

# A Risk management framework for the BYOD environment

AlHarthy, Khoula

*Award date:*
2022

*Awarding institution:*
Coventry University

# A Risk Management Framework for the BYOD Environment

**(Case study *of the organisations in Oman)***


**Khoula Al Harthy**

PhD

Feb 2022

# A Risk management framework for the BYOD environment

**(Case study *of the organisations in Oman)***

***A thesis submitted in partial fulfilment of the University's requirements for the Degree of Doctor of Philosophy***

Feb 2022

# Certificate of Ethical Approval

Applicant:

Khoula AlHarthy

Project Title:

Intelligent information security strategies and risk management for BYOD environment

This is to certify that the above named applicant has completed the Coventry University Ethical Approval process and their project has been confirmed and approved as Medium Risk

Date of approval:

18 April 2016

Project Reference Number:

P42216

# Abstract

Computer networks in organisations today have different layers of connections, which are either domain connections or external connections. The hybrid network contains the standard domain connections, cloud base connections, "bring your own device" (BYOD) connections, together with the devices and network connections of the Internet of Things (IoT). All these technologies will need to be incorporated in the Oman Vision 2040 strategy, which will involve changing several cities to smart cities. To implement this strategy artificial intelligence, cloud computing, BYOD and IoT will be adopted.

This research will focus on the adoption of BYOD in the Oman context. It will have advantages for organisations, such as increasing productivity and reducing costs. However, these benefits come with security risks and privacy concerns, the users being the main contributors of these risks. The aim of this research is to develop a risk management and security framework for the BYOD environment to minimise these risks. The proposed framework is designed to detect and predict the risks by the use of MDM event logs and function logs. The chosen methodology is a combination of both qualitative and quantitative approaches, known as a mixed-methods approach. The approach adopted in this research will identify the latest threats and risks experienced in BYOD environments. This research also investigates the level of user-awareness of BYOD security methods.

The proposed framework will enhance the current techniques for risk management by improving risk detection and prediction of threats, as well as, enabling BYOD risk management systems to generate notifications and recommendations of possible preventive/mitigation actions to deal with them.

# Acknowledgement

I start by thanking God for support during all my PhD phases, and for giving me the strength to complete this step of my life, in spite of all the good and bad situations I passed through.

Thanks to my parents who have always believed in me and have motivated me to keep learning and studying.

Thanks to my brothers and sister who have kept guiding and supporting me professionally and emotionally.

Thanks to my husband for his understanding and encouragement and for joining me on all the trips.

I express my deep appreciation to my Director of studies Dr. Nazaraf for his guidance and encouragement during my studies, and for Dr. Arun and Dr. James as members of the supervisory panel.

I am grateful to the Middle East College board for their scholarship and for trusting in my ability to complete these studies.

I thank my fellow researchers, Thoufeeq Ahmed, Priya Mathew and Santhosh. The friendship I have with them is what kept me going through tough times.

Special thanks for Alya Al Farsi for her nice soul, who has supported me through hard times, in both sickness and health.

## List of publications:


1. AlHarthy, K. and Shawkat, W., 2013, November. Implement network security control solutions in BYOD environment. In *2013 IEEE International Conference on Control System, Computing and Engineering* (pp. 7-11). IEEE.

2. Al Harthy, K., Shah, N. and Shuttleworth, J., 2016. Smartphones Hotspots Intrusion Detection System (SHIDS). *Int. J. Inf. Secur. Res*, *6*(1), pp.643-650.

3. Shah, N. and Shankarappa, A.N., 2016, December. Smartphone's hotspot security issues and challenges. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 113-118). IEEE.

4. Al Harthy, K. and Shah, N., 2019, October. BYOD Security and Risk Challenges in Oman Organisations. In *International Conference on e-Business Engineering* (pp. 290-301). Springer, Cham.

## Table of Content

# List of Figures

# List of tables

## Abbreviations

| | |
|---|---|
| BYOD | Bring Your Own Devices |
| MDM | Mobile Device Management System |
| SVM | Support Vector Machine |
| ML | Machine Learning |
| MAM | Mobile Application Management |
| MIM | Mobile Information Management |
| IoT | Internet of Things |
| IT | Information Technology |
| IS | Information Security |
| URL | Uniform Resource Locator |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| TP | True Positive |
| TN | True Negative |
| FP | False Positive |
| FN | False Negative |
| AIS | Artificial Immune Systems |

# Chapter One: Introduction

This chapter introduces the research topic and highlights the research questions, aim and objectives. It also discusses the motivation for conducting this research and the thesis structure.

## 1.1 Environment Background

In the BYOD environment smartphone users in organisations are allowed to use their own devices for their work. Smartphone and tablet users are the main controllers of the technology and data in a BYOD environment. Although the concept appeared in 2010, the real implementation of BYOD had already commenced in the business environment. BYOD is an approach which allows the employees to use their own personal smartphones and tablets rather than the devices supplied by the workplace (Brooks 2013). This approach started due to the increase in the number of remote workers who accessed the services and data of organisations remotely through their personal phones.

This research focuses on Bring Your Own Device (BYOD) security threats and risks which will be analysed and demonstrated in Oman organizations, a middle-eastern country located in the east of Asia. Oman is adopting the "Smart City" concept. This has started in Al Duqum, and will then move to Sohar in 2022 and Matrah in 2025 as part of the Oman Vision 2040 developments. A smart city is an urban area which applies technology to improve city services (Nam and Pardo 2011). Smart cities are created by the use of cloud technology, Internet of Things (IoT), Bring Your Own devices (BYOD) and artificial intelligence. This research will focus specifically on BYOD. Currently, Oman has automated most of the government-department procedures, which users can access remotely through cloud-based services. Employees, using mobile devices are able to access network resources for their work. This study will propose a framework which predicts the security risks for the adoption of BYOD in Oman organisations.

### 1.1.1 Benefits of BYOD

This section discusses the two main advantages of adopting BYOD for organisations, which are, cost saving and the enhancement of work performance.

Buying devices for all employees has been very costly for IT budgets especially for small and medium-sized organisations, therefore, many IT departments have reduced these costs by allowing employees to use their own mobile devices. As stated by Baillettea et al. (2018), the IT departments can support nearly three times as many users in BYOD tablet programmes than company-purchased tablet programmes. Similarly, Harris et al. (2012) claimed that the BYOD environment will help to reduce the consumption of company-owned devices. However, other authors have argued that although BYOD saves the cost of purchasing devices, there are still hidden costs involved. These hidden costs include: the implementation of security and manageability systems to control BYOD, re-structuring the business network, applying new policies or updates to the current policies and enhancing the servers and service performance, which consume IT budgets and resources (Harris, et al. 2012; Kelly 2013; Kaneshige 2012). Therefore, before the adoption of BYOD, decision makers should carefully consider the budget that needs to be allocated for its implementation.

### 1.1.2 Enhancing the Work Performance and Productivity

Allowing BYOD has impacted the business environment in several ways as shown in figure 1.1.



Figure 1.1 BYOD Growth in the Business Environment (Burt 2011)

However, personal phone use in business increased by 10% in one year between 2010 and 2011 (Burt 2011). Labek et al. (2013) reviewed a number of studies on the influence of BYOD on users, including employee satisfaction and performance. They concluded that employees find it convenient to carry their work in personal mobiles to enable round-the-clock accessibility, which increases business productivity. Additionally, as has been noted by Harnesk and Lindström (2011),

enhancing the user performance will also affect customer satisfaction,. Doargajudhur and Peter Dell (2019) investigated the different impacts of adopting BYOD in workplace. Their research also indicates that adopting BYOD impacts the work performance and job satisfaction of employees.

Combining personal data and business information in the same smartphone has been considered a significant security-challenge for IT professionals, therefore, providing work flexibility and maintaining data integrity is considered to be highly complicated and a risk factor. Policy gaps, lost or stolen devices, management of user accounts and data privacy are examples of BYOD challenges which affect security. These challenges have an impact on data confidentiality, data integrity and data availability (Gajar et al. 2013), so, it is necessary to understand the impacts of BYOD, which are discussed in section 2.2 under BYOD threats and challenges.

## 1.2 Problem Statement

In the BYOD environment smartphone users in organisations are allowed to use their own devices for their work. Although the BYOD model has advantages, such as the increase in productivity and cost reduction, these benefits come together with both security and privacy-risk concerns and the users are the main contributors of these risks.

However, there is a tendency to ignore the fact that user awareness of risk is also a part of the security strategy (Al Harthy 2013), which could result in non-intentional or even deliberate data leakage and other security breaches. The major security challenges in the BYOD environment will be: monitoring the network traffic, controlling the access of users, and the security policy of the organisation. It is imperative to achieve the business objective of a company, without compromising security policies and procedures (Miller et al. 2012). Information governance will play a crucial role in balancing the human factors with the technical aspects involved, in order to enforce effective information security in the BYOD environment. The BYOD threats and risks are discussed in the work of Ganiyu and Jimoh (2018) which mainly focusses on risk detection, and covers the risks factors and possible countermeasures.

BYOD also raises several ethical issues and challenges for the users and the business (Marilyn, et al., 2014). The research questions and objectives of the proposed research attempt to address the risks associated with the implementation of BYOD in an organisation.

The lack of security knowledge of users can lead to attacks on their personal devices, which in turn can lead to a loss of business data. For example, when a user downloads malicious applications, or connects to an open network without secure encryption, it can lead to a breach of data confidentiality. Furthermore, one of the BYOD risks, known as “rooting” or “jailbreaking”, where the changing of the security settings make devices vulnerable, is a particular concern. However, there are many other risks and attacks that can happen intentionally or unintentionally because of a lack of user-security knowledge. A detailed list of these are discussed in section 2.6.

## 1.3 Research Motivation

The most critical factor for maintaining the reputation of the organisation is maintaining a secure environment protecting: customer and employee privacy, data confidentiality, data integrity and data availability. A particular requirement of BYOD is that users should be aware of all security processes and procedures, as they are the owners of the mobile devices and the business cannot take any action without their agreement. Currently, there are many security measures which perform actions to secure the BYOD environment. However, these measures, such as mobile-device management, mobile-application management and mobile-content management focus on securing specific areas with specific features, which is a solution limitation. Additionally, implementing a solution combining all these measure is increasing the cost, so this research is proposing a security framework for BYOD in Oman organisations which will predict the risks and notify users accordingly. This research employs a novel approach, creating a dataset to predict the risks, which is a mixture of both mobile device and application-management logs.

## 1.4 Aim and Objectives

The aim of this research is to propose a risk management and security framework to minimise the risks in a BYOD environment.

## 1.5 Research Questions

The aim of this research will be achieved by providing answers to the following research questions:

1. What are the limitations of current BYOD frameworks and available countermeasures in general and in Omani organizations in specific?
2. How can the MDM events log and function log analysis can be used to improve the detection of imminent risks and the mitigation of malicious actions in BYOD environment?
3. How can existing BYOD risk-management frameworks can be enhanced to ensure the security of BYOD environment?

**Objectives:**

The research questions will be answered by the achievement of the following objectives:

1. To investigate the problem domain and review both existing and emerging technologies encompassed by the BYOD environment.
2. To conduct a field study in Oman to analyse the user awareness of the potential security breaches and their consequences within a BYOD environment.
3. To propose a framework that encompasses risk management and security governance.
4. To develop a prototype to measure the effectiveness of the proposed framework.
5. To evaluate and validate the proposed framework functionality and accuracy.
6. To publish this research work in international conferences and academic journals.

## 1.6 Thesis Structure

This section provides the thesis structure with a summary of the content of each chapter.

**Chapter 1: Introduction**

This chapter introduces the research topic and highlights the research questions, aim and objectives. It also discusses the motivation for conducting this research and the thesis structure.

**Chapter 2: Tools and techniques**

The main aim of this chapter is to provide an account of the tools and techniques used in a BYOD environment. The basic concepts of these tools and techniques are explained together with the BYOD domain and applications. Section 2.1 provides an explanation of the tools used in the various research phases. Section 2.2 briefly describes the structure of the hybrid network involved.

**Chapter 3: Literature review**

This chapter reviews the current literature on BYOD risk management from both a technical and user-awareness perspective, introducing both the concept and the risk management aspects of BYOD. The first part of the literature review discusses the different security challenges and threats associated with the BYOD environment. It also discusses the risk-management frameworks, and the current countermeasure techniques, such as Mobile Device Management (MDM) systems. The last section of the chapter introduces the risk-management process challenges and evaluates the widely used risk-management approaches, finding the gaps in the literature which need to be addressed by the primary research.

**Chapter 4: Methodology**

This chapter presents the research methodology adopted to answer the research questions, focussing on the primary and secondary data-collection and analysis, as well as the methods, techniques, tools and strategies used.

**Chapter 5 Survey Findings and Analysis chapter**

This chapter presents the findings of the survey, then, the results discussed in sections 5.2 and 5.3, together with the results of the literature review, will inform the development of the proposed framework. This chapter also achieves one of the thesis objectives which is: to conduct a field study to analyse user awareness of the potential security-breaches and their consequences within a BYOD environment.

**Chapter 6: Proposed Framework**

This chapter discusses the proposed framework which enables the effective prediction and management of the security threats in a BYOD environment. The framework enables the analysis

of MDM-log records and function log records and then applies organisational policies to manage security effectively. The chapter discusses the theoretical concepts of smartphone-security traffic analysis, the log datasets, and the approach used for data classification.

**Chapter 7: Prototype**

This chapter presents the prototype to evaluate the functionality of the proposed framework. The flow of the data through the classification process of the prototype is demonstrated. The chapter discusses the implementation environment, the steps followed to run the prototype, and the results.

**Chapter 8: Evaluation chapter**

This chapter provides details of the evaluation methods used for the proposed framework. The evaluation checklist and the analysis of the findings of the evaluators, are both included in this chapter.

**Chapter 9: Conclusion**

This chapter will summarise the thesis findings, then discuss the thesis limitations, and the future-research recommendations.

## 1.7 Summary

This chapter has given: a brief discussion for BYOD and its adoption in Oman organisations, together with the aim of the research, research questions, research objectives and the thesis structure. The following chapter will detail the basic tools and concepts which will be used during this research

# Chapter 2: Basic concepts and Background Technologies

## 2.1 Introduction

In order to achieve the aims and objectives mentioned in section 1.4 and 1.5 of chapter 1 the tools and techniques used in this research are discussed. The chapter is structured as follows: Section 2.1 explains the tools used in the various phases of this research. Section 2.2 briefly describes the structure of the hybrid network. Section 2.3 presents a functional description of the MDM system. Section 2.4 provides a brief discussion on machine learning. Section 2.5 presents the Support Vector Machine algorithm (SVM). The chapter then concludes with discussion of BYOD risks and threats.

## 2.2 Tools Used in this Research

This section presents the tools used, table 2.1 describes each tool, the name, the reason, and the phase of the research where it is used.

Table 2.1 Tools used throughout this research

| Research Phase | Used tool | Purpose |
|---|---|---|
| **Data Collection and investigation** | MDM mobile engine | To get the account of MDM activities from the log files.<br>To understand risks that affect the BYOD environment<br>To Understand the challenge of hybrid networks |
| **Analysis** | excel | To find the BYOD security challenges and gaps in Omani organisations.<br>Survey 1 and Survey 2 |
| **Classifications** | Machine learning SVM, NetBeans | To classify the normal and malicious activities |

## 2.3 Hybrid Network

Today computer networks within organisations contain different layers of connections, which are either domain connections or external connections. A network can contain standard domain-connections, cloud-based connections, BYOD-device connections, IoT devices and IOT-network connections. If the network provides more than one network path and connections, it is termed a hybrid network and may contain a combination of multi connection layers for different technologies. The hybrid network also noted as smart grid network.

The main advantage of the hybrid network is that there are multiple service-provider connections for each technology. That means that there can be different connections for IoT devices, cloud services and BYOD devices. These alternative connections have the advantage of reduced delays and a balanced load, when the service provider of the cloud is different from the BYOD device-connection provider. Also, the reasons which cause organisations to move to hybrid networks is to achieve a balance of system control between legacy devices and new technology (e.g. IoT, Software Defined Network (SDN) and cloud control challenges). However, upgrading of a networks to hybrid network leads to different security challenges and risks.

Pradip Kumar Sharma, Jong Hyuk Park (2018) analysed the hybrid network security challenges such as data processing overload, network delay and single point of failure of the gateway. Whereas Sudhakar Sengan et al. (2020) analysed the hybrid network security challenges from a different perspective, such as multi-access methods control which are concerned with privacy risks and data transaction risks.

Elbasiony, R.M., et al (2013) state IDS related risks detection methods and counter measures in hybrid network. For example, current counter measures and detection method of intrusion detection systems (IDS) may not be able to detect network traffic correctly in all cases. Some old detection mechanisms may not be suitable for detecting risks in mobile traffic. However, hybrid networks inherently have dealt with huge data traffic from different sources such as cloud traffic, mobile devices and IoT devices traffic, which require effective risks detection mechanism to deal with these different sources of the traffic.

BYOD traffic is one of hybrid network traffic sources which raise the security concern as well. Hence, securing remote access traffics from BYOD devices become a priority in term of security strategy developments in today's business. The security attacks and risks which may occur in hybrid network such are Denial of Service attack (DoS), Man In Middle Attack (MIMT) and security Socket Layer (SSL) attack are also relevant to BOYD environment. Upasana Raj and Monica Catherine S (2015) discussed the BYOD threats and security requirements with hybrid networks, where they propose a hybrid authentication system, which include many authentication services and factors to help in verifying the users who are accessing services from mobile devices, cloud computing and local area network (LAN).

## 2.4 Mobile Device Management

The Mobile Device Management System (MDM) is a cloud-based system which helps in the management of all types of mobile devices such as smartphones, tablets and laptops. The MDM system provides various levels of BYOD management, such as application management, content management, remote wiping, tracking device-locations and management of security. As this research focuses on security factors, MDM can be used to create a secure BYOD-environment by controlling the mobile devices of users. Controlling means the ability to enforce password strength, to wipe and recover data from smartphone users and to secure the devices by detecting malicious applications, because there is always the risk that these controls can be bypassed. However, in this research, the MDM system is used to collect MDM activities from MDM logs in order to gain a deeper understanding of BYOD risks and threats. Although MDM has the ability to exert a certain level of control on mobile devices, it lacks the ability to detect function-level abnormalities in applications.

This research is concerned with smartphone risk-detection and management in the business environment. It is imperative to design a system which can manage smartphone security-threats within an organisation. MDM is a system which is used as a security layer in the BYOD environment which monitors and evaluates the functionality and data utilisation of smartphones, especially the organisation data which is stored in the personal phones.

There are three levels of security in MDM

- Device security: which mainly focuses on the hardware level and physical security, such as detecting the loss of devices.
- Data security: which detects blacklist applications and ensures that data can be wiped remotely in the event of device loss.
- File synchronisation: which is mainly about data transmission and storage.

**MDM Architecture**

MDM has the following components:

- An MDM agent: It is a small application installed by users on their mobile devices to allow the enterprise administration-team to control the device.
- An MDM server: It is the controller where an administrator can set all the policies and monitor all the mobile devices. Additionally, it has a dashboard which displays the MDM device-information such as the operating system, installed applications, any new installations, or any policy breaches.
- An MDM channel-gateway: It is the interface between the agent and the server which assign the MDM to demilitarized Zone (DMZ). DMZ acts as a security zone between the borders of the public and private network (Meisam Eslahi1 et al. 2014). DMZ zone works to isolate the services with high internet access from the private parts of the networks to enhance the access control and intends eliminate the attack to private networks. However, the MDM server will be in contact with MDM agent in internet and authentication server in the local area network.



Figure 2.1: MDM general architecture, (Meisam et al. 2014)

### 2.4.1: MDM Functionality:

The MDM system detects smartphone traffic, which helps to identify the number of mobile nodes accessing the network. Additionally, the system gets the control-level details to manage the risks and threats effectively. MDM enforces an effective policy for different smartphone operating-systems. After the enrolment stage, the mobile devices are synchronised with MDM, which detects all apps installed on the user smartphone. Additionally, the MDM administrator has the right to wipe phone data which can be either a complete wipe for all the data in the phone, or a corporate wipe which only wipes the business data in a specific folder. However, the version of MDM most appropriate to the needs of an organisation should be carefully selected.

### 2.4.2 Types of Mobile-Device Management System

To enhance the detection, prediction and management of risks by the BYOD, MDM event-logs will be used. The fundamental purpose of MDM is to provide countermeasures for BYOD risks. Thus, it is imperative to study and identify the features and differences of the MDM systems available from different vendors (Caldwell et al. 2012).

**MaaS260**

MaaS260 is a mobile device management-system produced by IBM. This MDM solution can support smartphone platforms such as iOS, Android, Windows and Blackberry. Maas260 MDM provides functionalities which include tracking, remote control and the wiping of data. Additionally, MDM helps to follow the mobile-experience management which is responsible for mobile-update dispatches. As noted by (Rhodes and Junis 2012), this MDM requires the BYOD user to carry out self-registration.

**Manage Engine**

This MDM supports all major platforms except Blackberry. The Manage-Engine MDM provides features to track, control remotely and wipe data. Additionally, the organisation can control the

documents that are shared with MDM users by MDM agents. The Knox platform provides an MDM to support Android smartphones, which enhances the secure connectivity between the MDM server and the user.

### VMware Airewatch

VMware Inc. have developed the Airwatch MDM which will support all major operating system platforms except Blackberry. The main features of this MDM are tracking, remote control and wiping of data. Additionally, it provides virtual and digital workspace and supports Android, and Knox operating systems.

