Research Methodology

Ifra Ejaz	Abdullah Awan	Ali Hassan Zaidi
21L-7508	21L-7713	21L-5274
l217508@lhr.nu.edu.pk	l217713@lhr.nu.edu.pk	l215274@lhr.nu.edu.pk

Introduction:

This chapter will commence by revisiting the research aim. Drawing from the literature review, the conceptual framework will be presented as a response to the potential gaps that were identified. The methodology outlined in this chapter will systematically navigate the domain of SDN and its implications for IoT security, meticulously identifying specific security risks that plague IoT networks encompassing qualitative and quantitative research methods. It will then proceed to articulate the research that has been done to identify mechanisms through which SDN in conjunction with cloud computing, can effectively mitigate these identified risks.

Research Design:

We have adopted a mixed-methods approach to conduct our research. This approach facilitates an in-depth exploration of SDN's role in IoT security through both quantitative and qualitative analysis. Furthermore, we have validated our research by secondary research methods to establish a solid theoretical foundation and situating the study within the existing body of knowledge.

Data Collection:

1. **Secondary research**: First of all, we started our research by systematically collecting, evaluating and analysing published material, including reviewed articles, industry reports, white papers, and case studies related to SDN's role in enhancing IoT security.
2. **Literature review**: Conducted a systematic review of existing research. Each selected publication was critically reviewed, with key information extracted including study objectives, methodologies, findings, and conclusions. This process not only allowed for the collection of data relevant to IoT security and SDN but also facilitated the identification of research gaps and emerging trends in the field.
3. **Surveys:** This approach entails a comprehensive review and synthesis of existing surveys conducted by IT professionals and experts in the fields of IoT (Internet of Things) and SDN (Software-Defined Networking). The aim is to

identify common themes and insights regarding current security challenges faced in these areas. Through the examination of collected data from multiple sources, this research seeks to highlight the perceived effectiveness and potential gaps in SDN solutions as identified by industry professionals.

4. **Interviews:** Findings from existing semi-structured interviews with cybersecurity experts and network administrators who specialize in IoT and SDN will be analysed. This method allows for a deep dive into expert opinions and experiences, providing a nuanced view of the potential and limitations of SDN technologies in enhancing IoT security.

Data Analysis:

Both qualitative and quantitative research approaches are essential to the study of leveraging Software-Defined Networking (SDN) to improve the security of the Internet of Things (IoT). Every technique makes a distinct contribution to our knowledge of the intricacies of IoT security issues and the possibilities presented by SDN solutions. Here is a closer look at the application of these methodologies and their importance to the study.

1. **Qualitative Analysis**: Recorded opinions and experiences of individual involved directly in the IoT and SDN domains will be analysed. These will offer insights that cannot be quantified. Examination of recorded cases where SDN has been used to resolve security concerns in Internet of Things configurations. These case studies provided rich insights into the research by enabling a thorough analysis of particular problems, solutions used, results, and lessons learned.

2. **Quantitative Analysis:** Statistics on the frequency of security issues, the adoption rate of SDN solutions, and the perceived efficacy of these solutions will be obtained through thorough examination of quantitative surveys of IT professionals and organizations engaged in IoT and SDN implementations. Controlled trials that simulate Internet of Things environments both with and without SDN-based security improvements will be done. The influence of SDN on key performance indicators (KPIs) such as intrusion detection rates, network performance during attacks, and the effectiveness of threat response mechanisms will be quantified through these simulations.

Expected Results:

The study anticipates that SDN's centralized control, enhanced visibility, and dynamic response mechanisms will greatly enhance the security of IoT networks. Its goal is to create a set of guidelines for applying SDN solutions in Internet of Things environments, taking into account particular security risks and difficulties found in the research.

Conclusion:

This technique lays the groundwork for a thorough research of how SDN might improve IoT security, with the goal of offering insightful analysis and useful recommendations to the cybersecurity community.