CHAPTER V

CONCLUSION AND FUTURE WORK

5.1 Introduction

In this chapter, the summarization, contribution, limitations and the future works of this research are illustrated. The research answers all the research questions defined in chapter one to achieve the main objective of this research which is proposes a new framework for BYOD security. This research focused on solution to mitigate the emerging attacks from using the employees their own devices for work purposes. The framework was developed based on SLR of previous approaches to solve the issue of BYOD security through control the access of the user.

This chapter is organized in sections, section 5.2 the summary of the research findings, section 5.3 research contribution, section 5.4 research limitations, section 5.5 the recommendations and future works.

5.2 The Summary of the Research Findings

The overall purpose of this research was to propose a new framework as a solution to secure BYOD based on SLR. On the one hand, it identified the elements of BYOD security framework based on SLR. On the other hand, this included an evaluating the acceptable of identified elements for BYOD security framework.

The research findings are classified based on the research questions that are related within the elements that needed to design BYOD security framework based on systematic literature review and the interview findings to validate this framework.

Therefore the descriptions of the research questions answer are listed below:

1st Research question: What are the elements that needed to propose BYOD security framework?

The answer of this question targets to find the elements that needed to propose framework for BYOD security. These elements distributed onto two layers of security control which are device control layer and BYOD server layer. The elements of device control layer are device profiles and anti-malware scanner. In the BYOD server layer are user profiles, user role, internal apps and external apps. This research used systematic literature review method to find the elements from previous frameworks. The elements generated from systematic review to be a successful keys towards BYOD security.

The answer of this question is illustrated in the proposed framework and the elements can be summarized in the following table:

Tier 1	Device Control
	1 - Device Profiles 2 – Anti-Malware Scanner
Tier 2 BYOD Server	User Control
	1 – User Profile 2 – User Roles
	Application Control
	1 – Internal Apps 2 – External Apps

Table 11: BYOD Security Elements

2nd Research question: How to propose a framework for BYOD security?

The goal of this research question is to define how the new framework for BYOD security can be developed. The research reviewed systematically the previously works related to BYOD security policies to identify the elements that needed to develop the BYOD security framework. From the review that we conducted we found that each study has focused on a solution to a single and specific problem, none of these approaches were able to fully addressing the issue of BYOD security. The research evaluated these approaches and combined each element in these approaches into BYOD security framework consists of two layers of security control. These layers are device control and BYOD server.

3rd Research question: To what extent the chosen elements of BYOD security framework are acceptable?

This question aims to know to what extent the chosen elements of BYOD security framework are acceptable. Through our evaluation for the proposed framework by interview method and using qualitative analysis methodology we can summarize the results as a follow:

For the device control layer, which is consists of two security elements (device profiles and anti-malware scanner), the control of devices' profiles will provide high level of security by defining the allowed devices to access the BYOD system. In addition, using anti-malware scanner will keep tracking the devices for any malicious apps or scripts. For second layer BYOD Server which consists of four security elements (user profiles, user role, internal apps, and external apps), the setting of user profiles have a good trend to prevent any misuse of any data or resources by any unauthorized user as the system admin configure each user profile according user role to define user level and allowed activities. Moreover, accessing to internal and external apps is very important security challenge as the use of internal apps consider as main gates to the organization data and resources, also using external apps within the working hour could cause many security issues. Internal apps must be controlled to be used according to users' roles. Implementing of VPN and applying the right permission could be a good choice to provide the required security to access within the organization to avoid and unexpected security issues.

5.3 Research Contribution

This research proposed a framework for BYOD security. This framework gives a solution to BYOD problem in business. By BYOD security framework an organization is able to ensure the security of devices accessing their network and keep their critical data secure.

This framework allows employees to use their personal device at home and at work in more security way. This framework can be applied in different organizations and educational institutions as well.

5.4 Research Limitations and Difficulties

Although the research has reached its aims, there are some unavoidable limitations:

1- Because of the time limit, the systematic review conducted on limited databases which are listed in chapter III. The articles selected for the review were only in English language. The review included only research papers and chapters of books on BYOD security policies.

2- Lack of skills in qualitative analysis making the data analysis stage takes long time.

3- The difficulty of academic writing in English language because it's a second language.

5.5 The Recommendations and the Future Works

1-The future work of this research could address the first implementation of the proposed framework and the testing of the prototype in real world scenarios.

2- Also, adding another layer of monitoring may help to improve the efficiency of this framework.

5.6 Summary

This chapter concluded the research. It summarized the main findings of this research and provided a better understanding of this research. It also presented the limitations and difficulties of the research. Finally, presented the recommendations and the future work for the research.