### Microsoft Intune

The Microsoft Intune MDM supports all mobile-device platforms except Blackberry and provides features for tracking, remote control and the wiping of data. (Rhodes and Bettany 2016).

### MDM Operational-process

This section explains the process for enrolling smartphones on the MDM server, as well as generating and extracting MDM logs. Figure 2.2 shows the smartphone-enrolment process, allowing the user to install the MDM agent on their mobile devices and grant permissions to allow the device to access resources from the network. The enrolment address appears as a bar code or URL address in the MDM system which is passed to the user to enable the enrolment process for the smartphone.

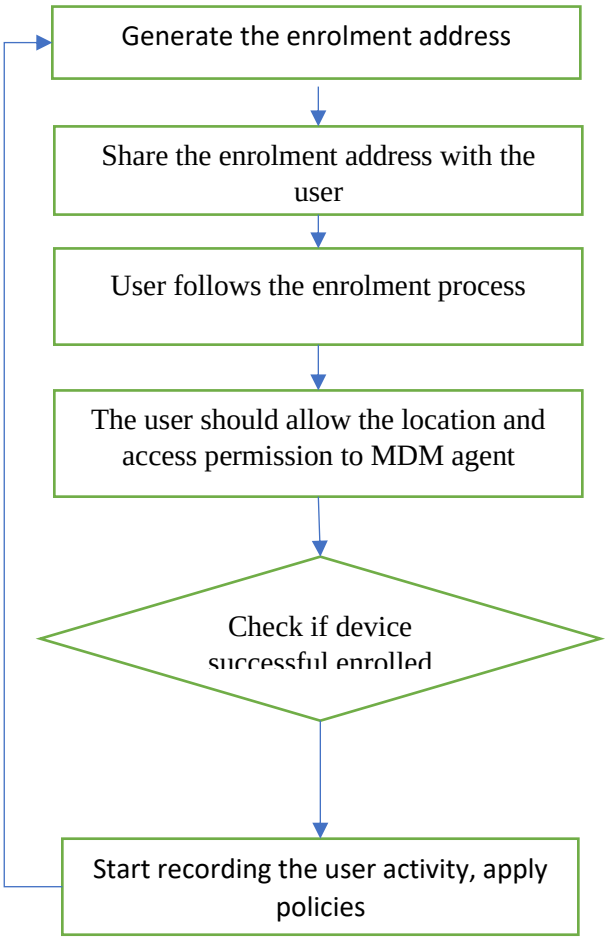



Figure 2.2: Device Enrolment in MDM

The MDM enrolment steps in the initials stages are different for Android and iOS operating systems. For enrolling iOS devices, the MDM configures the Apple Push Notification (APN) certification. APN is a cloud-based certification for the enrolment of Apple devices, ensuring that users follow a specific set of guidelines. For Android devices, however, certification is not required. Users can scan a barcode to install an app called M-MDM or access a shared URL. After the enrolment stage, the mobile devices will be linked with the MDM server. This synchronisation process will detect all apps installed on the user smartphone, as well as distributing apps from the Google Play Store as required. By using MDM, the administrator can monitor and track the location, or, in the event of loss, lock or wipe all the data on the device.

However, the MDM also detects the applications which are categorised as “blacklisted”, then, the user will receive a notification email stating that the blacklisted apps must be removed within a

specified period of time. This notification allows the user to backup any associated data before the app is removed automatically by the MDM server. The features of the MDM are described below.

### 2.4.3 Mobile Device Management Functioning:

Running MDM in the network means running a set of services which support the connected smartphones (Barthwal 2016; K Ortbach, 2014). The following subsection describe the set of features, functionalities and operations supported by an MDM system.

1. Enrolment

To manage smartphones which contain business data the administrator should enrol the devices on the MDM system. The enrolment process will download the MDM agent on to the mobile phone and set permissions on the server to control what the user can do.

2. Distributions

After MDM detects the enrolled device, the next step is to start the distribution of the organisation policies. Based on the characteristics of the device an organisation profile will be installed. The use of profiles enables the placing of restrictions on the device to protect network resources.

3. Detection

The MDM system automatically detects the device type, operating system and installed applications. The detected applications will be classified as “whitelist” or “blacklist” based on security requirements. The administrator can set a detector for the mobile-application installation process for a user smartphone, so, when the user downloads an application, it will be considered as blacklisted by default. The new applications then stay as a blacklisted application until it is verified by the administrator. The administrator then has the ability to change the application category manually from “blacklist” to “whitelist” if there was no malicious content or activity. The MDM system will then send a notification mail to the phone user to remove any blacklisted applications within a specific time period. The figures 2.2 demonstrate major processes for blacklisting applications.

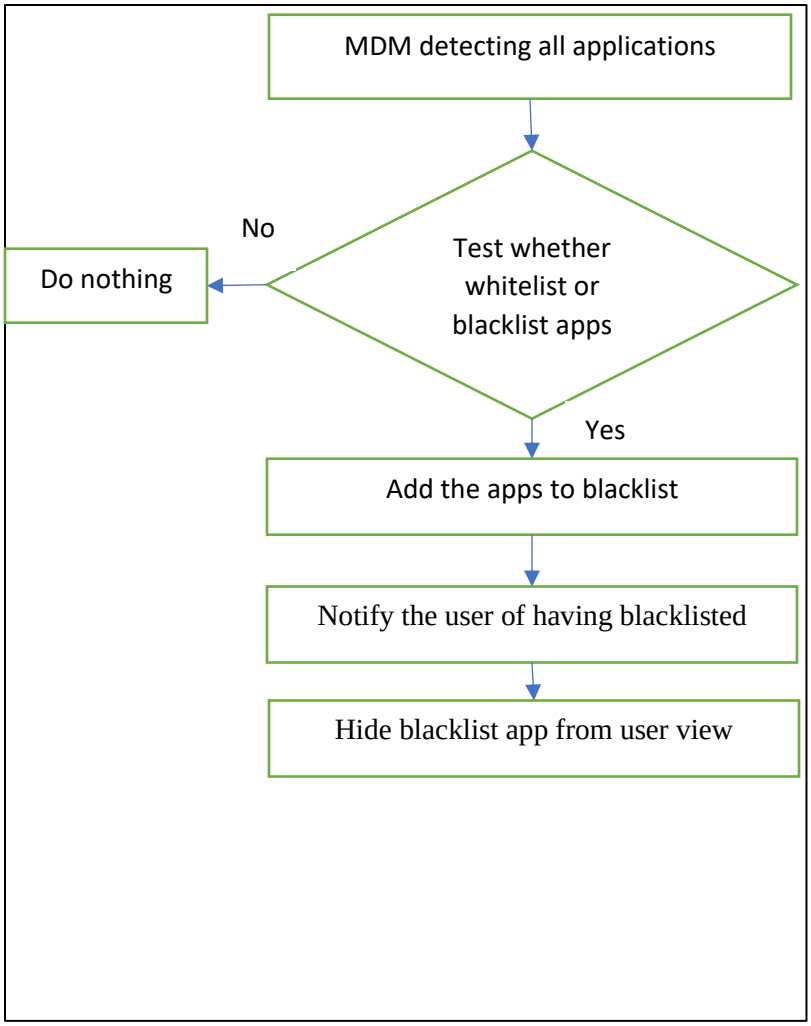



Figure 2.3: Process of Marking Blacklist Apps

4. Inventory

The main purpose of the MDM system is to give the administrator control of security in the BYOD environment. The most drastic threats in BYOD environments are loss of data, disclosure and loss of confidentiality. Therefore, the administrator is able to trace the device location. And the MDM will then enable the remote blocking or wiping of the device where necessary.

5. Admin and Reports

All management and security functions and services in the MDM system are recorded and the system can provide security reports where required. These reports will identify devices which have had their operating systems corrupted by "jailbreaking" (on iOS phones) or "rooting" (on Android

phones) creating a security risk. Other security reports are the applications reports. Additionally, server logs are also available for further analysis and checking.

6. Tracking lost devices

MDM is also used to track the connected devices' locations. In case a BYOD user reports that his device has been lost then MDM admin runs the tracking locations service to track the lost device. Figure 2.4 explains the flow of lost device service in MDM and the actions that will be taken.

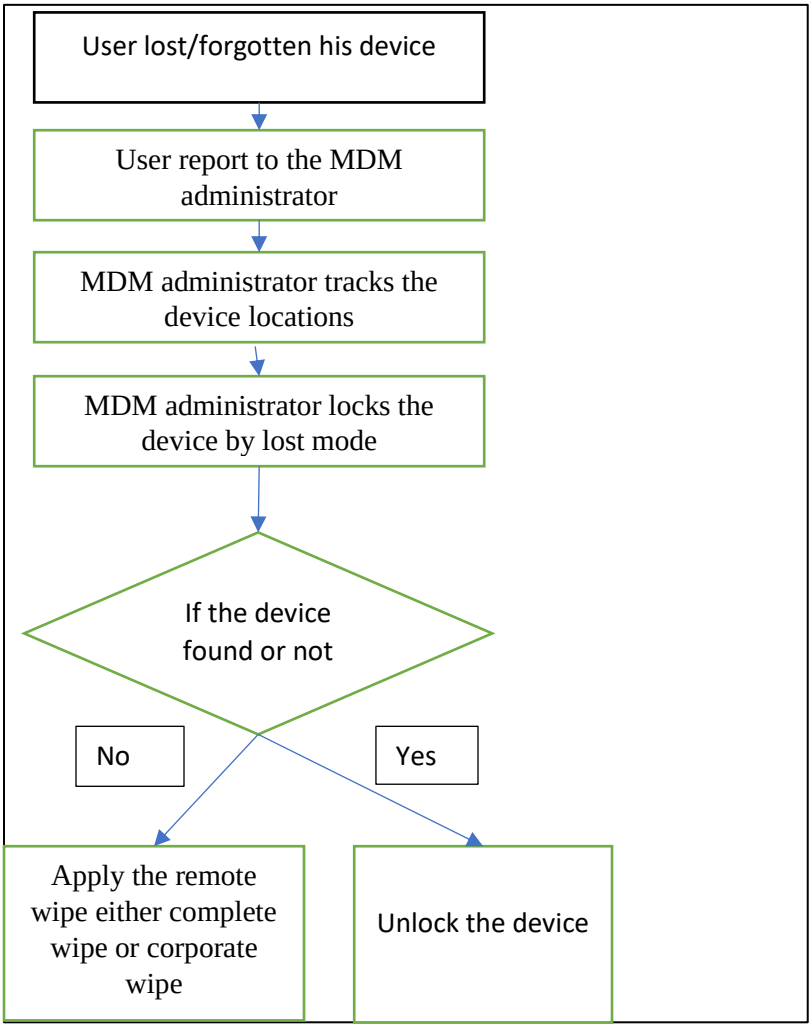



Figure 2.4: Process of Lost Devices

Therefore, with all of these MDM user activities and MDM services, the log records will be recorded for future review and audit.

**Limitation of MDM**

Researchers have identified MDM itself as having some security vulnerability, as well as operational limitations which reflect on the system performance (Guo, et al., 2004; Downer and Bhattacharya 2015; Leavitt, 2012). In order to address these issues, mobile application management (MAM) and mobile content-management (MCM) systems have been introduced by researchers as countermeasures to manage BYOD security (Yamin and Katt 2019). However, these systems focus on data security. Although, MDM focuses on both content and application security (Dhingra, 2016), it cannot detect malware on a phone and it can only manage the data traffic.

The research of Mohammed Ketel (2018) noted that MDM mainly focuses on management and control of BYOD security issues rather than network security which creates a vulnerability that can be exploited by hackers (Ketel, Mohammed 2018).

## 2.5 Machine Learning

Machine learning (ML) is an artificial-intelligence concept which aids systems to learn automatically learn from past data or experience. Additionally, machine learning is used to create a model which builds on different attributes and parameters. These attributes help to predict the future or gain knowledge by analysing a given dataset (Alpaydin and Bach, 2014). ML consists of a number of functions, which include classifications, clustering, and evaluation and can produce good results (Matthew and merriam 2002). The machine performs the learning in 6 steps, which are: data collection, data cleaning, choosing the model, training the model, evaluation and parameter tuning. Jordan and Mitchell TM (2015) define machine learning from two questions. Firstly, “How can one construct computer systems that automatically improve through experience? Secondly, “What are the fundamental statistical, computational, and information-theoretic laws that govern all learning systems, including computers, humans, and organisations? Eric Horvitz and Deirdre Mulligan (2015) stated that the machine-learning process helps to disclose issues and understand the behaviour of data. They proposed methods for enhancing data privacy by machine learning. Machine learning is used to increase the accuracy of results and help in decision making using specific processes which are: classification, recognition, clustering and regression. Nguyen

et al. (2016) define classification as dividing the data into a class based on its functions and attributes but define clustering as dividing the data into groups of small streams of data. Fallahzadeh, R. and Ghasemzadeh, H., (2017) define machine-learning recognition as teaching the system to detect and monitor physical and biological conditions such as face recognition, eye recognition and disease detection, and classification assists in the decision-making mechanism.

ML has been widely used in the field of IT security to enhance the available security methods and can be categorised based on its function as follows:

Supervised machine-learning: With this form of ML, both inputs and anticipated outputs must be provided. Supervised-learning algorithms can produce classifications after the completion of model training and uses a labelled training-dataset for the prediction process. Supervised machine-learning methods have been used in IT security for the classification of spam, malware and face recognition etc. The well-known supervised machine-learning algorithms are decision-tree algorithms, native-based algorithms and SVM algorithms.

Unsupervised machine-learning: This type of machine-learning approach, which is used for more complicated data analysis and classification, does not need the anticipated outputs to be provided, and supports clustering to allocate the data into a group with particular attributes. This method functions without setting the desired output and non-labelled data, such as regular text can be processed. Unsupervised machine-learning algorithms can be used for factor analysis, such as the algorithm for K-mean neighbours.

Semi-supervised machine learning: This is a combination of both supervised and unsupervised machine-learning methods, which outperforms supervised machine-learning, reducing complexity and requiring less computation for large data and less human resource effort for labelling. By combining both supervised and unsupervised machine-learning methods, semi-supervised machine learning provides for the processing of both labelled and unlabelled data and can be used for classification and regression (Chapelle, et al., 2009).

Reinforcement machine-learning: This type of machine learning, where the algorithm uses a portion of the data for training, is designed to process large streams of data, characteristic of gaming and real-time video applications,

Machine learning has been adopted in this research for the prediction of abnormal events in the BYOD environment by using classification of the data. A more detailed description of this is discussed in the framework chapter section 5.2.2. The following section presents the SVM being used in the proposed framework.

## 2.6 Support Vector Machine Algorithm (SVM)

The SVM algorithm can be applied for both linear and nonlinear classification. SVM is a binary classification algorithm which maximises the margin between classes (Mavroforakis, M.E. and Theodoridis, S., 2006). It can cope with classifications having up to 100 features in the dataset. Additionally, it provides a high rate of accuracy with either a short or long training time. SVM works by mapping data to a class using a hyperplane and margin value. A hyperplane is a line that separates two SVM classes, and the margin is the distance between the hyperplane and the class as shown in figure 2.4.

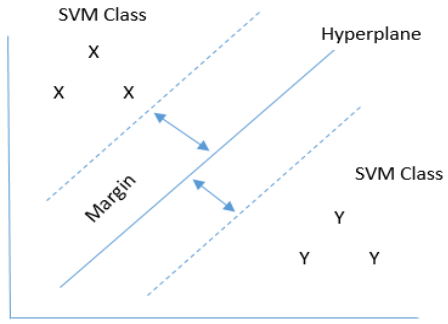



Figure 2.5: SVM classification

SVM is classified as supervised machine-learning, which require both the inputs and the anticipated results and can produce classifications following completion of model training.

This research has adopted SVM to classify the BYOD data and was chosen because only two classes needed to be generated from the data which were normal and malicious actions.

## 2.7 BYOD Risks and Threats

As a risk-management framework is being proposed in this research for the BYOD environment, this section covers the definition of risks, threats and vulnerabilities and then discusses some of the BYOD risks and mitigation actions.

### 2.7.1 Risk

A risk is the likelihood of threats to the vulnerability of an installation which can lead to data loss or a breach of data confidentiality or data integrity within an organisation (David Watson, Andrew Jone 2012). Risk = Threats x Vulnerability where the level of risk is determined by the vulnerability and the threat level is determined by the impact and likelihood of the threats.

In a BYOD environment, risks can be categorised as internal or external. The internal risks are risks which emanate from the internal environment, such as an employee breaching the security policy. The external risks are risks that come from the external environment, such as an unauthorised access or network-connection breach.

### 2.7.2 Threats

Threats are dangers which may or may not happen and exist because of vulnerabilities in any of the technology deployed by the organisation. The threats can happen intentionally or non-intentionally, Intentional attacks include denial of service attack, phishing attack or backdoor attack, whereas natural disaster threats such as floods are non-intentional.

### 2.7.3 Vulnerabilities

Vulnerabilities are a weakness in the procedure's technology, hardware or software (Dahbur, et al.2011). They can be described as a weakness or gap in safeguarding data, computers or networks. For example, a weak password, misconfiguration, an improper network topology or an unclear policy.

A BYOD risk is a possible malicious impact which targets and affects the BYOD environment or user. This risk can result in the BYOD devices being used as a gateway to the organisation and its network resources. The following table 2.1 presents the BYOD risks together with the possible threats and suitable mitigation plans. The plan, which is shown for both organisations and individuals represents actions, which are the safeguarding steps required to avoid and maintain the risks at an acceptable level. This plan helps to undertake risk assessment and management for the BYOD environment. The mitigation is a selection of proper actions which aid in the detection, prevention and correction of the risks.

Table 2.2 BYOD risks with possible threats and mitigation plan

| **Risks** | **Possible attacks and threats** | **Mitigation plan** |
|---|---|---|
| **Access organisations resources through unsecure network** | Effected by malicious attacks; virus attacks, data theft and unprotected | User awareness to use VPN as a secure channel. Use of VPN |
| **Employees not aware of their activities' risks** | Lead to increase threats and attacks possibilities | Increase the user awareness level such as training, and awareness notifications |
| **Losing device which contains organisation data** | Exposing of business data | Remote wiping and remote accessing (selective wipe or general wipe)<br>Track the device location<br>Lock the device till returned |
| **Losing organisation reputation** | losing data confidentiality and privacy | Update the policies |
| **Malware infections** | Untrusted applications installed | Mobile anti-malware, restrict application installation from MDM |

| | | |
|---|---|---|
| **Untrusted applications** | Backdoor attacks: signature attack, phishing | Restrict application installation from MDM<br>Add application in Blacklist in MDM |
| **Network and web** | DoS attack to cloud services or application servers | Update the countermeasures for traffic filtering and alarming when high bandwidth and traffic observed. |
| **Exceeded the number of access-failure attempt** | Breach the user account unauthorised access | Reset password and keep monitoring the account for further checking.<br>Use two-factor authentication |
| **Rooting and jailbreaking** | Access to devices<br>Improper manufacture features<br>Malicious apps | Monitor the devices through MDM reports and take preventive actions |
| **Legal challenges** (Dhingra, M., 2016) | Policy weakness<br>Legal issue in storing data | Updating and reviewing the policy and procedures |
| **Lacking current countermeasures in managing BYOD risks** | Any attack can happen in the area lacking countermeasures | Update the security systems.<br>Ask security team to do penetration to discover the gaps.<br>Ask the users to report the incidents. |
| **Lack of device management** | Losing data confidentiality<br>Data leaking | Implement MDM system |

| | | |
|---|---|---|
| **Incompatibility of BYOD risk strategy to all smartphone operating systems (Shumate and Ketel, 2014).** | Malware can attack one operating system and not others<br>Security control cannot be a function of an operating system because of manufacturer security-settings. | Plan the risk management and security strategy before adopting BYOD to cover all your employee OSs. |
| **Jailbreaking and root (Vinh, et al., 2020.)** | Users remove the default settings to run some applications making the devices vulnerable to unauthorised access and data thefts. | Keep monitoring the jailbreaking and roots cases through MDM.<br>Notify the users of malicious applications if jailbreaking cases appeared. |

## 2.8 Summary

This chapter has discussed the tools and techniques that will be used in this research. This discussion helps to understand the purpose of the tools, techniques, and concepts in the proposed BYOD risk-management framework. A hybrid network has been presented to understand the network architecture within a BYOD environment. Additionally, this chapter has defined BYOD risks and threats together with suitable mitigation methods. Furthermore, this chapter has discussed the basic methods and tools which will be part of the proposed framework which are: MDM, machine learning and the SVM algorithm.

The next chapter summarises the current knowledge in the literature regarding BYOD.

# Chapter 3: Literature Review

The literature review chapter is an important part of all research as it highlights the work of other researchers in the same domain. The purpose of a literature review is to review and critically analyse the current knowledge of the topic area. The analysis identifies the gaps between the current knowledge and the information required to answer the research questions.

## 3.1 Introduction

This chapter reviews the current literature for the Bring Your Own devices (BYOD) risk management. BYOD is an approach which allows employees to use their own personal smartphones or tablets rather than the devices supplied by the workplace (Brooks 2013). The application of BYOD has shown increase during COVID-19 pandemic. A large number of organizations allowed their employees to work from home and used their personal devices to complete the work tasks (Lallie, H.S., et al 2021).

This chapter is based on the research question (see Chapter 1.5), "What are the limitations of current BYOD frameworks and countermeasures". Also, it covers the objective of this research which is to investigate the problem domain and review both existing and emerging technologies encompassed by the BYOD environment.

