the challenges of providing secure mobile VPNs; users gain valuable knowledge about reliability.

This serves as a guide for future research and progress in the field of mobile VPN security in a globally linked society with constantly evolving cybersecurity risks. To establish robust, secure, and user-friendly mobile VPNs in fast-changing scenarios, it is necessary to overcome challenges and adopt innovative approaches.

REFERENCES

[1] Wilson, J., McLuskie, D. and Bayne, E., 2020, August. Investigation into the security and privacy of iOS VPN applications. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-9).

[2] Shunmuganathan, S., Saravanan, R.D. and Palanichamy, Y., 2020. Securing VPN from insider and outsider bandwidth flooding attack. *Microprocessors and Microsystems*, *79*, p.103279.

[3] Lehmoud, A.A.M., Obeis, N.T. and Mutar, A.F., 2022. Proposing a security system for the VPN through design and implementation of a scheme for android and IOS mobiles based on two-factor authentication. *Periodicals of Engineering and Natural Sciences*, *10*(2), pp.292-303.

[4] Ahmat, D., Barka, M. and Magoni, D., 2018. Mobile vpn schemes: Technical analysis and experiments. In *e-Infrastructure and e-Services for Developing Countries: 8th International Conference, AFRICOMM 2016, Ouagadougou, Burkina Faso, December 6-7, 2016, Proceedings 8* (pp. 88-97). Springer International Publishing.