



Open-Source Information Security and Audit framework for BYOD

D.P.K.L.Peiris

Reg. No.: MS20903138

M.Sc. in IT

Specialized in Cyber Security

Supervisor: Mr.Kavinga Yapa Abeywardane

Oct 2021

18882

**Department of Cyber Security
Faculty of Graduate Studies and Research
Sri Lanka Institute of Information Technology**

Table of Contents

Table of Contents.....	2
List of Figures	4
List of Tables	4
Abstract.....	5
Chapter 1 Introduction	6
1.1 Background	6
1.2 Elements which donates to a lack of security concern.....	11
1.3 Existing BYOD Security Frameworks	12
1.4 Framework for BYOD Security	14
Chapter 2 The Importance of the BYOD Security Study	17
Chapter 3 Bring-Your-Own-Device Opportunities and Risks	20
Chapter 4 BYOD Controls on Information Security and privacy	22
Chapter 5 Requirements for BYOD Security	23
5.1.1 ACCESS CONTROL LIST FOR BYOD.....	25
Chapter 6 Problem Statement	26
6.1 Model of access based on VPN	27
6.1.1 Problem definition	27
Chapter 7 Research Objectives and Research Question.....	29
<i>Chapter 8 Literature Survey</i>	<i>35</i>
8.1 BYOD's Evolution.....	37
8.2 Challenges of BYOD security	37
Chapter 9 Methodology.....	39
Chapter 10 Developed Design	46
10.1.1 Architecture	47
Chapter 11 Source code of the development.....	48
11.1.1 Routing to the system URL configuration	48
11.2 Login Template.....	69
11.3 User Login Template	75
11.4 Admin Login template.....	91
11.5 Report Generation	112
11.6 PDF Report generation.....	131
Chapter 12 System interface.....	135
Chapter 13 Working plan and Time Schedule.....	140
13.1.1 Work Plan.....	140
	2

13.1.2 Time Plan.....	141
Chapter 14 Facilities Required	141
Chapter 15 Feasibility	142
Chapter 16 Budget	144
Chapter 17 Appendices.....	144
Chapter 18 Conclusion	145
Chapter 19 Future Work	146
Chapter 20 Reference	147

List of Figures

Figure 1 elements of influencing the BYOD devices in corporate environment	10
Figure 3 Existing BYOD Security Frameworks	14
Figure 4 Framework for BYOD Security	15
Figure 5 Access control list.....	26
Figure 6 BYOD security Challengers	39
Figure 7 Framework process.....	41
Figure 8 Framework Design and communication diagram	44
Figure 9 BYOD security model conceptual design	47

List of Tables

No table of figures entries found.

Abstract

In today's pandemic environment, businesses are continuously looking for innovative solutions to assist with their corporate operations. Businesses aim to incorporate contemporary technological advances in order to stay ahead of the competition and expand their business in terms of both outcomes and productivity. "Bring your own device" is one of the new phenomena (BYOD). Instead of company providing the required hardware/software to their employees they can use their own device. Employees are permitted to use their own laptops, tabs or cell phones at work when BYOD rules are adopted. Because they are already familiar with how these devices work, they are more likely to be more efficient. The benefits of this led to greater employee satisfaction and allow the company to pass on more expenses to the employee, therefore improving its cost-effectiveness. [1] This has made workers' jobs easier and contributed to increased efficiency.

Security is the most important factor in BYOD, which has a range of issues. [2] By 2020, 74% of organizations would have experienced data breaches due to unsecure mobile device use. The idea of employees bringing their own devices to work would keep any IT manager up at night (BYOD). While bringing your own device increases productivity, IT experts are aware that bringing your own device exposes your organization to severe security threats. [9] As a result, BYOD device security methods have irritated the interest of IT experts. MDM, MAM, and NAC are just a few of the BYOD device security frameworks that are now accessible. As a consequence, businesses can employ those security measures to prevent data breaches. If such a security system exists, there is no automatic IT Security and auditing tool in it to deliver compliance information to IT experts so they can respond quickly.

As a result, I've picked that gap as a study topic in order to present open source as a compliance alternative to companies. Based on the study's findings, the suggested security and audit methodology would assist businesses in reducing and recognizing BYOD security concerns. This security and audit methodology will also help to the creation of