Section 3.2 discusses the different security challenges and threats associated with the BYOD environment and the existing risk-management frameworks. It also examines the current countermeasures for the risks, such as mobile-device management systems. Section 3.3 presents the challenges in the risk-management process and evaluates the widely used risk-management frameworks. Section 3.4 discusses the research contributions for machine learning and SVM. Figure 3.1 shows the areas that covered throughout literature review.

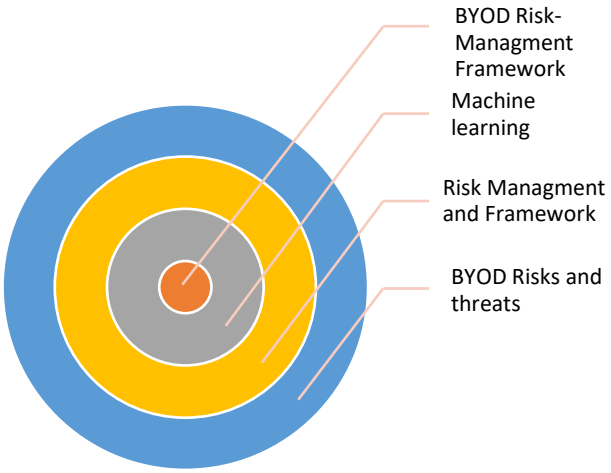



Figure 3.1: Literature Review Structure

In their research, Oktavia, T. and Prabowo, H., (2016), found that the BYOD environment was subject to security threats and challenges, which are discussed in the next section.

## 3.2 BYOD Security Threats and Challenges

With the integration of personal mobile-devices into the business environment, the landscape of IT security for organisations has been changed (Eslahi, Salleh, and Anuar (2013). In their paper, Ghosh et al. (2013) pointed out that BYOD, by the integration of business data into personal devices, raises a data security issue which causes problems at both the personal and business level. At the personal level it is a breach in the privacy of user data and at the business level it loses control of business information, reputation and money (Chen et al. 2013; Assing and Calé 2013; Zulkifli et al. 2015).

Ismail et al. (2017) classify BYOD attacks into intentional and non-intentional. They state that the actions taken by users may lead to loss or leakage of the data. These non-intentional actions could be due to human error, a lack of threat awareness, loss of storage, or missing security procedures. Recognising that intentional risks and threats refer to information sharing with unauthorised people, they propose a taxonomy which helps to reduce the threats which come with non-intentional activities from the users.

The following subsection will discuss BYOD attacks and their associated categories.

### 3.2.1 BYOD Attacks

As noted in the literature, the BYOD environment attracts different categories of risks and attacks, which will be covered in this section. Priscilla Boadi et al. (2018) discusses the BYOD vulnerability matrix where BYOD risks are classified as: people (such as misuse technology and privilege), technology (mobile devices, operating systems and applications) and process (such as policy). The following subsections discuss how they impact the current network, user security, business security and privacy.

**Personal Attacks**

These types of attacks target the personal information of the user, such as social-media accounts, e-mail, contacts and photos (Bell 2013). The personal attacks have serious consequences, because the attacker is impacting personal data and business information. A lack of user knowledge of the possible attacks and malicious actions, makes them victims of these attacks (Scarfo 2013). They can happen to the smartphone itself or any connected smart accessories. The literature shows that the modern smartphone has many connected e-accessories, which can display much of the information it contains, making these devices, such as personal smartwatches, vulnerable to attack (Siboni et al. 2018).

**Application Attacks**

The explosive growth of the number of mobile applications has caused an increase in smartphone traffic and made it difficult to track the smartphone-user behaviour (Chen, et al. 2017). The application attacks are generally more dangerous and challenging (Lounsbury 2013; Krombholz, et al. 2013; Spoorthi & Sekaran, 2014). Since some of the mobile applications are linked through cloud computing and installed in a virtual environment, CEO's and IT managers recognise that a number of attacks occur through the application connections and traffic. Some examples of these attacks are malware, viruses, application-permission hijacking, as well as untrusted or unknown developer-manipulations of application coding (Chen et al. 2013, MOROLONG et al. 2019)

As previously discussed, attackers take advantage of the lack of knowledge of the user and fail to set access permissions to prevent "backdoor" attacks on the applications. Shila et al. (2017) identified the challenges for current security-systems, with applications deployed in cloud servers, which can be subject to various kind of attacks. This issue has been highlighted by Khairun et al (2017) in studies of the challenges for adopting BYOD in higher-education establishments. They stated that challenges faced were due to the downloading of unauthorised applications, such as malware, which has led to the unauthorised access of networks. Furthermore, the lack of user knowledge in identifying malicious applications has also affected the other network users.

Lounsbury (2013) and Birchall (2014) both agreed that mobile applications and services which are accessed through cloud computing has increased the level of attacks in the BYOD environment. These can occur through malware, phishing, electronic-signature theft and poor authorisation checking. High levels of traffic and the need for network compatibility has increased the security implications and the possibility of attack in the BYOD environment (Howard 2008). This demonstrates the importance of recognising the security challenges for network administrators (Atallah et al. 2006; Ra et al. 2010; Conti and Giordano 2014).

**Network and Internet Attack**

The computer-network architecture has been built to provide centralised management to the services and user devices which are owned by a business. Therefore, the traditional security countermeasures in the networks such as firewalls, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS) and router filtering, are used for securing both users and services under one domain, either a LAN or a WAN (Roberts and Issler B. D 1970; Ioannis Andrea et.al 2015). However, the concept of centralised management is not applicable to current technological environments such as cloud computing, virtualisation and BYOD. Because personal mobile devices such as laptops, smartphones and tablets are connecting via remote access, the number of network attacks has also increased (Eslahi et al. 2014). The effect of these attacks has been reflected in the traffic security. As noted by Siboni et al. (2018), with the rise of IoT and BYOD, vulnerabilities and risks have increased and the need for cybersecurity has also increased.

K Downer and M Bhattacharya (2015) analysed the BYOD security challenges by dividing them into four categories as shown in figure 3.2.



Figure (3.2): BYOD Security Challenges (K Downer and M Bhattacharya 2015)

**Policy and Legalisation Risks**

The challenge most highlighted in research for the adoption of BYOD is the ability to control personal devices which contain business information. The BYOD environment needs to be covered by legal policies and ethics considerations. Carla J. Utter and Alan Rea (2015) in their research, had highlighted the BYOD legal issues, and organised them based on their impact, such as the ownership of data and access permissions which were the main points discussed. Furthermore, Ratchford, M. et al. (2018) agreed that BYOD legal control was a challenge, especially if the organisations needed to prove ownership of the data held on personal devices. Therefore, personal and organisational privacy are the most critical legal issues in a BYOD environment.

After discussing the key categories of BYOD threats, the following section discusses the individual BYOD threats and risks in more detail.

### 3.2.2: BYOD Risks and Threats

The main interest of this research is risk management in the BYOD environment, therefore this section will give brief details of the risks and threats in that environment

### A. **Access Through Unsecure Network**

The lack of user awareness regarding the risks of using business resource over open and public networks can make users victims of phishing attacks. Access through open networks poses a threat to the data of: BYOD users; business-network users; any information vulnerable to data sniffing; Man-In-the Middle Attacks (MIMA); and different types of viruses and malware (MOROLONG, M 2019).

Lallie, H.S., et al. (2021), highlighted that social engineering was one most prevalent attack in BOYD during COVID-19 pandemic. With the increase of virtual environment and information exchanges, the hackers are trying to get the information and gain access to the network resources and manipulate data. Hence, they proposed a protocol that focuses on employee behavior and awareness.

### B. **Loss of Devices**

The theft of smartphones from BYOD users, places at risk the personal and business information held on those devices. The work of Yong Wang et al (2014), shows that data stored in BYOD devices as plain text makes it easily readable by thieves. The challenge is not only losing the hardware devices themselves, but that business contacts, data and files stored on them could end up in the public domain, putting at risk the reputation of the business. A paper by Tu et al. (2019) points out that if the data on these devices was lost then privacy and legal issues could also arise.

### C. **Malware Infection**

Adopting BYOD can lead to malware infection of the business network. This is because mobile devices have limited resources for the deployment of security applications. Peng et al. (2013) stated in their research that users can download malicious applications on to their smartphones which will distribute the malware to other devices on the connected network. When smartphones and other mobile devices are infected by malware it will affect other network users in different ways, such as fake antiviruses and email hijacking and spreading of malicious mail attachments (Gudo, M. and Padayachee, K. 2015).

### D. **Untrusted Applications**

Andrea Vaca Herrera et al (2017) state in their research that most of the risks in the BYOD environment are associated with users installing untrusted applications. These applications can contain malicious code that can lead to "backdoor" attacks, which negate authentication procedures allowing unauthorised access to the user device. The article by Bill Morrow (2012) also identifies the risks posed by careless users installing mobile applications, stating that attackers can target BYOD users with malicious applications to extract business information. Additionally, some users do not take adequate care when keeping network resources, such as mail and SharePoint, open on their smartphones, allowing intruders to access applications and gain access to company data.

### E. **Rooting and Jail Breaking**

According to Harris and Patten (2014), rooting and jailbreaking is a risk which appears when a user tampers with the security settings installed by the manufacturer of the smartphone (called "jailbreaking on IOS devices and "rooting" on Android devices), García, L. and Rodríguez, R.J., (2016) discuss the impact of jailbroken devices as the most targeted smartphones for malware which can push malicious applications on to the business network. As well as considering devices that have been tampered with in this way to be a risk for the organisation networks, some researchers (Ansgar Kellner et al (2019) consider it as an attack.

### F. **Policy Breaching**

Information-security strategies include policy, procedures and standards. Policy is a control measure for managing user behaviour (Palanisamy, et al., 2020). Palanisamy, et al (2020) discuss the main risks which lead to the breaching of BYOD policies. Another example of BYOD policy non-compliance is when users share resources with unauthorised people, breaching the access privileges. This could be the sharing of data through smartphones which contain business data, as well as sharing resources with unauthorised people, both of which are considered as a policy breach. Too strict a policy can also led to policy breaching, especially if users are not happy about the use of their personal phones being controlled by business policy. Also, unclear policy

guidelines can lead to policy breaches where users are unaware of what they should or should not do.

The challenge is not only detecting the security threats and risks from the smartphones but also having effective methods in place to prevent them. The following section analyses the current countermeasures and the challenges of dealing with the BYOD risks and threats.

### G. **Threats in Cloud Based Environment**

Martin et al., (2017) discussed the security tools that can be used to manage the BYOD, IoT and cloud-based services traffic over the cloud. The most vulnerabilities in cloud-based environment are traffic based attack from IoT and mobile devices. Hence, they apply the honeypot and honeynet as security mechanism. Moreover, Adurey Asente and Vincent Amankona in (2021) discovered that the BYOD threats still occur at networking level and cloud-based services level. Hence, they propose a Digital Forensics (DF) solution which helps in collecting the threats data from different layers of network.

### H. **Tracking Polices and users privacy.**

Hovav and Putri (2016) through their research highlighted the user factor in term of BYOD policy enforcement and tracking. The users have feelings that they are restricted through their personal devices' usage. Moreover, the users believe the application of the policies compliances and tracking act as a barrier to their freedom of using the device. Additionally, other research efforts found that the users believe that this type of actions disrupt their work or even slow down the devices which is also confirmed by Rathika Palanisamy et. Al. (2020).

MD Iman Ali and Dr. Sukhkirandeep Kaur (2020) analysed the threats and risks in BYOD environment. Their research classified the threats source as user and traffic. However, they acknowledged the challenge of making users to collaborate with security solutions provided by their organizations. Hence, researchers proposed a networking solutions including traffic and users protection by adopting encryption and Software Defend solutions as countermeasures.

### I. Threats Based on Operating System

BYOD is an environment which is based on smartphones and mobile devices connectivity. Therefore, there is a necessity to understand the security strength and weakness of different smartphone operating system platforms. The most challenges in BYOD environment are dealing with various operating systems such as Windows, iOS, and Android, which has different level of heterogeneity (Le, et al., 2018). Therefore, (AI-Qershi, et al., 2014) in their research compared the security threats and capabilities of iOS and Android operation systems. They compared iOS and Android based on the model defence, vulnerabilities and strengths aspects as shown in the following table. The table include the Strengths, vulnerabilities, and model of defence.



Figure (3.3): Capabilities of iOS and Android operation systems (AI-Qershi, et al., 2014)

However, Shivi Garg and Niyati Baliyan (2021) investigated the security issues and architecture of iOS and Android operating systems. They analysed the security gaps in smartphones from two sources which are web based and application based. Moreover, they stated that the Android

security is lacking in term of availability of source code as open source operating system, whereas iOS does not share its code, believing that it provides stronger security. Another view of comparison is that iOS is not easy to jailbreak. This is due to fact that both hardware and software is controlled by Apple. Data encryption in iOS is not configurable, therefore it cannot be disabled by the users.

### 3.2.3 Current Network Countermeasuers and Security Practices

Security should play a significant role in protecting the incoming and outgoing network traffic. Therefore, the following literature will discuss the traditional security countermeasures, which are currently used for network security. Additionally, the challenges imposed on countermeasures when dealing with BYOD threats and attacks which have different characteristics, are also discussed. The security countermeasures investigated in the following sections are:

- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Firewall
- Router Security

#### *Intrusion Detection System (IDS)*

Patel et al. (2013) discussed the features of intrusion-detection system (IDS) services within the cloud. This system is designed to maintain the security and privacy of data, users, and resources. Cloud IDS has been classified as layers which are network IDS-services, host IDS-services and Applications IDS-services, which can be combined with intrusion-prevention systems (IPS). Mitchell and Ing-Ray Chen (2013) observed that it has become necessary to propose many different enhancements to IDS. Enhanced IDS to deal with one of the most common current security issues which exist in mobile ad hoc networks (MANET), which was to perform advanced-level detection of attacks and mistrusted activities (Marchand, et al. 2017; Liu, et al. 2017). Muhammed and Ayesh (2019) note in their research that network-based IDS can be used for the security of BYOD but should be used in an environment with its own integrated level of security to enhance packet filtering, which are now not enough to run IDS only.

### *Intrusion Prevention System (IPS)*

Yamin et al. 2019 argue that current countermeasures for security threats, in particular the IDS, are inadequate for BYOD in the business environment. Abhishek Gupta (2019) discusses the limitations of IPS integrated with BYOD with the new smart-grid network. The paper points out how the protocols and threats which accompany the smart-grid network eliminate the filtering of content and addressing which is employed by IPS.

IPS has different trigger techniques and methods, based on patterns of functions such as behaviour-base prevention and anomaly-base prevention (C. M. Akujuobi, 2007; E. Carter 2006; kjeyil haslimm et al. 2008). The anomaly-based prevention contains a set of profiles containing normal activities, therefore, when an abnormal activity occurs, the IPS generates an alarm which classifies the activity level accordingly

The behaviour-based prevention is a combination of the well-known pattern prevention or anomaly-based prevention which takes the content of the activity and classifies it as either normal or abnormal behaviour (Frias-Martinez.V et al. 2008).

### *Firewalls*

Researchers have proposed different solutions to enhance the firewall manageability, such as the creation of different levels of functionality to control and filter smartphone traffic. Scarfò and Maticmind. S (2013) have proposed a solution for the BYOD environment, called the Cirtix IT delivery Model, which creates different zones containing two levels of firewall security. The proposed solution includes traffic filtering, clustering and the classifying of data from the BYOD environment before it reaches the network.

Due to the changing landscape of security, enhanced countermeasures have been proposed in current networks. Bohn et al. (2006) proposed an approach called SIREND which integrates with the stack schema and uses the current devices to enhance the security and management, to achieve the desired level of security in a hybrid environment. Framework dealing with controlling the services and applied the policy based on networking requirements. The authors proposed a clear division of the structure and protocols to enhance the network-security performance. However, this approach ignored the risks through services usage and other issues related to the BYOD trust scheme at the different layers and stages (Bohn et al. 2006; Dannewitz et al. 2013). Consequently, it was necessary to develop a system suitable for the BYOD environment which would enhance

the data management and mitigate the risks. Akande, A.O. and Tran, V.N., (2021) state in their research summary that the "failure to implement an effective information-security program can expose the organisation to significant security breaches and data loss".

Hence, with the appearance of the BYOD environment, multiple countermeasures have been developed to help the IT administrators and professionals to manage the BYOD-accessed resources and users. These are discussed in the following paragraphs.

Mobile Application Management System (MAM): This is an application-based policy which run the protection policy based on the organisation requirement. The application manager will apply a set of rules and download permissions before the user is able to use the applications (Rivera, et al., 2013). This is required because some applications run with permissions that asked the user to enable the application to access to files and locations. This breaches the data confidentiality of the business.

Mobile Information Management (MIM): This is used for storing information in centralised locations such as the private cloud and enables a limited set of BYOD users and applications to gain access to this information.

Mobile Device Management System (MDM): This countermeasure has been discussed in detail in Chapter 2.

The following section discusses the current BYOD risk-management system.

## 3.3 BYOD Risk Management Framework

Although MDM has been widely used to address security issues by determining the risks and providing assistance for decision making, Matulevičius, et al (2008) defined risk management as a method to address the risks by considering the impact and then to decide on the appropriate countermeasures. Ekelhart, et al (2009) also agreed with this definition and stated that risk management was an approach which evaluates, analyses and corrects the risk. Therefore, these researchers have both agreed that risk management is a process for controlling the risk which involves risk identification, analysis, monitoring and treatment.

Risk management leads to the mitigation of the risk at an acceptable level. Lalanne et al. (2013) declared that the motivation behind focusing on risk management was that previous systems were only concerned with users within the domain, but this has changed to networks facing risks from users with smartphones, and remote-access users via cloud channels (Lalanne, et al. 2013). They argued for the importance of building a database of the significant risks that are emerging from cloud and BYOD environments. Other researchers have also agreed that cloud and BYOD are generating new and unknown threats (KO & Choo, 2015; Saha & Sanyal, 2015). However, Ivan Veljkovic and Adheesh Budree (2019) have highlighted that to build risk management into the BYOD environment, all mobility elements must be considered. These should include flexibility of movement which make information available anytime and anywhere. Examples would be the mobile environment for users in motion; individual mobiles used for business data; and smartphones, laptops and tablets in the cloud.

This research focuses on proposing a risk-management framework for detecting and predicting risks which will contribute towards efficient decision making and the control of risks.

Yang et al. (2013) defined risk management for BYOD, as a system which is applied to secure staff devices and restrict their impact upon business information. They highlighted the main BYOD challenges, such as policy enforcement, risk-acceptance level and user behaviour. Also, to provide network compliance for a secure BYOD environment, the network administrator or security manager should evaluate and monitor the performance of the risk-management procedure with the support of security audits and organisation policy. Wilbanks et al. (2014) outlined BYOD risk management as controlling the risks which emerge from the integration of user devices such as smartphones and laptops in the domain network. Accordingly, all of the researchers mentioned agreed that BYOD brought with it a huge number of threats, which need to be addressed by policies, countermeasures and proper security processes. For that reason, a risk-management plan to cover the smartphone issues becomes mandatory for security managers.

Ratchford and Wang (2019) discussed in their paper the need for changing the security strategy from a “technology based only” strategy, to a strategy which covered four main areas, which were: management security, user security, mobile device security and IT security. They argued that consideration of these four areas would help in the building of a BYOD security module. They

also highlighted the need to understand the risks and level of vulnerability, define security control, and provide security-mitigation recommendations.

Additionally, the study of the literature showed that there were BYOD frameworks for dealing with specific type of attacks (Petrov.D and Zanti.T, 2018) which proposed security frameworks to secure the environment from DoS, privacy, and confidentiality attacks. Their work mainly focused on unauthorised access to a BYOD environment. Zeeshan. A and Nazia. B (2019) proposed a BYOD-security framework highlighting the security threats and possible mitigation measures, although the framework only focused on a limited number of threats.

### 3.3.1 Current Risk Management Process

The risk-management process identifies the action plan for the risks the main steps being risk identification, risk assessment, risk treatment, risk monitoring and review of risks. In this section each step of the process will be explained.

Risk identification: This is considered to be the first step in the risk management process, where the risk is defined, highlighted and understood (Ezrahovich et al. 2017).

Risk Assessment: This stage includes risk analysis and risk evaluation. Risk analysis examines the previously identified risks, and their impact, and is necessary to enhance decision making, and to reduce the possibility of risk occurrence in the future. The second step of risk assessment is to evaluate the solution and amend the existing standards and policies accordingly. This gives the security manager the ability to reduce the risks and the gaps within the system (Nagamalla & Varanasi 2017; Tanimoto et al. 2016)

Risk Treatment: This refers to the actions that can be taken in the risk-management system to control the risk. These actions can be classified to avoid the risk, reduce the risk impact, detect the risk or prevent the risk (Ezrahovich et al. 2017). The risk treatment step can also be part of the risk mitigation strategy which focuses on remedial plans (Agudelo et al. 2016).

Risk Monitoring and review: This is the last step of the risk management process, where the administrator and steering committee make decisions to track the risk to ensure that actions are in accordance with the policies and plans of the organisation.

To introduce and evaluate a suitable risk-management approach for the current BYOD security threats, different researchers have proposed different solutions and techniques which are highlighted in the following section.

### 3.3.2 BYOD Risk Management Solutions

Zhauniarovich et al. (2014) proposed a framework for the Android environment which focuses on enforcing the business policies for smart devices. Currently, smartphones contain hundreds of mobile applications which are developed by unknown or untrusted developers. Therefore, by downloading these applications, the user allows full access to their smartphone data. A security issue occurs when these phones are used for storing work-related data, which could be resolved by the complete virtualisation of the environment. However, applying this to smartphones would use too many resources which would be expensive, so using para-virtualisation is a cheaper solution, which can be managed through small devices. Para-virtualisation is a type of virtualisation that adds the operating system of the smartphone to the virtual machine.

Armando (2014) proposed the SMM workflow which applies a set of rules and filtering for a particular application based on the mode of application behaviour. This filtering means no application will be installed or downloaded by the client which either bypasses the SMM server or has not been verified as being compatible with the organisation policy. They also propose BYODroid, which is an Android application that supports the approach used in the paper by Armando. BYODroid checks the applications and gives security details to the end user. The proposed solution has a set of workflow procedures for the user to extract, validate and check the application, while comparing its behaviour with the business policy.

Additionally, there are research efforts which propose a security and availability architecture for the cloud and smartphones. The proposed architecture has been built based on the SABSA framework (Samaras et al. 2014). The proposed architecture uses BYOD to access the Software as

a Software as a Service (SaaS) component of the cloud environment. The design is a combination of both new-trend technologies and high-security challenges based on the work of legal, ethical and privacy experts. The proposed architecture contains five main layers, which are: connections, environment, resources, components and people. The proposed architecture has been built for a particular case study which was applied to an enterprise located in the European Union. In the case study, different access levels were applied to smartphone users where the data transaction, database access and connection via wireless were controlled, to maintain confidentiality, integrity and availability in line with the security requirements of the organisation. ISP 37001 was used to evaluate the security context, and FIPS was used to provide risk assessment, gap analysis and risk priority. Identifying the threats and vulnerability was highly recommended because it helped to identify problems, take remedial action and thereby reduce the threat impact (Singh 2013).

In their research, Nima Zahadat et al. (2015) evaluate the ability to apply the policy, which concerns application management and help reduce the BYOD risks. Hence, their proposed BYOD security framework discusses the process starting from device enrolment in the network through MDM until the device removed and wiped the data. Their framework depended on identifying the devices that gain access to the network resources and authenticate the users, then introduce the best security countermeasures and practices.

### 3.3.3 Risk Management and End Users

Agudelo et al (2015) studied BYOD security issues covering the user attitudes, behaviour and expected actions. Their work provides risk management and analysis of user behaviour. Other authors have also studied BYOD security issues and have agreed that user attitudes are affecting the understanding of risks, risk management, user access needs and the design of the BYOD risk-management process (Herenandez & Choi 2014). Singh et al. (2017) categorised the security breaches of the BYOD user into different types of risk which included: lack of user awareness, loss of devices, installing malicious applications, connecting through public Wi-Fi, random internet browsing, smartphones without security apps, frequent changes of devices, data leakage and data loss.

### 3.3.4 Machine Learning in Information Security

Machine-learning approaches have been widely used for detecting security breaches in different applications. As stated by Barreno, et al. (2010) the goal of machine learning in application security is to allow legitimate live-data transactions and reject any unwanted behaviours. This can be achieved by the classification of the various activities.

This research focuses on the classification of actions using machine learning. Breier and Branisova (2017) proposed a Dynamic Rule Creation Based Anomaly Detection Method for Identifying security breaches in log records. Their research focused on network activity analysis by utilising log records from a number of currently available monitoring systems such as IDS, IPS, firewalls and proxies. However, they relied on two approaches, including both IDS, and the collection of log records, for analysis. The paper presents classifications based on the properties of the data, and the clustering of data without knowing its features, as two methods for data mining.

Similarly, G Sathya and K Vasanthraj (2013) proposed multilevel classifications for security-attack detection in cloud computing. This research addressed three main challenges which were: access to the resources in the cloud, the efficiency of the current IDS to detect different attacks, and log management for big data held in the cloud. The proposed approach used a multilevel IDS and ran classification algorithms which not only recognised the attacks on the cloud environment but also classified them according to the type of attack. The classification used the C4.5 supervised machine-learning algorithm to deal with attributes that contained a large amount of detail.

However, this research provided interesting insights into current security-countermeasures which were relevant to the BYOD environment. Other researchers have also focused on enhancing the IDS network-security performance for dealing with attacks (R.Jakhale 2017; G Sathya 2013). R.Jakhale (2017) suggested a framework based on network IDS, using host IDS-generated logs as the dataset. The proposed approach used the JACOP java-application for data mining to detect events in real time. Samrin and Vasumathi provided a survey paper on the performance of network-event detection systems for host-based intrusion detection (Samrin and Vasumathi, 2017)

However existing papers only cover network-related security issues but have largely ignored the security issues related to BYOD (R.Jakhale, 2017), (G Sathya, 2013), (Sultana & Jabbar, 2016)and (Samrin & Vasumathi, 2017). Accordingly, it becomes imperative to design approaches which are

able to correctly classify normal and abnormal events in a BYOD environment. This provides the motivation for this thesis, which is to develop an approach to deal specifically with security issues in the BYOD environment. Shiomi et al (2015) proposed a classification algorithm for smartphone data to generate traffic categories. This research used an SVM linear approach to detect the real-time data of the smartphone to build the model. This had a limited scope when compared to the approach proposed in this thesis, which uses an MDM log and a service-function log for detection.

Many researchers have proposed detections methods for smartphone security. Schmidt et al. have proposed an evaluation study for detecting smartphone traffic and application use, as well as classifying malicious and normal traffic (Schmidt, et al., 2009). Andrey Finkelstein et al. (2017) also proposed an approach which classified the internet traffic of smartphone users. The purpose of their study was to sort the users based on their technical skills and demography to evaluate the security risks generated by their usability style. The authors focussed more on the classification methods and tools, and any discussion about the risks emerging from the smartphone traffic, or how the proposed approach dealt with them was missing, which made it difficult to assess how their framework was built.

Some other research efforts propose their own classification algorithms for dealing with smartphone security. Muller et al. proposed a prototype called MDoNA (Müller, et al., 2017). The proposed system ran a classification-based algorithm to perform both a static and dynamic risk-calculation. However, the proposed classification algorithm was not efficiently tested or evaluated and lacked the evidence of proven accuracy.

The proposed research in this thesis will attempt to apply risk classifications in the development of a BYOD risk management system. It is necessary to apply appropriate machine-learning algorithms to classify the events as normal or abnormal. In this research, the main objective will be to detect and analyse events and classify the event as either normal or abnormal. SVM has been chosen as the classification method. This algorithm can classify up to 100 features of the dataset and provides a high level of accuracy whether the training time is of short or long duration.

Sunchacka et al. (2015) proposed an approach for the classification of e-commerce sessions using SVM, the focus being to evaluate the customer reaction within a web session. They demonstrated the utilisation of SVM in classifying high-dimensional datasets. The research used real data traffic obtained from web-server logs. The authors evaluated the proposed approach by comparing it with

four different SVM models. Although this research effort used server logs for classification, it is focused on separate session-related information. Similarly, Casas et al (2017) utilised smartphone traffic to enhance the quality of the customer experience. Their research compared four types of machine-learning classifications which were SVM, Bayes Native, neural network and random forest to generate predictions in smartphone-traffic access and behaviour (Casas, et al., 2017).

The classification approach proposed by Moin A and Khansarii M et al (2010). Detected software bugs based on path and history and employed SVM for classification. The study also highlights the challenges faced when reading numerical and string data. However, the proposed approach in this theses uses the MDM log and functions log for classification, which has the advantage of predicting the more BYOD risks than other BYOD frameworks

Demontis at al. (2017) present a classification approach to enhance security performance. The authors suggested a novel approach to improve linear classification, applied separately for both security and regularisation concerns. The paper compares different sets of SVM and elaborates on a situation where an attack can be made on the classification process, which affects the security alarms or predictions. This means that the attacker can change features of the classification mechanism which makes the security-detection system itself vulnerable.

After classification, the next step is the decision making. D. Rana stated that using one class of SVM will generate the output target for only one parameter, which is fewer than using traditional classifications. Nevertheless, two class or more classification is normally performed as linear classification will handle more parameters. (Rana, 2015).

Recent years have seen a surge in the application of SVM in security applications and has been shown to be effective for spam and malware detection, vulnerability and attack categorisation (Dalvi, et al., 2004) (Lowd & Meek, 2005) (Kolcz & Teo, 2009). Exceptionally, linear SVM classifications have been more widely used in mobile networking and embedded systems (Demontis, et al., 2017). However, the SVM can work as a standalone classifier, or can be part of the solution which combines SVM, decision tree and naïve Bayes, enhancing data classification by reducing the false positives (Goeschel, 2016). The term ‘false positive’ considers the high-risk percentage in security terms. The method proposed by Goeschel aimed to filter the datasets in three phases where each phase ran a different machine-learning algorithm.

However, compared with the approaches of other researchers, machine-learning is costly and takes longer for decision making, although it increases the level of security and accuracy (Rana, 2015) (Breier & Branišová, 2017) (Suchacka & Potempa, 2015).

### 3.3.5 Risk Management Frameworks

Risk management frameworks help to secure the assets of an organisation based on the unique requirements of the business. Therefore, the board or senior management should be taking extra care when dealing with risk-management processes, maintaining business activity by proper information-security governance. In this section the most popular risk-management approaches, which are COSO, COBiT and ISO 37001 and their use in BYOD environments will be discussed and analysed.

Committee of Sponsoring Organisations **(COSO)**

The COSO framework has been defined by ISACA. It is a framework which includes all components of control (COSO.org, 2014). In the annual report of COSOs executive board (2013) it was noted that the adoption of the framework into the organisational environment achieves information-security objectives relating to operations, reporting and compliance. The COSO framework has five main components (often referred to by the acronym C.R.I.M.E), which are: control environment, risk assessment, information and communications, monitoring activity and existing control activities (Magruder, et al. 2015; Landsittel, 2013). COSO covers all business factors such as financial management, regulation and IT and is suitable for small and medium-sized companies.

COSO covers only general IT control, which results in a gap in the technical-risk management and is only used for internal purposes. However, effective intelligent risk-management should cover control methods for both internal and external environments. For IT control, the COSO framework proposes standard security-countermeasures such as firewalls and anti-viruses, but such a framework should also be enhanced to include the latest countermeasures for smartphone security, such as Software Defined Network (SDN), secure middleware, and standalone devices.

William Brown and Frank Nasuti (2005) estimated that the COSO framework only covers 13% of the control methods required for an IT system.

Ramandip Kaur (2014) stated that COSO could be used in a BYOD environment to evaluate the internal risk because mobile devices are affecting the environment, changing workflow, exchanging sensitive information, breaking current policies and changing employee roles. Rui Wang (2013) also noted that COSO can be used for evaluating the information-security issues for mobile devices and that the monitoring of risks generated from these devices should be audited by reference to the mobile computing auditing/assurance security program initiated by ISACA (Wang, 2013).

Although the COSO framework is used for internal control and monitoring many researchers agree that it is not good enough to control the current mobile-device threats and attacks. Therefore, to be more effective, the framework should be combined with other frameworks such as COBiT or ISO 37001 (Jans, et al., 2009).

**COBiT**

The CoBiT framework was designed to link the non-technical and technical control methods (Campbell, 2005). It has different versions to evaluate the tools and components used by the organisation (Tuttle & Vandervelde 2007). The framework consists of five versions, the latest one being released in 2013 by ISACA. CoBiT version 5 is divided into 34 processes which are attached to different concepts of IT governance. The framework is compatible with other frameworks such as COSO, ITIL and ISO 37001. COBiT 5 has five principles which are meeting of stakeholders needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach and separating governance from management.

The main principle is the meeting of stakeholders needs and with the emergence of BYOD risks and challenges, COBiT 5 includes BYOD information-security strategies (Pozza 2014). Additionally, a process for ensuring resource compatibility makes COBiT suitable for BYOD content. There are concerns at board level about employee-owned devices holding business information, therefore, adopting the latest information-security frameworks such as COBiT 5 and

including procedures for both auditing and user awareness, will simplify security (Sitnikova & Asgarkhani 2014).

Recent studies have argued that COBiT has more advantages than other frameworks by taking account of both business and IT processes. Especially, researchers have noted that COBiT provides some support in IT decision making (Davos & Ginste 2014) but has difficulty in fully supporting the technical and practical aspects which influence decision making (Simonsson and Johnson n.d. 2006). Additionally, Alessandro Aldini and Jonathan Guislain (2017) proposed an approach focussing on improving policy compliance in the BYOD environment which influenced decision making speed and performance. In the current BYOD environments, it is strongly argued that real-time decision making is needed (Aldini and Guislain 2017). Ward et al. (2017) also agreed with this, stating that BYOD needs faster decision making to prevent or reduce the impact of risks.

**ISO 37001**

ISO 37001 is an international standard which has been developed to support all types of organisations. Previously it was named as BS 7799, but after 2005, it was adopted by ISO and became the ISO 37001 standard (Susanto et al. 2011). It combined safeguarding with proper cost control in security investment (BOEHMER 2009). ISO 37001 has ten main areas of security (Hall 2013). The ISO 37001 standard together with COBiT frameworks are considered to be the two best options for information-security management strategies (Solms 2005).

Researchers have used ISO 37001 for the BYOD environment, which helps to take into account most of the required security factors (Samaras et al. 2014). However, the main weakness of the standard, which can also be observed in other frameworks, is that it does not cater sufficiently for the security of mobile devices. Therefore, ISO 37003 has been developed in an attempt to provide technical support to fill these gaps (Arthur 2013). The rapid rise of BYOD threats and risks over the network, or even over the cloud, is the reason for researchers to recommend upgrading to ISO 37003 to provide a more comprehensive information-security infrastructure for mobile devices (Williams 2013).

However, the gap still remains in terms of implementation, and so technical guidelines need to be added (Pell 2013). Additionally, ISO 37001 and ISO 37003 have the most suitable technical

standards and are recommended by most researchers. However, the real-life scenarios can fail to meet expectations, especially with the increase in the smartphone applications, imposing technical threats, requiring technology defences which are beyond the scope of the standards (Arthur, 2013; Sitnikova & Asgarkhani 2014; BOEHMER, 2009).

**Information Technology Infrastructure Library (ITIL)**

As has been noted above with other frameworks, information-technology management is facing enormous challenges, especially in terms of implementation. Therefore, ITIL has been developed to support IT practices (Radovanović et al. 2010). Currently, ITIL has three versions which cover almost all the phases for controlling, designing, implementing and optimising services. ITIL has been a focus of security professionals due to the rapid increase in mobile devices and the associated BYOD security threats.

ITIL is mainly IT-process based and is greatly needed for implementing information-security frameworks (Brand et al. 2015; Jennex 2014). However, it is used for IT strategy and security planning, but cannot be used as a stand-alone security framework for any organisation (Armstrong 2009). Although security management is part of the ITIL steps and phases, it is not completely satisfactory, so many researchers have used combinations of frameworks to achieve a high level of security with better IT practices and support (Huang et al. 2009).

Therefore, ITIL has its own limitations when applied to HR, operations and communication security as is shown in figure 3.5 below.

**Security Frameworks Findings**

The discussion of the information-security frameworks and standards clearly indicates the importance of applying security measure in the BYOD environment. This issue has attracted the most prominent security leaders such as ISACA and individual researchers. Therefore, ISACA has enhanced frameworks or developed new versions to include smartphone risk-management. Additionally, it has added standards or processes into other approaches such as ITIL and ITAF (Kaur 2014). Different researchers have acknowledged the limitations in the implementations for

these frameworks, which need the support of third-party enhancements to provide solutions to the security problems of BYOD (Hall 2013; Salle & Rosenthal 2005; Huang et al. 2009).



Figure 3.4: Features of each Standard (Susanto et al. 2011)

Retnowardhani et.al (2019) used ISO 27002:2013 in their research to enhance BYOD security, where they recommended the use of different BYOD protection functions such as access control, network management and information management. They highlighted the ISO 27002:2013 detection functions as being suitable for the BYOD environment which included continued monitoring, anomaly detection and the detection processes. This provides the necessary support to the standard for the process of risk management and subsequent actions which will aid in decision making, although the research generally discussed the countermeasures without noting the BYOD risks and threats.

Therefore, to fill these gaps in the current knowledge the proposed research in this thesis will focus on enhancing the IT implementations to detect/predict the security threats that can occur in the BYOD environment. It was noticed from the literature that researchers were working to enhance the detection mechanisms, whereas this thesis study is focussed on both risk detection and

prediction. The following section highlights the role of machine learning for security-risk detection and prediction.

## 3.4 Machine Learning

In order to detect and predict the risks, the risk-management system should receive a set of instructions to recognise the data and apply an algorithm to classify the activities of the BYOD-user into either normal or abnormal. The literature for information security using machine learning is discussed in the following section

### 3.4.1 Artificial Immune System

Artificial immune system (AIS) is a paradigm which take inspiration from human immune systems. Moreover, it provides a technical bridge between the immunology and computer science. AIS has been used in application domains such as learning, recognitions, and anomaly detection. There are three main algorithms used in AIS, which are negative selection algorithm, artificial immune networks and clonal selection algorithm (CSA).

Artificial immune systems have also been applied in security environment to detect malicious applications in androids operating systems. Diogo A.B. Fernandes et al (2017) highlighted the use of AIS in computer security in two major areas which are malicious process detection and fraud detection. They have described malicious process detection including anomaly detection, intrusion detection and scan and flood detection. The nature of the problem being addressed in this research is not fit for AIS application as this researches focuses on log file and SVM approach suits well to this research problem.

Artificial immune systems have also appeared to improve the analytical process in different domains such as mathematics, information, and science.

## 3.5 Summary

There are many technologies and solutions that have been proposed to deal with BYOD security attacks. However, the major challenge found is the capability of risk-management systems to deal with BYOD risks. MDM is one of the widely used risk-management systems for a BYOD environment, but has not been shown to be effective enough to secure the environment and provide safeguarding for companies. As these MDM systems deal with various kind of threats and they use log files to record activities they have limitations when dealing with application-level threats, therefore, a gap was identified in risk prevention at the application level of MDM.

Also, it can be observed from the literature that there are two strands of research regarding MDM systems. The first strand deal only with a small set of attacks which limits the application of the solutions to other environments, which are subject to different types of attack. The second strand proposes only theoretical frameworks and processes which does not guarantee the data security in case of lost or compromised devices. Consequently, both of these gaps need to be investigated

Table 3.1 shows the functionality of current countermeasures compared with the proposed framework.

Table 3.1: Highlighting the gaps in current countermeasure

| **Functions** | **IDS** | **Firewall** | **IPS** | **MDM** | **SIEM** | **Current Risk management** | **Our Proposed system** |
|---|---|---|---|---|---|---|---|
| **Data security** | Monitoring and detecting risk | Filtering based on allow and block | Detecting/ preventing risks | Apply policy to data access | Analysing the events log | Recording the action for furthers plan | Follow the user activity and predict the risks |
| **BYOD environment** | Not functioning | Isolate the traffic | Isolate the traffic | Restrict control/ tracking of | Lacks the detection of malicious | Reports process and basic | Detect the data/ user's |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | devices and apply policy | traffic in BYOD and does not protect the data itself | network limitations | activity and protect the content. |
| **Monitoring the smartphones** | No | No | No | Yes | Log analysis | No | Log analysis and access control |
| **User awareness** | No | No | No | No | No | No | Yes, by pushing notifications of predicted risks |
| **BYOD and Data confidentiality** | Not controlled | Not controlled | Not controlled | Yes, can wipe business data if risks happen | Not control | Not controlled | Can raise the notifications before the data even infected or risk accrue |
| **Action taken** | Based on configuration rules | Based on configuration rules | Based on configuration rules | Based on user activity, Manual action done my administrator | No action | Based on recorded history and documents | Based in user activities from different services. |

# Chapter 4: Research Methodology

## 4.1 Introduction

The Research Methodology is a phase where the researcher highlights the steps, processes and data required to ensure the research is successfully completed. Therefore, the following sections of the methodology chapter discuss the selection of data collection methods, tools and processes needed to answer the research questions and achieve the research objectives. All this with the ultimate aim of proposing a risk management and security framework to minimise the risks in the BYOD environment. To demonstrate the capabilities of the proposed framework a prototype which developed for Oman organisations in Oman.

The choices made for the methods, techniques, tools and strategies used for data collection and analysis, the justification of the choices made in relation to the research questions, and the ethical considerations in respect of the primary-research participants are presented. Section 4.2 details the research approach and methodology. Section 4.3 presents the research-methodology flowchart. Section 4.3 highlights the research stakeholders. Section 4.4 defines the tools that are used to implement the proposed framework, Section 4.5 maps the research questions to the selected methodology. Section 4.6 gives the ethics considerations for the research and Section 4.7 summarises the chapter.

## 4.2 Research Approach/Methodology Overview

The methodology used in this thesis is built on the aim, research questions and objectives, which has been discussed in section 1.4 and 1.5 of chapter 1. This research has adopted a methodology which is a combination of both qualitative and quantitative research, which is also known as a mixed-methods approach (Hussein 2015). The qualitative-research analyses the common-sense behaviours, motives and gaps in the current work on BYOD risk-management frameworks, while the quantitative research is used for identifying the risks and the impact of risks in the BYOD environment and the user attitudes towards risks (R.Kothar 2004). The mixed-methods approach

provides a deep insight into the data, which comes in both textual and numerical formats. The quantitative and qualitative methods are presented in the following subsections.

### 4.2.1 Qualitative

Qualitative analysis is the detailed analysis regarding the research judgments and gaps presented in text-based analysis (Creswell 2017). This research is broadly concerned with the risk-management field and users are the main actors, therefore it is imperative to take human knowledge and activities into account. The survey in this research contains open questions which allow the professionals to add their own experience in the controlling of BYOD and the associated risks.

However, analysing these subjective inputs is not easy, especially when dealing with textual inputs, such is the case with the weaknesses, security challenges and control methods for the BYOD environment. Part of this study will involve identifying the theoretical concepts underlying the different BYOD risks, and so, qualitative research will provide the means to achieve the required outcomes which are the identification and analysis of the risks and the likelihood of their occurrence.

### 4.2.2 Quantitative

Measuring the findings and performing proper numerical evaluation will require the support of deep analysis to design the proposed framework (Cramer 2004). The quantitative analysis will involve using statistics to analyse the risks within the current BYOD environments and use the knowledge gained from the analysis to enable the building of a risk-management framework.

Quantitative results are considered appropriate for this research for enabling both the taking of informed actions, and effective decision-making. Surveys and systematic data-collection will be used to obtain the quantitative data.

A qualitative research method is used for extracting the log file data from the MDM system and function logs and then these are compared with the quantitative outputs from the surveys to generate the current knowledge regarding BYOD risks. Finally, all the findings are used to identify the challenges of currently used frameworks and the system administrator behaviour in a BYOD

environment. Further details regarding the current security-frameworks are provided in the literature review section 3.2.4.

However, the compelling challenge in the information-security field is to validate the information collected. This challenge mainly concerns the ability to verify the characteristics of the risk. Therefore, it compares the literature review findings with both the results of the surveys and the MDM data, to identify the features of the risks and the likelihood of their occurrence. The following section presents the flowchart for the methodology used in this research and discusses the content.

## 4.3 Research Flowchart

Figure 4.1 shows the flowchart which has been adopted to answer the research questions and achieve the research objectives, illustrating the research stages.

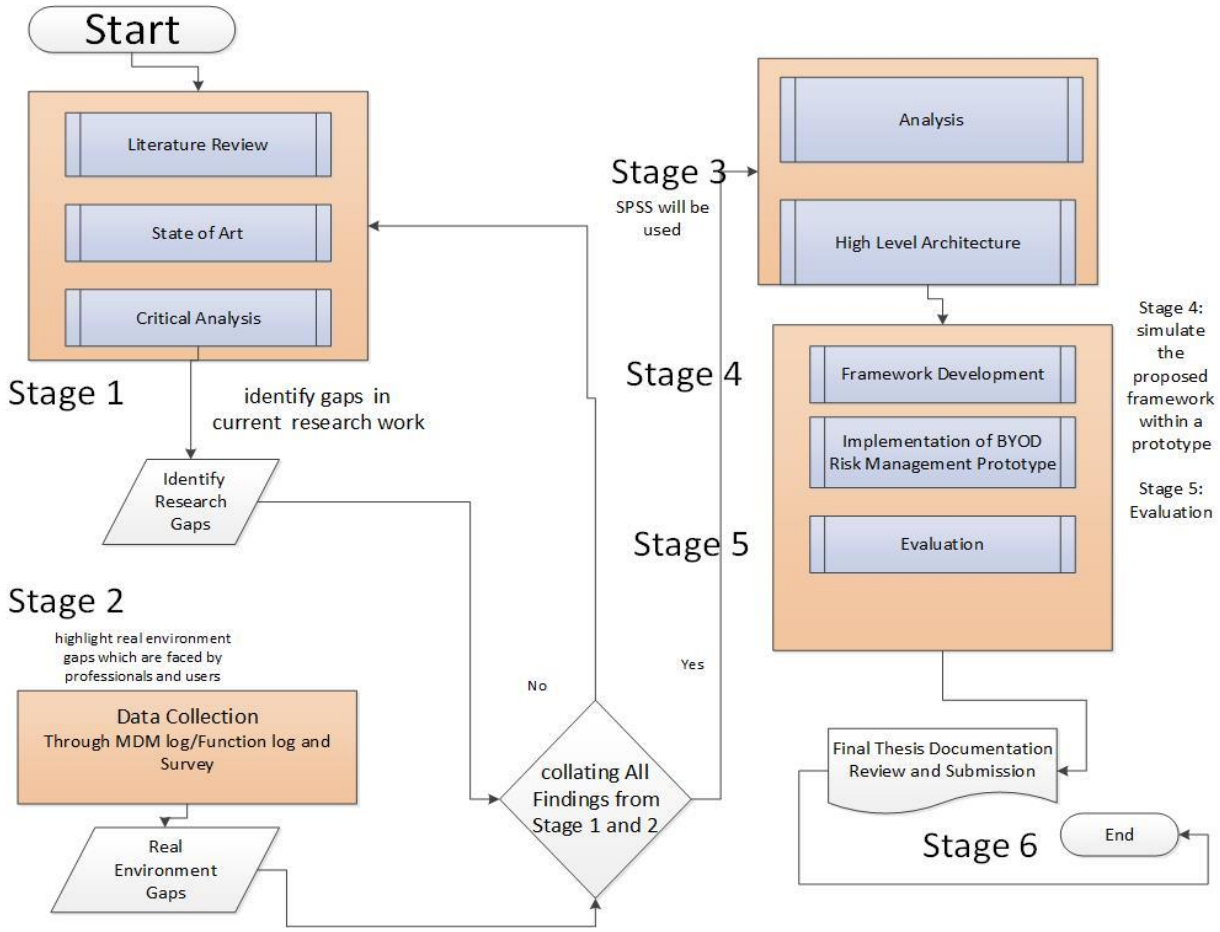



Figure 4.1: Research Flowchart

This research relies based on both primary and secondary sources of information. The reasoning behind this is to perform an in-depth study of risk in the BYOD environment. This will be achieved by, firstly, gathering the existing knowledge of risks from the literature (i.e., secondary research). Then secondly, validating the existing knowledge and adding new knowledge from the survey (i.e., primary research).

This will also help in the design of effective detection and prediction strategies for the proposed risk-management framework.

### 4.3.1 Stage 1

The literature review is the first and foundational step to initiate the research and investigate the specific research topic. This will collect information from the work of other researchers to answer the research questions which will identify the gaps in the current knowledge. Therefore, the output from stage 1 will be the current knowledge of risk-management in the BYOD environment.

### 4.3.2 Stage 2

Following the literature review, and the identification of the gaps in the existing literature in relation to the research questions, the primary data collection will be performed. This primary data will include the surveys, MDM event logs and function logs.

Dana Lynn and Driscoll (2011) describe data collection as the creation of a new set of data which clarifies the issues which are highlighted in the secondary data methods. The data will be collected to identify the research gaps and support assumptions with facts. In this research two types of primary-data collection methods will be used. The first method is to conduct automated observation and data collection through an MDM server and function server. Additionally, two survey forms will be distributed, one at the organisational level which evaluates the usable frameworks and risk management approaches, and the second to evaluate the awareness level of the users. Table 4.1 shows the mapping of the data-collection methods and the research objectives.

Table 4.1: Mapping the objectives of the data collection methods.

| Objective | Data Collection methods |
|---|---|
| • **To conduct a field study to analyse the user awareness of the consequences of potential security breaches within the BYOD environment.** | Survey |
| • **To investigate the problem domain and review the existing and emerging technologies related to BYOD security.** | Literature review |
| • **To evaluate the proposed risk management system in the BYOD environment using real world business scenarios.** | Interview the system admin |
| • **To develop a framework that encompasses intelligent risk-management and security governance** | Literature review / MDM system/function logs |

Primary data can be collected through three main methods, which are, observation, interview and survey. This research will not use observation but will focus on survey and systematic data generation from the MDM server and function servers, including database and application servers.

Two surveys were designed and distributed to participants to achieve the first two objectives for this research, which were:

1. To conduct a field study in Oman to analyse the user awareness of the potential security breaches and their consequences within a BYOD environment.
2. To propose a framework that encompasses risk management and security governance

The first survey focuses on the organisational level for evaluating the effectiveness of the frameworks and risk-management approaches which are currently applied in the BYOD environment. This survey will identify the challenges with the current control-methods and frameworks, which are used to achieve security in the BYOD environment. The survey will include both open-ended and closed questions. The closed questions are designed to get direct answers without any possibility of confusion. The open-ended questions are needed to give flexibility in the answers and allow the professionals to add their knowledge and experience to identify the security threats and risks.

The second survey was designed to evaluate the awareness level of users regarding the potential risks in the BYOD environment, especially in terms of security practices and activities. This survey was designed for the end users who have less knowledge of security concepts. Therefore, the questions were written in a simple language with less technical jargon. All questions in the survey forms were closed questions to provide precise answers.

The primary research does not just depend on the survey results but also utilises data from the MDM-system history and log files. From this data, smartphone access in the network traffic can be detected, which will identify the number of mobile nodes accessing the network. Additionally, details about the control levels applied and how effectively security risks are managed, for the different versions of the smartphone operating-systems will be obtained.

However, any gaps found through analysis of the literature in stage 1 should with the gaps from the data collection in stage 2 to check if same issues were highlighted at the investigation stage. Only processing those issues which are found from both stage 1 and stage 2 will help to narrow down the scope of the problems which need to be covered in the proposed risk-management system.

If the issues at stage 2 do not match those at stage 1 the literature should be reviewed again at stage 1. This process has to be followed because the data collection through participants cannot be changed. Hence, as discussed above, the MDM system will also be used to ensure the accuracy of the data collected.

### 4.3.3 Stage 3

This stage contains two sub-stages which are analysis and modelling. The analysis phase will analyse the combined data sets from the previous stages and identify the risks in the BYOD environment and the challenges with the existing frameworks. The analysis will use the Statistical Package for the Social Sciences (SPSS) which will be described later in this chapter.

The second sub-stage is classification which models both the traffic (i.e., into categories of normal and abnormal BYOD traffic) as well as the features of the potential threats to security. The analysis of the logs from the MDM system will help to predict the risks so that remedial actions can be taken.

### 4.3.4 Stage 4

This stage will process the findings from the data collection and analysis stages to generate the strategy-architecture requirements and the implementation tools required. This stage contains three sub-stages, which are: the architecture-requirements definition, the implementation of the proposed intelligent risk-management framework, and the evaluation of the framework.

The first sub-stage will produce the definition for the intelligent risk-management framework and the prototype system.

The second sub-stage will be the implementation of the prototype which will process the inputs from the previous stages (i.e., the classified risks and the features) and record any actions. By processing this information, advance warning can be given about any threats or attacks to the security of the network.

### 4.3.5 Stage 5

The proposed framework will be tested and modified accordingly in the event of any extra functionality being required.

### 4.3.6 Stage 6

This final stage of the research consists of the production and review of the documentation produced from all of the stages.

## 4.4 Research Stakeholders

This research focuses on securing the business data of smartphones in the BYOD environment. Therefore, the users, and the enterprise employing the BYOD environment, are the main stakeholders in this research. This research mainly affects the business environment, so senior management and IT professionals are both used as research participants. Stage 2 of the primary-data collection uses these participants to identify the research problems in the BYOD environment and to identify the risks and threats to security.

## 4.5 Tools

The following sections provide descriptions of the tools adopted to achieve the objectives of this research. The tools are MDM, PSPP, Weka and NetBeans. These tools will be used in different stages of the research and be used to extract and analyse data coming from different sources. This research will also utilise machine learning, SVM, and hybrid networks which are discussed further in chapter 2.

## 4.6 Mapping Research Questions to Research Methodology

It is necessary to choose an appropriate methodology and research plan to meet the objectives of the study and to map each method to the research questions being addressed. Therefore, this part of the chapter will elaborate the relationship between research question 2 and the planned research methodology. The research question is:

How can the MDM event log analysis and enterprise-security risk management improve the detection and prediction of imminent risks and mitigation of malicious actions in the BYOD environment?

The research question contains of three elements: the MDM event log and function log; risk management; and the improvement of detection, and prediction measures. Therefore, while building the research methodology flow chart, the following factors need to be considered:

- MDM functions event log and function logs: these will be used to determine the network traffic, with an analysis of device access details and smartphones activities. This will generate the detail of the risk assessment and analysis, together with the data extracted from the function-services server event-log.
- Risk management: this is achieved by the updating the risks from the literature review with the results from the two surveys, to identify those risks which occur in the BYOD environment for organisations in Oman.
- Improvement in detection and prediction: this is the most important part of this research. After gathering and analysing all the data, the proposed intelligent framework will be created which will enhance the risk detection and risk management techniques.

## 4.7 Ethics Considerations:

This research ensures that the ethical issues concerning the business and participants are considered. Data presented in the theses will not contain any information that would: identify the businesses who participated in the study, either directly (i.e., by name) or indirectly (IP address, domain names); or negatively affect the competitive position of the companies. Any participant data collected will be anonymised before being presented to ensure that the requirements of both data privacy and data-confidentiality are maintained. All collected data will be kept confidential and properly stored until the end of the research and then will be destroyed.

## 4.8 Summary

A detailed explanation of research methods chosen for this study has been given in this chapter. The flowchart of the methodology and associated steps, together with the data collection methods are presented. A mixed method approach has been chosen and explained together with justification for the choices made. The development of the proposed intelligent risk-management framework which will be discussed in the following chapter.

# Chapter 5: Survey's Findings and Analysis

## 5.1 Introduction

This chapter achieves one of the thesis objectives, which is: to conduct a field study to analyse the user awareness of the potential security breaches and their consequences within a BYOD environment. This chapter also aims to demonstrate the gaps identified through the findings of the surveys. The expected outcomes of the surveys will be to attempt to answer a set of questions covering for example: What are the current challenges in BYOD frameworks and associated countermeasures? What is the current level of user awareness regarding BYOD security issues in Oman? Do Omani organisations use the event log in their risk management process?

This chapter is organised as follows. Section 5.2 targets participants and environment for the survey. Section 5.3 presents survey-one findings. Section 5.4 presents' survey-two findings. Section 5.5 presents the recommendations and a summary of the chapter.

## 5.2 Participants and Environment:

To achieve the thesis objectives, two surveys mentioned in the methodology chapter (section 4.5), have been conducted in five participating organisations in Oman. The purpose of these surveys was to investigate BYOD security concerns and provide a comprehensive picture from both a user and organisational perspective.

The targeted organisations have been chosen from different sectors in Oman where the government is taking the initiative to begin to build smart cities and they have already announced the development of a few cities using many supported technologies and mobile applications. BYOD is an important component of smart cities, so it is important to address the risks of BYOD technology in order to ensure the safety and security of smart cities. The sectors which had been chosen in Oman were education, governmental, private, banking and oil and gas. The selected organisations had been chosen, in order to have an in-depth understanding of the challenges posed

by the BYOD environment in different sectors. Also, it was important to know what needs to happen for these organisations to address the BYOD security challenges.

This study was conducted to understand the level of adoption of BYOD and the associated security issues and provide the necessary guidelines for organisations considering implementing this new technology.

The organisations have agreed to participate in the surveys because they allow smartphone users to access the organisational resources as a part of their work. The educational institute has agreed to participate, as they allow state of the art teaching methods using smart devices, for the smart education environment. The government-sector organisations are a bit more restrictive in giving BYOD a specific role in their business. The banking sector relies on M-banking applications and mobile transactions, and some of their employees access resources thorough mobile phones. The oil and gas sector allows the use of smart devices in field work and for tracking the status of different machines using applications. However, these organisations have shown their interest in the BYOD technology and their concerns about risk management by being willing to participate in these surveys. The results from question 1 of the survey (see tables 5.1 and table 5.2), shows the percentage of survey respondents from each of the industry sectors.

Tables 5.1: Organisation participation in professional level (survey 1).

| Question 1 (in survey 1) | Responses | Respondents | Percentage |
|---|---|---|---|
| What is the industry sector for your organisation? | o Oil and gas | 4 | 20% |
| | o Educational | 5 | 25% |
| | o Government | 9 | 45% |
| | o Banking | 2 | 10% |

Table 5.2: Participation in user awareness (survey 2)

| Question 1 (in survey 2) | Responses | Respondents | Percentage |
|---|---|---|---|
| What is the industry sector for your organisation? | o Oil and gas | 60 | 26.66% |
| | o Educational | 50 | 22.22% |
| | o Government | 58 | 25.77% |
| | o Banking | 17 | 7.87% |
| | o Private | 40 | 17.48% |

## 5.3 Survey One Results: Professionals and Organisational Level:

In order to find the BYOD challenges and risks, the survey was designed to highlight the current frameworks adopted and the countermeasures that were applied within the organisations. The intention was to gain an insight into how different organisations deal with BYOD security challenges and also if there are disparities in the application of countermeasures and the kinds of framework being adopted in these organisations.

The survey was randomly distributed to 20 experts, with a mixture of security and IT skills, within the five different organisations. Among the participants were network administrators, a security manager, a CEO, security/IT consultants and IT Technicians as shown in Table 5.3. This variety of different roles help in adding a value to findings the challenges from different security and technical perspective.

Table 5.3: Professional work affiliation.

| Question 2 | Responses | Respondents | Percentage |
|---|---|---|---|
| What is your Job Role? | o IT technician | 6 | 30% |
| | o Network administrator | 4 | 20% |
| | o Security manager | 1 | 5% |
| | o CEO | 1 | 5% |
| | o Security/IT consultant | 8 | 40% |

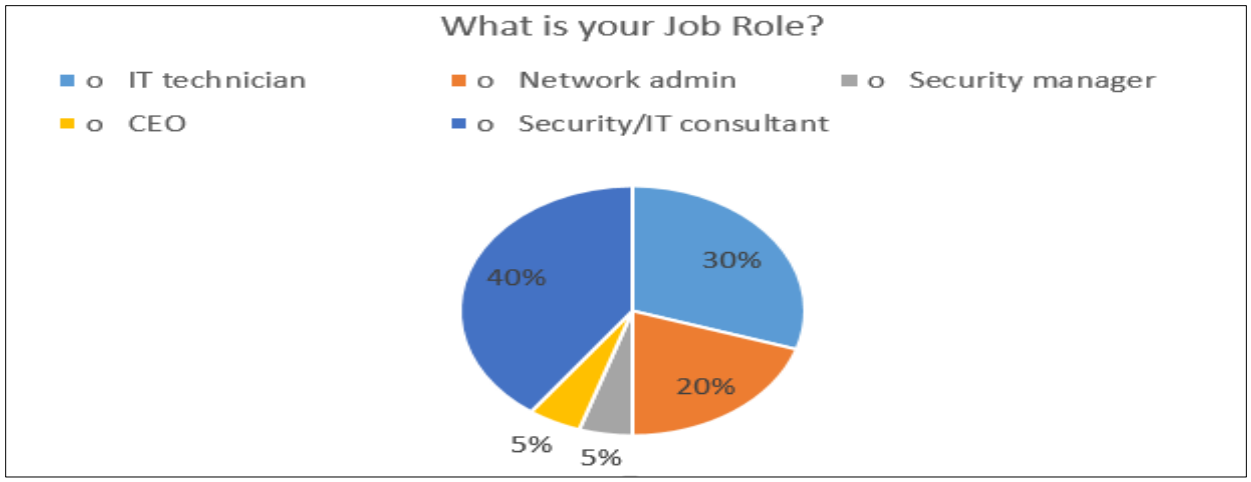



Figure 5.1: Professional work affiliation

The results from question 2 (see Table 5.3 and Figure 5.1), shows that nearly 67% of the participants had more than two-years of experience in risk management, and the remaining 33% had more than five years of experience.

Question 3 (see Table 5.4 and Figure 5.2) results show that 70% of the participants among the five organisations, stated the reason for adopting BYOD in their business was to increase productivity. This reflects the necessity of considering BYOD as part of business continuity plan.

Table 5.4: BYOD adoption in business network.

| Question 3 | Responses | Respondents | Percentage |
|---|---|---|---|
| Do you allow BYOD adoption in your business network | ○ Yes<br>○ No | 14<br>6 | 70%<br>30% |

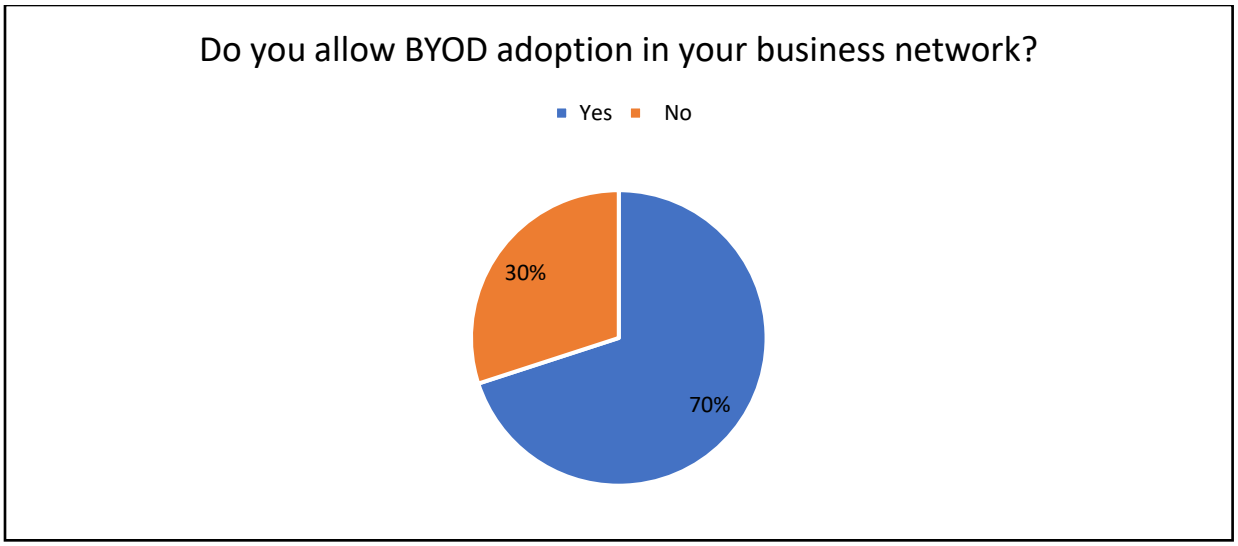



Figure 5.2: BYOD adoption in business network.

It is clear from the responses of the participants that there are some concerns regarding BYOD, because only 70% of the participants would allow personal devices to have access to the intranet resources.

Question 4 (see Table 5.5), results show that only 10% of the professionals would allow Wi-Fi access and about 40% of the participants would allow BYOD users to access business resources. The majority of the participants (50%) would not allow any access to resources using personal devices. This indicates the security concern regarding the access control of the BYOD devices.

Table 5.5: Allowing BYOD devices to access intranet.

| Question 4 | Responses | Respondents | Percentage |
|---|---|---|---|
| Do you allow BYOD users to access your intranet resources? | o Yes | 8 | 40% |
| | o No | 10 | 50% |
| | o Partial access (Wi-Fi access) | 2 | 10% |

Question 5 results (see Table 5.6), show that some network and security administrators believed that there was no security risk in providing Wi-Fi access to BYOD users, which is not true in reality. Definitely, allowing internet access can result in DoS attacks, SYN flood DDoS attack, or

even ICMP ping attack (Park and Lee, 2001; Arash et al., 2018). On the other hand, the participants referred to the fact that they were facing a high level of risk and security challenges by allowing smartphones to access their intranet services. 40% percent of the participants agreed that the most comprehensive attack which targeted their organisations over the BYOD environment was the denial-of-service attack and 40% identified unauthorised access as significant. Other security attacks can also occur, such as phishing attacks and fake application attacks which were noted by 10% of the participants. The presented percentage of attack accuracy indicates the increase of security risks and challenges associated with adopting BYOD.

Table 5.6 Well known risk and attacks:

| Questions 5 | Responses | Respondents | Percentage |
|---|---|---|---|
| What are the most well-known risk and attacks that has been faced or noticed by allowing BYOD? | ○ Unauthorised access. | 8 | 40% |
| | ○ DoS attack | 8 | 40% |
| | ○ Phishing attack | 2 | 10% |
| | ○ fake application | 2 | 10% |

By knowing the most common attacks that can occur in the BYOD environment, it is necessary to understand the suitable control methods and risk countermeasures to address these BYOD attacks. The result of the survey showed that all the participants agreed that they needed multiple control methods to address the threats in their BYOD environment. For example, they chose: security management, security operations, MDM system, risk management and timely response, as these methods can minimise the likelihood of the risks or mitigate the impact of the attack, then the participants selected a list of countermeasures which are being used in their organisations to protect the resources.

Question 6 (see Figure 5.3) shows six countermeasures and control methods selected by the 20 participants, which are being used to secure business information. Each participant was asked to specify the countermeasures applicable to their organisation and in some cases more than one countermeasure was being applied. The countermeasures were: MDM system, network segregations, policy, encryption, VPN access applications restrictions. Figure 5.3 shows the distribution of adoption for the different control methods in the Omani organisations surveyed.

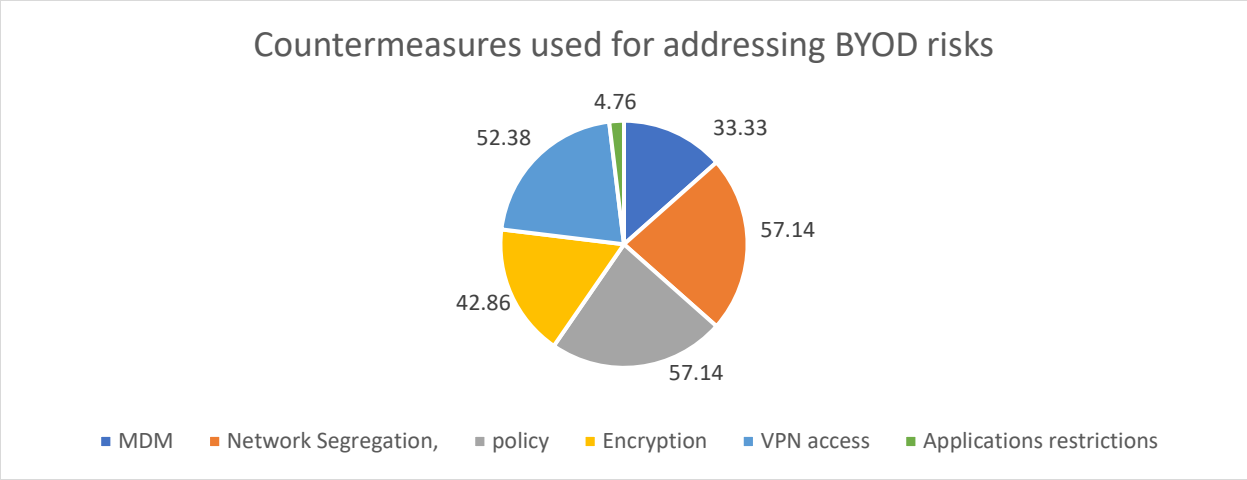


Figure 5.3: Control methods for BYOD environment used in organisations.

It is clear from the result that the 13 of the participants used policy and network segregation as countermeasures, while 7 participants answered that used MDM and 1 participant state that he/she used application restrictions. These results reveal an important fact that MDM control and application restrictions are the least used methods in a BYOD environment. This result indicates that the BYOD environment in these organisations is not secure enough to carry out business tasks safely and securely. Therefore, it is necessary for them to have effective control methods and countermeasures in place to ensure security when accessing business resources.

In order to develop the proposed framework, the design of the survey was designed to capture the risk-management processes that have been used by the information security experts among the participants. It is worth mentioning that they indicated using many risk-management processes in their organisations, and some more than one. The summary of the findings of these management processes collected from Question 7 is shown in Figure 5.4. (The full table of the survey answers is available in appendix A). To develop a risk management solution, it is necessary to know which risk management process steps are being used currently in the BYOD environment. 43.7% of the participants chose risk assessment as the most important step when developing a risk-management solution, 37.5% selected risk analysis, and only 0% selected a risk plan. This showed that most of the participants did not follow a proper BYOD risk plan to manage risks, and risks will happen, so, without a plan and the application of remedial actions, the consequences could be serious.


Figure 5.4: Risk management steps used to control BYOD risk

To identify the real gaps in risk management, it is essential to understand the effectiveness of the risk-management framework used in the selected organisations. 10% of the responses state that they are not following any framework or risk management standard in their organisations as is shown in Table 5.6. However, 60% of the survey participants stated that they practise ISO 27001 which is an information-security management framework. Only 10% follow the ISO 27002 risk management-framework and standards. 20% of the participants state that they are following COBiT, which is responsible for providing the relationship between business and IT environments.

The results from Question 8 (see Table 5.7) show that participants are aware of the frameworks. However, the extent to which they were applied in their organisations was variable.

Table 5.7: Current information security frameworks/standards used in participant organisations

| Question 8 | Responses | Respondents | Percentage |
|---|---|---|---|
| What are the current information security framework or standards used in your organisations | o COBiT | 4 | 20% |
| | o ISO 27001 | 12 | 60% |
| | o ISO 27002 | 2 | 10% |
| | o ITIL | 2 | 10% |

Table 5.8: level of synchronisation of participant IT strategy with BYOD IS strategy

| Question 9 | Responses | Respondents | Percentage |
|---|---|---|---|
| What is the level of effectiveness and control of these frameworks in a BYOD environment | o 10-30% controllable | **1** | 5% |
| | o 30-50% controllable | **7** | 35% |
| | o 50-80% controllable | **12** | 60% |
| | o 80-100% controllable | **0** | 0% |

As shown in the responses to Question 9 (see Table 5.8), 5% of the participants were agreed that the current frameworks and standards do not match the BYOD security requirements, where 35% state that there is a 30-50% match of effectiveness for risk management. However, 60% state that the capability of the frameworks to control the BYOD risks and threats is between 50-80%. It is significant that none of the participants were following any information security standard which has more than 80% or higher compatibility with the BYOD risks and security requirements. Therefore, there is a high possibility that the current standards and strategies used do not match the emerging BYOD risks and threats.

In Question 10 (see Table 5.9 and Figure 5.5), the participants were asked how often they update their risk management processes and framework. 30% of the participants never updated their risk management system which makes them more vulnerable to risks, 30% said that they updated every 5 years, 25% every 3 years and 15% every year. Considering the rapid change of technology in the world today every 3 years should be the longest period to wait before reviewing the risk-management system.

Table 5.9: How often the business risk management system is reviewed/updated

| Question 10 | Responses | Respondents | Percentage |
|---|---|---|---|
| How often you review/update your business risk management system | o Every year | 3 | 15% |
| | o Every 3 years | 5 | 25% |
| | o Every 5 years | 6 | 30% |
| | o Never reviewed | 6 | 30% |

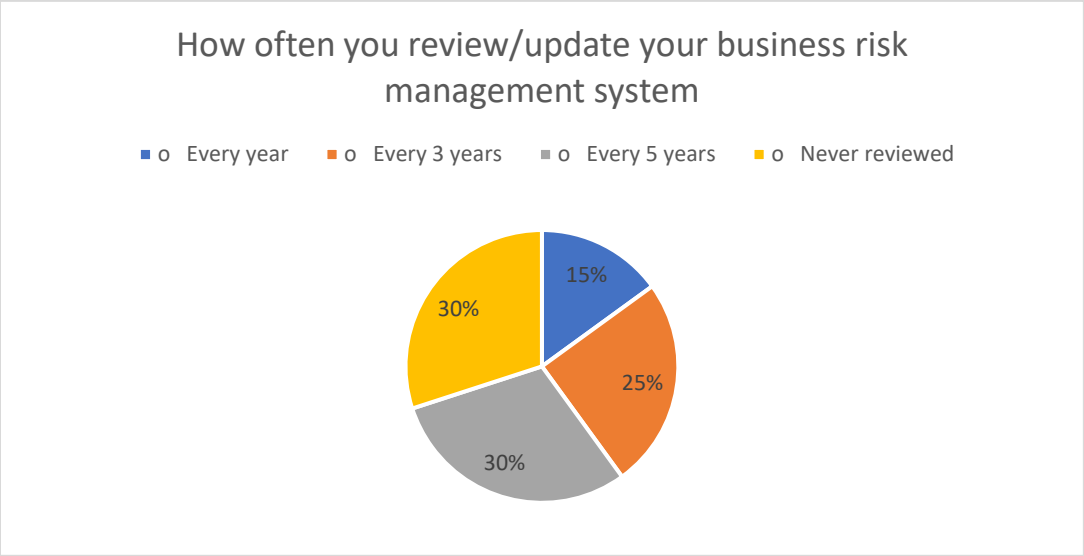



Figure 5.5: Review/update the business risk-management system

In order to propose a new risk management framework, it is necessary to understand the user behaviours and the activities carried out by them. The user activities are obtained from the event logs.

Question 11 responses (see Table 5.10) show that only 5% of the participants were using application-server event logs for developing their risk management systems and 95% were relying on some other means.

Table 5.10: Using the event log as part of risk management systems in Oman

| Question 11 | Responses | Respondents | Percentage |
|---|---|---|---|
| Do you use event log file to improve your risk management system? | o Yes | 1 | 5% |
| | o No | 19 | 95% |

### 5.3.1 Survey One: Qualitative Analysis:

The subjective data was designed to understand the environment, people, and context of the domain. Hence, survey-one was used to collect qualitative data using open questions which allowed the participants to add their own comments. The collected data was then subjected to

content analysis to provide valuable information on the behavioural concepts related to using BYOD in the business environment.

In the professional survey, there were two open questions. The first question inquired on the improvements needed to the security processes and risk management in the BYOD environment. The second question inquired on the technical improvements needed to provide the necessary countermeasures for those risks.

The literature highlighted the need for faster decision making to manage the increasing number of attacks on networks caused by the BYOD environment. The participants in the survey also confirm the risks to the organisation networks because of mobile applications. These mobile applications are from untrusted developers and sources, which sometimes contain hidden code (e.g., viruses or Trojans) designed to bring down networks or disrupt normal working. Shila et al. (2017) described the challenges to security from the ad hocking mobile networks. The applications are hosted by cloud servers and are in 'open public' mode which can lead to attacks because of the ease of access by unauthorised users. The participants highlighted the need to introduce application-management countermeasures to match the BYOD risk level.

In response to the second question, regarding the countermeasures being used to counteract the risks, the participants indicated that security managers were looking for smarter detection systems which were able to detect and prevent smartphone breaches. Also, they expressed the need to be able to monitor all smartphone activities. The proposed framework in this research will provide a centralised dashboard for all the smartphone users in the BYOD environment made possible by the merging of the function logs and MDM logs. The points raised by the participants in the survey can be seen in appendix A|, table 2

## 5.4 Survey Two: User Awareness:

The critical part during the development of security programs for an organisation is the awareness of end-users about the nature of the security systems. In the BYOD environment the end users are the controllers of the traffic and information on their devices, so it is critical that they are aware of the risks involved with using their smartphones on company networks, to achieve this with this

research a survey was designed and distributed to 225 participants from the same five organisations in Oman who took part in the first survey.

The rationale behind using the same participants was to discover whether the end users were aware of the practices employed by their organisations to predict, detect and mitigate against the risks in the BYOD environment. In order to determine the level of user the participants were asked to confirm their understanding by responding with yes or no answers to a series of questions, the questions and the responses from participants are presented in the following part. Question 1 of survey 2 is considered with participant affiliations with different organisations. Question 2 (Table 5.11 and Figure 5.6) shows that 44% of the user which representing 99 participants are not aware of the security measures used to protect their smartphones.

Table 5.11: Use of any security applications or features to protect smartphones

| Question 2 | Responses | Respondents | Percentage |
|---|---|---|---|
| Are you aware or do you use any security applications or features to protect your smartphones? | Yes | 126 | 56% |
| | No | 99 | 44% |

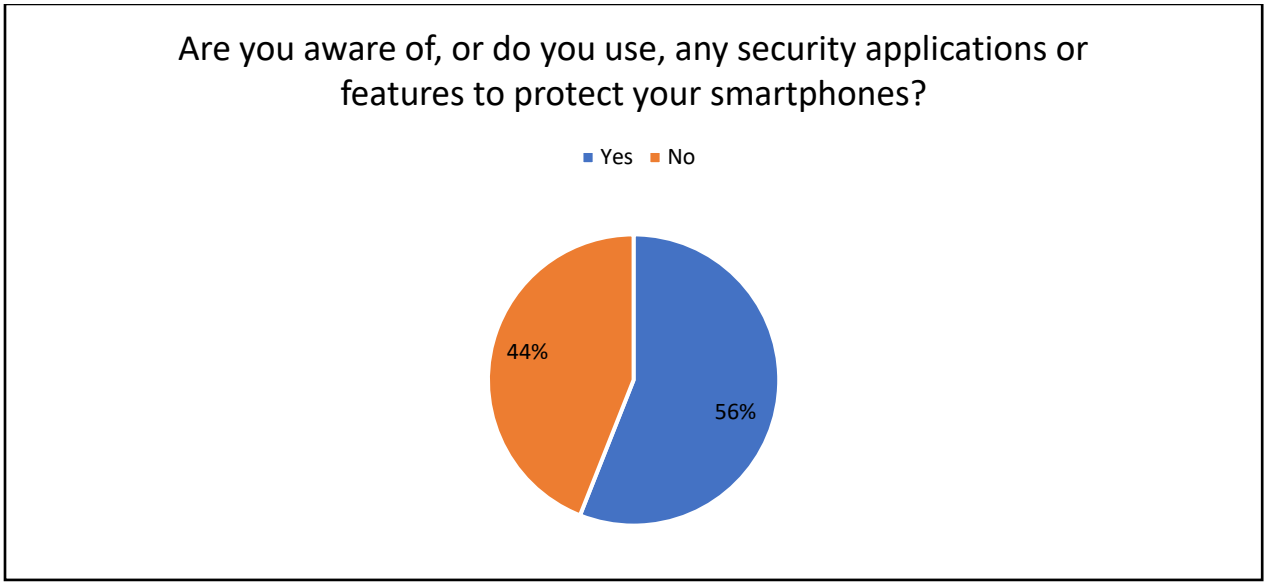



Figure 5.6: Level of Understanding of Smartphone-Security Risks

In Question 3 (as shown in Table 5.12), 32% of the participants replied to say they were not using any applications to secure their phones. These results show that there is an increased likelihood of risks due to the users' ignorance regarding the installation of security applications on their mobile phones and the need for measures to be in place to protect them.

Table 5.12 User defences against cyber-attacks on their smartphones

| Question 3 | Responses | Respondents | Percentage |
|---|---|---|---|
| Do you use any mobile application to detect the attack? | Yes | 149 | 67% |
| | No | 73 | 32% |
| | I never know that there are detection applications | 3 | 1% |

Furthermore, in Question 4 (as shown in Table 5.13 and Figure 5.7), 54% of the participants indicated that they had experienced data loss on their smartphones. This is an alarming situation for organisations and requires them to ensure that they maintain data availability on a priority basis. There are multiple reasons for data loss on user devices, hence, there is a need to have effective countermeasures in place to deal with the problem.

Table 5.13: User experience of smartphone-data loss?

| Question 4 | Responses | Respondents | Percentage |
|---|---|---|---|
| Have you faced any data loss in your smartphone? | Yes | 121 | 54% |
| | No | 104 | 46% |

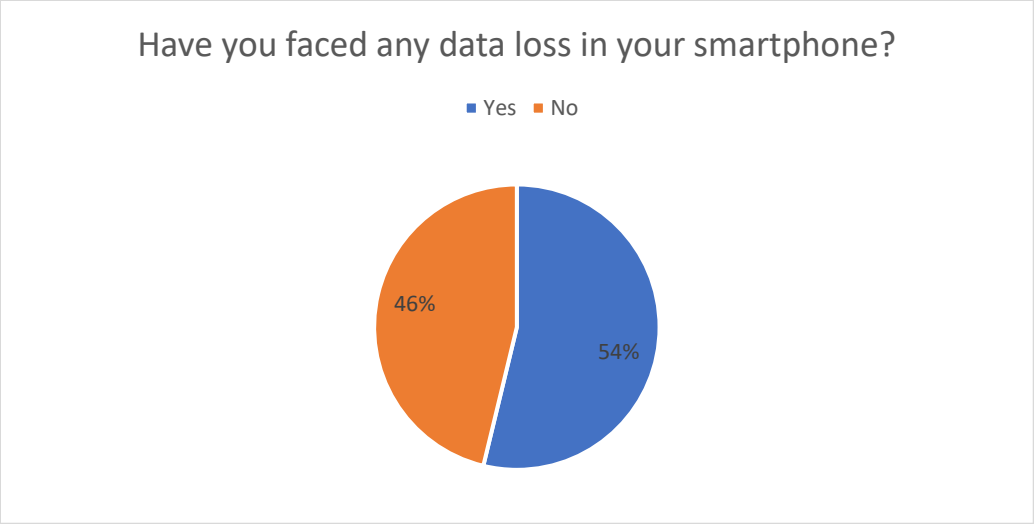



Figure 5.7: Data Loss Rate

In Question 5 (see Table 5.14), the reasons given by the participants for data loss on their smartphones showed that 34% of the participants specified fake and untrusted applications, and 16% specified malware from online services. The utilisation of function logs for risk prediction by should help to resolve these types of problem by giving an early warning of this type of risk.

Table 5.14: Reasons for smartphone-data loss

| Question 5 | Responses | Respondents | Percentage |
|---|---|---|---|
| What was the cause of the data loss? | Attack | 15 | 8% |
| | Fake application | 30 | 34% |
| | Online services malware | 28 | 16% |
| | Device damage | 56 | 24% |
| | Improper storage | 36 | 12% |
| | No data loss | 71 | 6% |

The results from Question 6 (see Table 5.15), shot that in order to protect their devices, users have various measures available to them, 60.8% backup their data on a regular basis and 17.3 % of them had cloud backup accounts. However, 16% of participants knew of the existence of measures, but they have done nothing in response or don't have any plan if they lose their data, so no action will be taken, with serious implications for possible business-data loss. 4.4% were not aware of the methods to protect their data and 1.5% said that they normally ask for help when any problems

occur which could be too late for the data to be recovered. These results have shown that administrative actions should be taken to ensure that data is not vulnerable to exposure, and should be in a safe and secure environment, and readily available to business users.

Table 5.15: User's awareness of measures to maintain data availability

| Question 6 | Responses | Respondents | Percentage |
|---|---|---|---|
| How do you apply disaster recovery when you face any damage and data loss? | Backup | 137 | 60.8 |
| | Cloud storage applications | 39 | 17.3 |
| | Do nothing | 36 | 16 |
| | Ask for help | 3 | 1.5 |
| | Don't know | 10 | 4.4 |

It is essential to know if the users had proper knowledge about the security settings in their personal smartphones. Question 7 (see Table 5.16) was designed to get this information. Security settings include enabled locations, applications permissions for applications, encryptions, and installation of protection software. 34% of participants knew about the security setting in their smartphones and 38% said they had limited knowledge. However, the responses from participants showed that 28% of them did not know, which meant they probably didn't consider the need for securing their phones and personal data. These results indicate the lack of user understanding in regard to BYOD security risks, showing again that the BYOD environment puts the business data held on the organisation networks at risk.

Table 5.16: Users applying security measures to their devices.

| Question 7 | Responses | Respondents | Percentage |
|---|---|---|---|
| Do you know how to use the security applications and settings in your smartphone? | Yes | 75 | 34% |
| | No | 64 | 28% |
| | Limited knowledge | 86 | 38% |

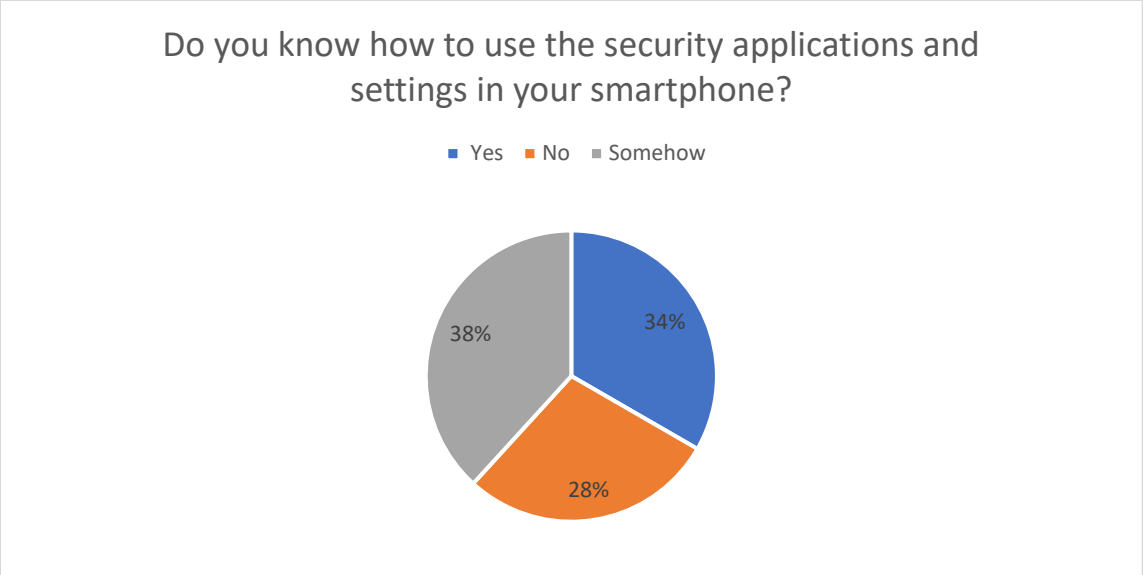



Figure5.8: Participant's awareness of smartphone security settings:

In Question 8 (see Table 5.17), the participants were asked if they needed security-awareness training from their organisation. 81% stated that they need training on the security capabilities to secure their personal and business information on their smartphones. This should act as an alarm to the organisations who are adopting BYOD. They need to act and take action to provide training and awareness sessions for their employees who hold business-information in their phones. The training not only provide knowledge of the security settings but should also cover the legal implications of losing business information or exposing the data to unauthorised people.

Table 5.17: user awareness training

| Question 8 | Responses | Respondents | Percentage |
|---|---|---|---|
| Do you think that you need training session to familiarise yourself with the process of securing business data in personal devices? | Yes | 181 | 81% |
| | No | 23 | 10% |
| | I don't know | 21 | 9% |

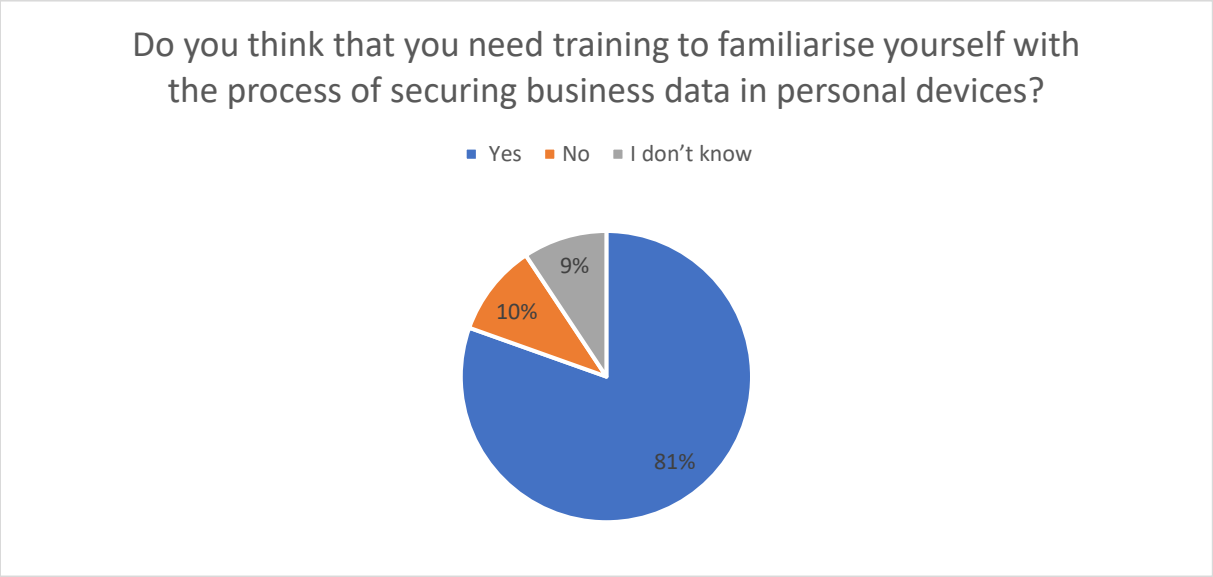



Figure 5.9: User Awareness Training

To conclude the user-awareness survey, the end users have a responsibility to secure their personal devices. The organisations also have the right to manage these devices as they contain business information. Nevertheless, the organisations should not have access to these devices as it is user-owned equipment, which poses challenging security issues to security managers and administrators. Finally, the organisations should have awareness sessions for maintaining data privacy and security in the BYOD environment.

## 5.5 Discussion and Recommendations

This chapter reflects on the findings from the surveys. The main aim was to find the current challenges in the |BYOD environment related to both the existing security-control methods and the application of security frameworks in Omani organisations. The survey also attempted to evaluate the technical challenges in the support mechanisms for risk management currently adopted in the government and private sectors. Additionally, the survey was intended to identify awareness level of smartphone users of the security requirements in the BYOD environment

The finding from these surveys demonstrates the gaps in the adoption of effective security and privacy measures in Omani organisations, for which a new framework has been proposed by this research. Figure 5.10 provides an overview of the requirements that need to be satisfied by the framework.

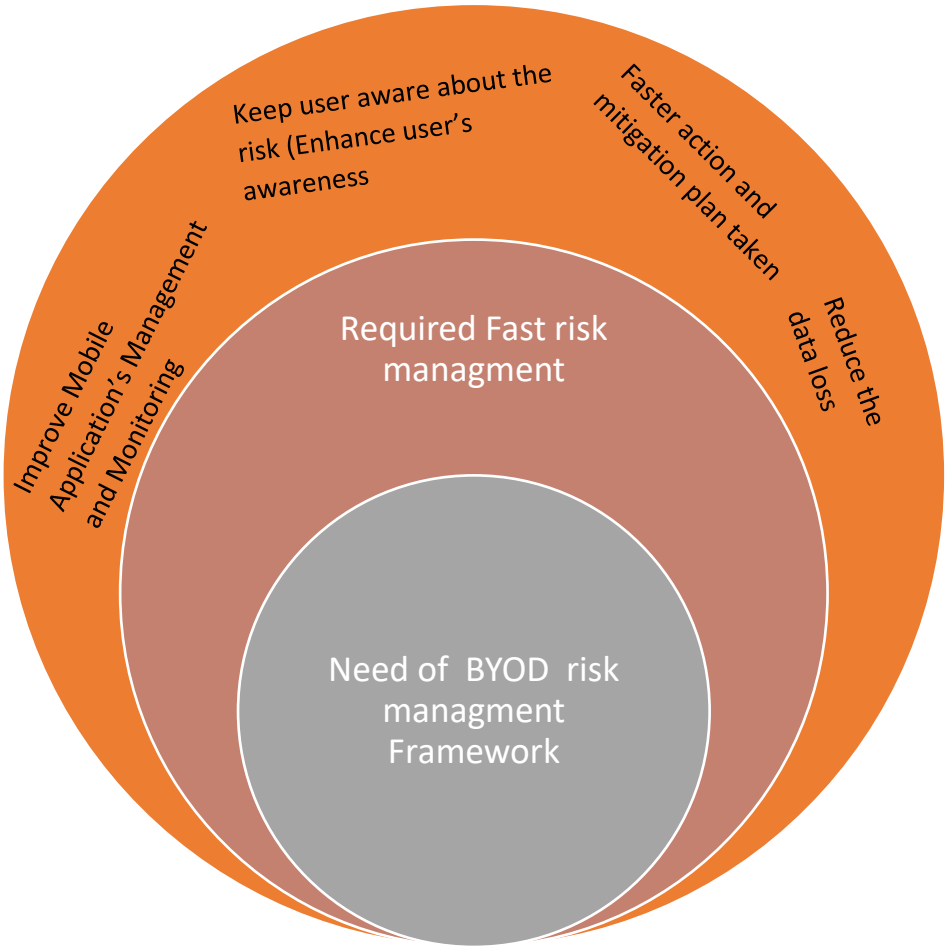



Figure 5.10: Survey data findings for the design of the proposed framework

The framework needs to meet the following requirements:

- Improve Mobile applications management:

As observed in survey responses especially in question 5 and 6 in survey one and question 3 and 4 in survey two, the mobile applications are considered one of the main sources of risk in BYOD environment. The control of these applications is challenging.

- Keep user aware of the risks (Enhance user's awareness):

As seen from question 8 in survey one and from question 1 and 7 in survey two, the participants and professionals agreed that the user knowledge needs to keep up to date regarding the latest BYOD security issues and challenges, which currently is not the case

- Faster risk management

This result, observed in the professionals-in survey one, especially in question 5, 9, and 10 responses showed that faster decision making, and availability of a risk-mitigation plan will help to reduce the BYOD risk impact for both users and organisations.

- Reduce the data loss:

The clear and most observed issues faced by users was the data loss. The results from questions 3, 4 and 5 in survey two show the data loss issue and its causes. In BYOD the data which can be loss from the user's phones can be business data as well, where this is the risk for the business itself more than the users. However, similar issue had been discussed in literature review in 2.2 section. These gaps lead into these two major requirements for a BYOD environment

- Accurate detection and timely detection of risks
- Timely response to detected risks

Therefore, it becomes imperative to propose a new risk management framework for BYOD risk from both server-side and client-side perspectives. All of the mentioned gaps are covered by the proposed risk management framework, where the user activity is detected through the log records and then the risk prediction through the traffic classifications. Notifications are then given to the security professionals to make them aware of the predicted risks. They will then be able to prepare for the risks and take the necessary action to avoid them.

Therefore, based on the results from the surveys the following recommendations are made:

1. User security awareness:

BYOD is based on the concept of using personal devices for carrying out organisational tasks, which means that the user would have to use the smartphones for business purposes. However, the user needs to be aware of the need for the protection of their devices as they contain data belonging to the organisation. As indicated in the user survey, the lack of user's awareness of BYOD causes many risks, including data loss and data leakage. User awareness of the security needs of the

BYOD environment is critical for the organisation. Sigh et al. (2017) identified seven risks caused by lack of user awareness, which include: devices lost, malicious applications, connections through public Wi-Fi, internet browsing, no security apps installed on smartphones, constant changing of user devices and a lack of data encryption (Singh, Chan, & Zulkefli, 2017).

Hence the major recommendation for the users is:

- Avoid installing unnecessary applications with many accesses permission requirement.
- Avoid public and unsecure Wi-Fi connectivity.
- Report any business data loss.
- Ensure of wiping of the business data in the event of device loss or theft of the device.
- Use a secure connection such as VPN to secure the data transaction and authentication details.

2. Institution security Recommendations:

The organisations which adopting BYOD, should keep reviewing the access policies and maintain the legal liabilities. They should also keep assessing the BYOD security needs which means maintaining control over processes, equipment, software, user devices and user behaviour. Security control means taking into account and making clear the responsibilities of all the relevant areas of the business environment, including IT, Management, users and mobile devices. In each of these areas, there are a set of control methods required, such as policies, risk management, human resource, frameworks, agent-based devices control, training and MDM (Melva M.Ratchford and Y. Wang 2018). Organisations should restructure the network or improve the network security to maintain the extra traffic which results from user smartphones. The extra network security can be through improving the monitoring, detecting and preventing of the risks from smartphone traffic. Traffic monitoring tools such as Wireshark, SDN (Software defined network), IDS, and IPS can be integrated with the BYOD environment to provide this extra level of security.

Organisations should maintain policies to serve the different layers that are interacting with a BYOD environment. AB Garba and K Armageo (2015) divide the BYOD policy into three layers, which are operational, tactical and strategic. However, for controlling the actions of the human

resources involved, the surveys and literature agreed that suitable and effective training needs to be provided to BYOD users and management.
Finally, the legal terms and conditions of the business should be updated to cover BYOD user access privileges, roles and responsibilities.

3. Recommendation to Oman government

The Oman E-law should be updated to include the necessary acts for the BYOD environment. These acts would need to consider both user and organisation privacy. In a protected area, the government could enforce a set of laws which apply for any organisations that adopt BYOD to ensure that legal liabilities are considered.

On the other hand, the government already has the Oman Cybersecurity Centre where a citizen can report privacy breaches or hacking of their systems. This centre publishes awareness messages to the city regarding the latest cybersecurity issues. Hence, BYOD awareness should be one of the subjects of these awareness messages. This action will increase the awareness of BYOD users and motivate other organisations to adopt BYOD as one of the smart city solutions.

## 5.6 Summary

This chapter has described the surveys used to collect the primary data for the research and the results obtained from the participants. The analysis of the primary data revealed the disparity in the use of security and privacy measures in various Omani organisations. The insight obtained from the survey was used to provide the recommendation for organisations and Omani government.

The data was analysed, and the results were then used to create the proposed framework discussed in the next chapter.

# Chapter 6: Proposed Framework

## 6.1 Introduction

The proposed framework represents the core deliverable from this research, which provides the mechanism for addressing the BYOD risk management problems presented in section 5.4 of this thesis. This chapter presents the components of the framework and the interdependencies between them.

The reminder of this chapter is as follows; Section 6.1 provides the overview of the framework. Section 6.2 describes the proposed framework's lifecycle and high-level architecture. The data-collection components, data processing, data labelling, classification and notification are presented in Section 6.3. Finally, the Summery of the chapter is provided in Section 6.4.

## 6.2 Framework Overview

The extant risk management practices and frameworks primarily focus on centralised network devices and users. However, the risk management landscape has been changed in recent years, as new smart and mobile devices have been incorporated in business networks to enhance the productivity and work flexibility. Moreover, the ability of the traditional risk management countermeasures to deal with emerging threats that exist in BYOD environment is restricted (Marchand, et al. 2017; Liu, et al. 2017, Bohn et al. 2006; Dannewitz et al. 2013). Therefore, it is imperative to have an effective risk management framework for BYOD environment, which can efficiently deal with privacy and other security breaches such as attacks on the system, loss of data and data leakage. This chapter aims to present the proposed framework which enables effective detection and prediction of threats in BYOD environment by analysing MDM log records and applications function logs records.

The proposed framework enforces the security and privacy policies set by the organisation. Indeed, it helps in detecting and predicting risks in traffic and suggests mitigation actions.

## 6.3 Proposed Framework

The organisations are striving to reduce the effect of BYOD risks in order to reap the benefits of BYOD. Therefore, it is important to have an effective framework which helps in reducing risk to a minimum level. A survey was conducted to achieve one of the main objectives of this research which is to conduct field study to analyse users' awareness of the potential security breaches and their consequences within BYOD environment. The goal of the proposed framework is to enable Omani organisations to address the security and privacy challenges of BYOD environment by addressing the limitation of the framework currently being adopted in these organisations. In order to achieve this goal a survey has been conducted to get deep understanding of frameworks and other security measures being used by Omani organisations. The survey was intended to get both users' and system administrators awareness of the BYOD security and also the adoption of various risk management frameworks. The development of the framework is driven by findings of the survey carried out in Oman. The adoption of the BYOD in Oman is still in its infancy. There are still some technological and social barrier in adoption of BYOD, but Omani Government is paving way for business and governmental organisation to adopt BYOD.

The proposed framework focuses on the enhancing of existing risk management frameworks by improving risk detection and risk mitigation, as well as, enabling the BYOD risk management to generate notifications of actions needed to prevent or mitigate the risks.

One of the most notable barriers to the adoption of BYOD in Oman is government regulation and this is true for other developing countries as well (French et al., 2014; M.S & Dell, 2019). Oman has its own unique culture and customs, where the top priority for the government is to protect citizen privacy. The Omani culture has its own privacy issues based on society norms and organisations place restrictions on unauthorised access to personal devices. However, in BYOD, personal devices contain both business and personal data which could conflict with the government regulations and legal requirements. Hence, the BYOD framework in this research should consider the legal obligations and regulations of the Omani government which will be discussed in section 6.4.

The other barrier to implementing BYOD management or risk management solutions is that users often have their social media accounts on the same device where they store business information. Therefore, the user may refuse access to their devices by organisations as personal privacy is a

major concern in Omani culture. In Oman, due to religion and custom, social data is considered as particularly sensitive, hence any BYOD management solution must consider the social issues involved. On the other hand, business managers do need to apply different measures because of the threat that social media in a BYOD brings to organisation security.

The Oman government has only updated the law to include electronic devices in the last three years. This new E-law does not yet include acts to cover the use of personal devices in a business setting as more organisations adopt BYOD technology.

However, they have initiated the Oman vision 2040 initiative and the plans will include the introduction of AI technologies and services into government departments so the E-law will be subject to continuous change in the future.

As the results of the survey in section 4.2 shows, the existing frameworks and risk management strategies lacked the measures for the mitigation of risks in the BYOD environment and these findings have also been confirmed by the literature (Arthur 2013; Sitnikova and Asgarkhani 2014; BOEHMER 2009; Salle and Rosenthal 2006; Huang, Zavarsky and Ruhl 2009). The survey also revealed that the MDM events log had never been utilised to detect risks which would have enhanced the risk-management capability of the organisations.

In the BYOD environment the end users are the controller of the traffic for both business and personal information. Therefore, it mandates a significant requirement for organisations to understand the risks of allowing the personal smartphones of their employees to access their business data. This is discussed in greater detail in section 4.2.1 of the analysis chapter.

The gaps and challenges identified in chapter 4 are used to come up with a new framework that enables:

- An accurate and timely detection of the risks in a BYOD environment
- A timely response to detected BYOD risks
- Faster decision making when BYOD attacks occur, so the users can take appropriate actions and the security manager can have access to user devices.
- The Reduction of data loss
- Allows users to predict the likely risks

The next section discusses high level architecture of the proposed framework.

### 6.3.2 High-level Architecture of the Proposed Framework

The proposed risk management framework has the ability to predict and identify security risks, and then to produce prevention notifications and mitigation/prevention plans to deal with them. The novelty of the proposed framework is to make timely decision and generate an effective action plan based on classifier output and the current security risk management policies of the organisations. The action plan will result in either mitigating or avoiding the action. However, running the datasets from the MDM and functions logs separately in the classifier step has not demonstrated the ability to manage BYOD risk and threats (Williams et al. 2016; Sahd and Rudman, 2016; Downer and Bhattacharya 2016; Leavitt 2013). The high-level architecture of the proposed framework is shown in figure 6.1

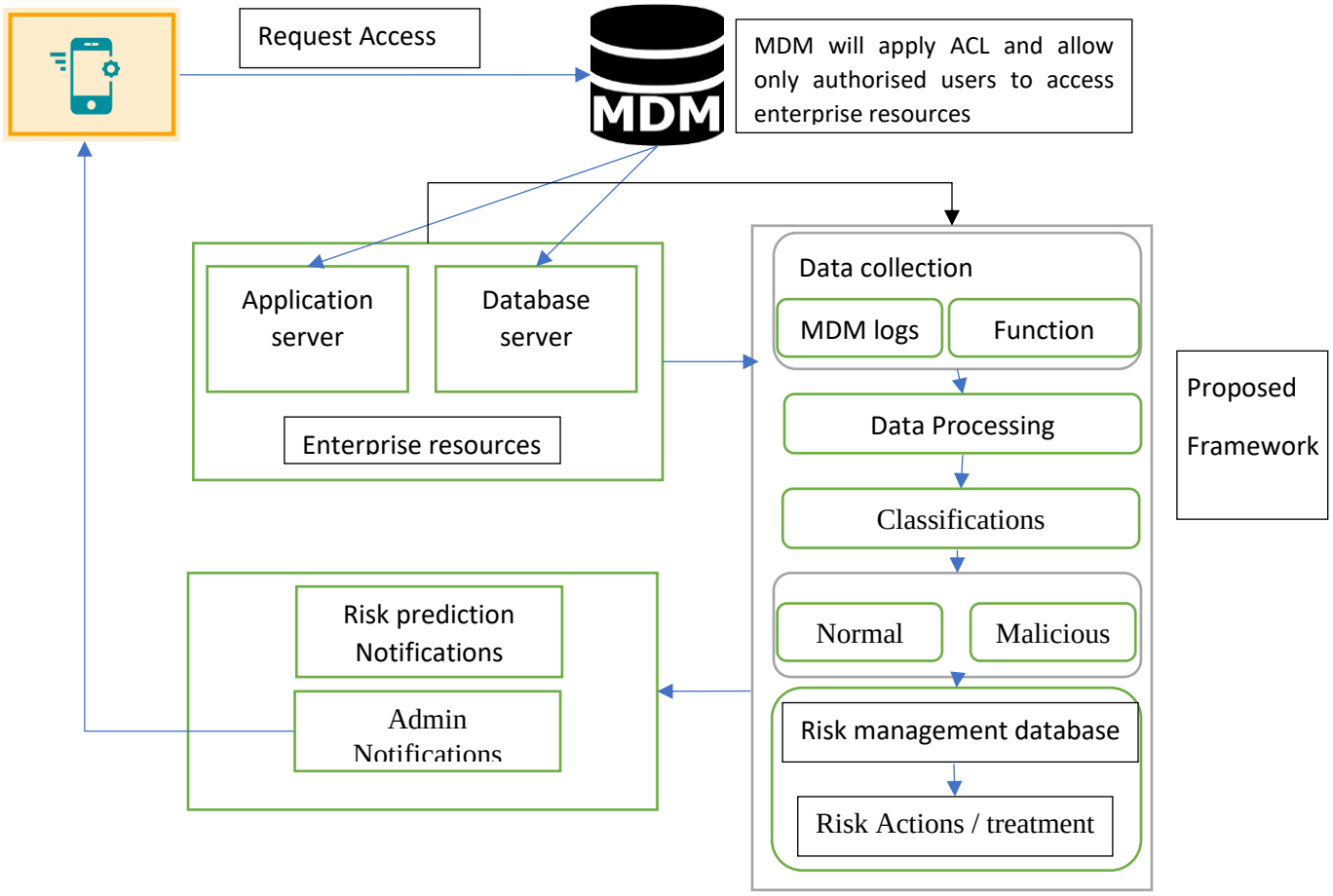



Figure 6.1 Proposed BYOD Risk Management Framework

### 6.3.2.1 BYOD Risk Management Framework Life Cycle

The proposed framework life cycle discusses the logical flow for each step in the framework processes. The following subsections define each phase of the framework and the related component.


Figure 6.2 BYOD Risk Management Framework Life Cycle

The framework consists of the following steps:

1. The user installs the MDM agent in advance before connecting to network resources.
2. The user connects to organisation resources through MDM
3. The MDM administration team apply Access Control List (ACL) which ensures that only authorised users have to access enterprise resources. The BYOD access control should be applied based on employee's category and roles.
4. User access to network database and applications.

5. The administrator extracts the log records of both the MDM activities log and the log of user accesses to the system-level functional activities.
6. The framework uses these log records to initiate the functions for the prediction/detection of risks
7. The framework classifies the log entries using machine-learning algorithms. The output is classified as either a normal or abnormal event.
8. Based on the classification result the framework generates the required prevention/remedial actions.
9. The final outcome is sent to the smartphone users as notifications and also used by the system to take remedial actions.

## 6.4 Components of the Proposed Framework

This section describes the components of the proposed BYOD risk management framework and relationship between them.

### 6.4.1 Data Collection

Currently, the business-computer network is called hybrid networking, as it contains multi service-platforms of technologies which include internal domain, remote cloud services and poorly managed smartphone (i.e. BYOD) connections. This research is concerned with the security and privacy threats that exist when using personal devices in business environments. The survey result for Omani organisations and the literature review has both revealed gaps in the approaches taken (see section 6.1) that are important to address in the proposed framework. It is imperative to have an effective framework that has the ability to detect and predict malicious activities in the BYOD environment. The framework must have data related to user activities, both at the MDM and application level. The two main sources of this data are the BYOD log file and the system functional activities log files. These files provide records for both MDM-level and application-level activities. The existing BYOD risk-management frameworks only takes MDM log-file activities without giving any regards to application-level activities. Also, MDM logs files are very rarely viewed or audited by the system administrators.

The following subsections discuss the role of MDM logs and function logs in the proposed risk-management framework.

#### 6.4.1.1 MDM Events Log

The Mobile Device Management (MDM) system was one of the solutions which was proposed in recent years to manage the BYOD environment which provides the ability to enforce policies on BYOD devices (John and Weintraub 2012, Bashayer Alotaibi and Haya Almagwashi 2018). The MDM-events log file, maintained by the MDM server, contains the raw records of user activity in the BYOD environment. These records are processed and labelled in order to make them suitable for model training and testing. Also, the MDM logs monitor the behaviour of the BYOD-users behaviour and records any attempt to breach the organisation policies.

The log-file analysis enables security audit, security compliance, and policy compliance, and helps to find the details of user-behaviour. The log analysis also helps to track the changes in policies or traffic-load to detect any vulnerabilities. Additionally, the process of log analysis helps to detect failure of the device network, services and even identify and track the location of lost devices. Therefore, this analysis helps to detect and predict the BYOD risks from real-time event logs. More details about MDM-device enrolment and functions can be found in chapter 7.2.

#### 6.4.1.2 Database Server /Function Systems Log

Organisations currently provide alternative access options for different source such as cloud base applications. The cloud-based services increase the availability of services and, for security reasons, isolates the user applications in the cloud, away from the organisation. In this research the application server is used to extract the activities of users of the organisation applications and services to generate the function logs. These function logs will then be merged with MDM logs, as MDM only works as an observer to authenticate users and set their permissions, which is not enough to reduce the BYOD risks. Hence, to deal with the BYOD risks, there is a requirement to monitor both the user activities and behaviour.

*Merge MDM and functions Log*

To improve the BYOD-risk detection and prediction, the proposed framework aims to increase the security level by using both the activities of users from the MDM log and also the activities related to application-level functionalities. A novelty of our proposed framework is that it takes into account both application-level and system-level events to generate the appropriate prediction of risks and their associated remedial actions.

The event-logs phase is a critical step in the development of the proposed framework which contains the following steps for data collection:

- The MDM logs are first extracted from MDM server which is the connection point of the smartphones connected to the organisation network. The MDM server maintains a log record of all the smartphones registered with it.
- Extract the function file which contains the event log generated by the application/database server.
- Merge the log records in one file: To increase the risk-detection ability and the accuracy-level of the proposed framework, the MDM log and functions log were merged into one dataset containing the smartphone log and issues from the MDM server as well the user activity and functions. Since both event-logs files come from separate sources they have different formats so the relevant information from both log files has to be manually extracted and merged together to give a unified view of events. To the best of the researcher's knowledge (at the time of writing this thesis), there is no existing BYOD framework that uses both the MDM event-logs and the application server-logs to deal with BYOD risks. The main focus of the existing frameworks is on just the MDM logs, which on their own to not give enough protection against threats to the system resources.
- Process the generated logs extracting the data for both the MDM and function services logs ready for the cleansing and labelling step which follows.

## 6.4.2 Data Processing

The data collection is an important part of the development of the proposed framework. The sources of data collection are the MDM log, data server log and application functions log. These

log files have raw entries of data and in some cases has missing information. This makes it imperative to process data and convert it into a proper form. The data processing includes the data identifications, data cleansing and data labelling. The data cleaning process is explained in the following subsection

## Labelling

Data labelling is a step which is required to prepare data for model training and testing. Dataset labelling is a process for tagging information in the dataset in a clear and unambiguous way. The purpose of data labelling is to define pieces of the information by assigning them attributes. After the data labelling is complete, machine learning algorithms are applied for training the model to predicate the data output.

In this research the data labelling was done manually because the data which was generated from both the MDM and application services were in a text format. Such as the following examples

Table 1: MDM events log samples

| Type | Activity categories | Activity details | |
|---|---|---|---|
| Information | Inventory | Inventory scan success for device iPhone | |
| Information | Enrollment | Device iPhone enrolled successfully | |
| Information | Inventory | New App ""Oman Airports"" has been detected | |
| Information | Inventory | New App ""Ø§Ù„Ù…ØµÙ Ø§Ù„Ø¬Ùˆ Ø§Ù„""  has been detected | |
| Information | Settings | Geo-Tracking settings has been updated to track devices only when lost. | |

Table 6.2 Function events log samples

| Type | Activity categories | Activity details |
|---|---|---|
| system | exceed the access limit | more than 5 attempts |
| Logs | Log report viewed | The user viewed the log report for the course |
| Logs | Log report viewed | The user viewed the log report for the course |

To test and train classification model labels should be given to all columns. The data labeling was carried out and it was shown to professionals from different sectors who already participated in the survey. The participants validate the class labeling and gave their inputs of normal and abnormal events in the log.

Limitations and Challenges:

The most challenges encountered in MobileEngin MDM were due to some Arabic based applications. These entries were hard to detect in log file as they show special characteristics in the events log. Hence, after communication with MDM vendors the issues were resolved. Additionally, the minor difference in professionals' opinion of what normal and abnormal events logs was another challenge reconcile.

## Model Training

To run any machine-learning algorithms, a training dataset needs to be collected to train the model. A training model is built to understand how the chosen algorithm works and generates the results. The dataset consisting of both MDM and application-function log files, is divided into two sets, one for training and one for testing the model. The trained model is used as a classification model to classify events as either normal or malicious.

## Data Cleansing

The generated data may contain incomplete or missing values. Therefore, it is important to clean it in order to reduce experimental errors or faulty results. The errors include missing values, misspelt or invalid data. Although, the data-cleansing concept appears complex, this process becomes easier nowadays through the use of software that is designed for the purpose. For example, the Keel software designed by Alcalá-Fdez et al. (2009). "Keel" refers to Knowledge Extraction based on Evolutionary Learning. It was observed from collected log files that there were missing values for different events. The missing values were called "null values". Hence,

losing the presence of null values is considered as an issue because the gathered feature will lose part of its usefulness

## Model Testing:

The testing dataset is separate from the training dataset which used for the final evaluation of the trained model. In this research the testing set represent 30% of the dataset. The testing dataset contains similar data to the training dataset from both the MDM and application-function log files. The major difference between the training dataset and the testing dataset is that the training dataset determine the SVM value where the testing dataset evaluates the decision value.

To clarify the classification process with using both training and testing dataset, the process flow is shown in figure 6.3.

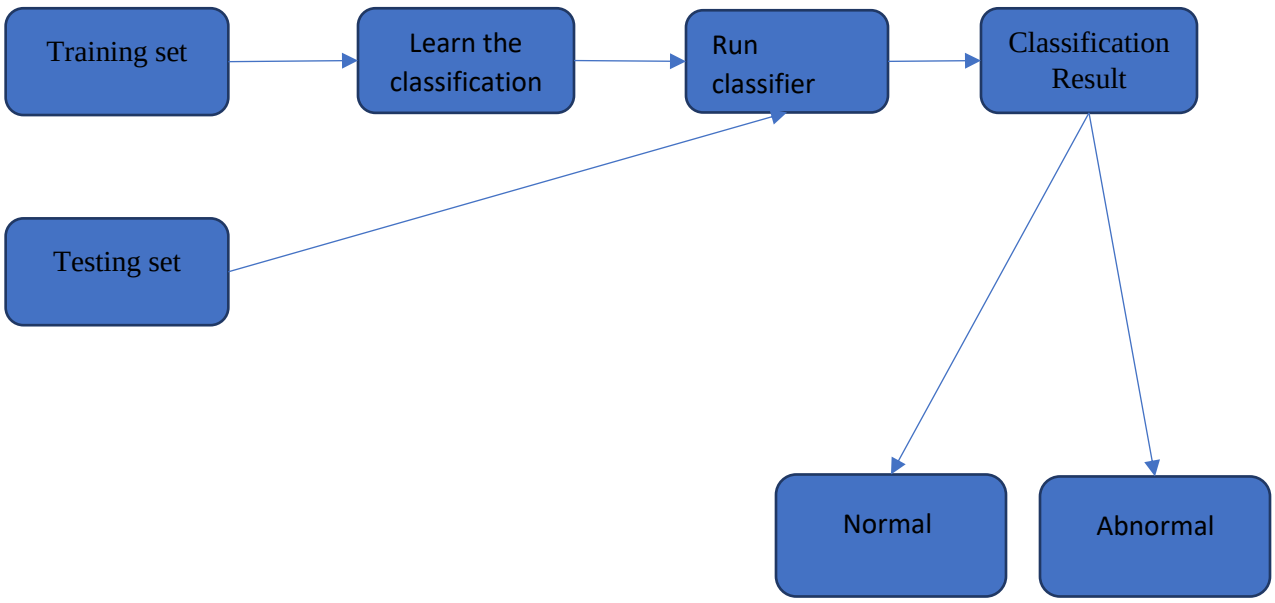



Figure 6.3: Classification Process

### 6.4.3 Classification:

Risk prediction is required to identify the likelihood of risk and helps in the preparation of avoidance/mitigation plans to avoid any eventual harm to the organisation resources. Therefore, this research work focuses on improving the risk management for the BYOD environment. The proposed framework enables the specification of the attributes and characteristics of the events from the event logs which are considered to be malicious. The abnormal events could be increased traffic load, devices lost, alarm logs, location tracking, locked devices, policy breaches, unauthorised applications, downloads, and exposed documents are all examples of malicious events.

The novelty of this research comes with the proposing of a framework which classifies the MDM and functions log records into normal and abnormal events. The proposed framework is designed to improve the risk management in a BYOD environment. Due to the nature of this problem which required to generate two prediction class either normal event or malicious event using labelled dataset, a supervised machine-learning algorithms was selected as it is more suitable for this research (Samal & Panda 2017 and Al-Janabi, et al. 2017). To detect any unusual activity, the research should provide full labelled datasets to compare the events based on the event type and then will be able to apply the detection mechanism.

The outcome of classification is used by the decision component to decide the action plan. Finally, user notification will be sent after detecting/predicting the risks; a notification will also be sent to the network administrators to give them notice of the threat. More details about the classifications algorithms and methods have been discussed in literature review chapter, in section 2.6

The classification of MDM logs and function logs is applied through a machine learning algorithm to generate the predictions. Section 6.3.3 section represents the theoretical basis for both machines learning together with machine learning in security-traffic analysis. The algorithm has been selected based on the analysis of the machine learning approaches described in Chapter 6.

### 6.4.4 Notifications:

One of the functions of the proposed framework is to generate notifications and send them to the users and administrators when abnormal behaviour is detected. The notifications include detected/predicted risk information and advice about actions to be taken. The notification will be passed to smartphones users only after administrator approval. The notification will include the detail of suitable actions that can be taken to avoid the threats and users should react to the risk within a specified time. Pushing the notifications to the users helps to increasing awareness of the possible threats and attacks. Additionally, it helps the administrators to understand the BYOD daily risks, thus enhancing the risk management systems and strategy. For example, if the prediction shows an abnormal increase in traffic from a specific application, it may be an indication of DoS attack, so a notification will be generated to make both users and administrators aware of the possible problem. The preventive action that could be taken would be to stop the source of abnormal traffic, which is the application that caused the problem. Also, if the log shows that there is a lot of attempts to get unauthorised access then a notification will be generated for both user and administrator requesting that the password should be reset. More risks and activities are explained in chapter 2 section 2.5.

The BYOD user will be notified of predicted risks to give them advance notice of a risk occurring so that they can take the necessary action to avoid it.

As discussed in this chapter section 6.2 there are legal conflicts when it comes to personal devices for processing business data. Hence, notifications were considered to be a mandatory part of the framework as the risk management within a BYOD environment should be owned by the users, to be advised of any possible legal issues, the notification should be generated in good time to allow the IT/Security manager to take the required action.

## 6.5 Framework Robustness

The framework provides robustness in detection of malicious activities in BYOD environment. Rigorous testing of model was carried out to ensure the framework is robustness in operational

environment. The test results have shown high accuracy of the prediction algorithms used in the proposed BYOD framework. The proposed framework is not able to deal with new unknown cases as such cases were not used while training the model. Hence, to deal with these new cases the model must be retrained by including new cases in the training set and test set.

## 6.6 Summary:

This chapter has discussed the components of the proposed BYOD risk-management framework. The purpose for proposing the framework is to cover the existing gaps in the BYOD environment which have been highlighted in the surveys. The surveys uncovered risks such as data loss and lack of user awareness. Additionally, as detailed in the analysis chapter, the surveys uncovered problems in the capabilities of existing security frameworks to manage BYOD risks. Hence, the proposed risk-management framework was designed to improve the detection, prediction and mitigation of risks. Moreover, the framework by predicting the risks helps to avoid or reduce the impact of risks.

Table 6.3 matrix to highlight each step of the framework and how it will be used to improve risk management.

| | Detect risk | Predict risk | Avoid risk | Treat the risk |
|---|---|---|---|---|
| MDM logs | ✓ | ✓ | | |
| Functions log | | ✓ | | |
| Classification | | ✓ | ✓ | |
| Notifications | ✓ | ✓ | ✓ | ✓ |

Table 6.4 lists the focus of the existing countermeasures and their limitations and indicates the advantages of the proposed framework.

| Research | Focuses | Countermeasure | Limitation |
|---|---|---|---|
| Patel et al. 2013 | Proposed a new level of Intrusion detection system (IDS) services within the cloud. This system works to maintain the data, user and resource security and privacy. The IDS Cloud is composed of layers which are: network IDS services, host IDS services and Applications IDS services. | IDS | Just segments the traffic and filters it. If there are malicious packets they will be discarded. Hence, it is waiting the risk to occur and then react. The proposed framework predicts the risk before it becomes a threat |
| Mitchell and Ing-Ray Chen 2013 | Technique enhancements through IDS to detect the Cyber Physical System (CPS). CPS is used to control and manage the physical infrastructure | IDS | It is taking care of one concept of security only which is a physical security and mobile devices. However, the proposed framework is comprehensive in its approach utilises events both from application log file and MDM log file |
| Marchand, et al. 2017 and Liu et al. 2017 | IDS enhancements in hyper network connections | IDS | It is a reactive approach. The proposed framework is proactive predicting the risks before they become a threat |
| Stiawan, et al. (2010) | surmised the security challenges as signatures issues, traffic volume issue, design topology, logging | IPS | It is based in normal network traffic and web traffic, which is not really analysing the user |

| | | | |
|---|---|---|---|
| | and defence IPS devices sensor management and collaborations | | activity through functions logs like the proposed framework |
| Scarfò & Maticmind SpA (2012) | have proposes a solution for BYOD environment which is to create different zones called the Cirtix IT delivery Model which contain two levels of firewall security. The proposed solution includes traffic filtering, clustering and classifying the data from the BYOD environment before it reaches the network | Firewall | This solution is only analysing the access level risks but not the usability risks like the proposed framework |
| Bohn et al. (2006) | Proposed an approach called SIREND which integrates with the stack schema and uses the current devices to enhance the security and management, to achieve the desired level of security in a hybrid environment. Their framework is concerned with controlling of services and apply the policy-based approach on networking requirements. The authors proposed a clear division of the structure and protocols to enhance the network-security performance. However, this approach ignored the risks through services usage and other issues related to the BYOD. | General management approach | However, the approach did not cover risks related to the services usage by BYOD users and it is not compatibility with the BYOD environment. The proposed framework uses functions logs and MDM logs to predict risks based on users' behaviours. |

| | | | |
|---|---|---|---|
| Guo, et al., 2004; Downer and Bhattacharya 2016; Leavitt, 2013 | Through the literature the researchers identified MDM security vulnerability, attacks and limitations which reflect on the system performance | MDM weakness | MDM had limitations in the tracking of traffic, and it just controls the data and policy. Does not have risk prediction like the proposed framework |
| application (Dhingra, 2016) | MDM functionality | MDM | Although, MDM is focusing on both content and application, it cannot detect malware through the phone it can only manage the data trafficking. The proposed framework is able to adapt to new malware once identified |
| Kathleen Downwe and, Maumita Bhattcharya (2016) | Compared different literature inputs and highlighted the limitations of the BYOD solutions | MDM | No main solution just a review of the literature. The proposed framework provides a solution |
| P. Kodeswaran et.al. 2012 | proposed a framework specially for the Android infrastructure, | BYOD Framework | Does not guarantee the data security in case of device lost or stolen as analysed by Sara Ali et al. (2016), unlike the proposed framework. |
| Musa Abu-Bakr Muhammed et al 2017 | Propose access restriction based on user profile | BYOD framework and event-log filtering | Restricts access before the user is authorised to network resources. However, this could affect the performance of the employees and restrict the security characteristics based on |

| | | | |
|---|---|---|---|
| | | | listed profile threats only and is not able to detect new abnormal threats, which the proposed framework is able to do. |
| Petrov.D and Zanti.T 2018 | Propose security framework to secure BYOD environment from 3 main intruder attacks. | BYOD Framework | Just focus on the three types of attacks so is not as comprehensive as the proposed framework |
| Zeeshan. A and Nazia. B (2019) | Proposing BYOD security framework. They highlight the security threats and possible mitigation. | BYOD Framework | The built framework focused on specific threats. Hence, any new threats will be unpredictable. The proposed framework will adapt to the changing nature of threats once identified |

# Chapter 7: Evaluation of Proposed Framework

## 7.1 Introduction

This chapter describes the steps of the evaluation process for the proposed BYOD risk management framework. The role of the evaluation is to prove the ability of the proposed solution to answer the research questions and achieve the objectives. This chapter aims at evaluating the proposed framework and validate the research findings. Additionally, the evaluation will demonstrate the contribution of the proposed solution to the research community. This chapter includes details about the targeted groups selected for evaluation from Omani organisations. The focus of this chapter is to get framework evaluated by the participants from different Omani organisation that took part in original survey. The participants endorsed that framework addresses the security privacy concerns in the BOYD environment. A prototype is also developed to show the accuracy of the proposed framework.

The contents of the evaluation briefing-session are provided in section 7.2. Section 7.3 provides the evaluation parameters. Section 7.4 presents evaluation questions. And finally, section 7.5 presents the analysis of the responses from the evaluators.

## 7.2 Targeted Groups for Framework Evaluation

As discussed in the survey chapter in section 5.1, the research will use participants from five Omani organisations to evaluate the proposed framework. The ten evaluators were used, and they are comprise of security managers, IT technicians and network administrators. Two of the evaluators work for Omani government in the National Security Centre with an exceptional level of knowledge of the BYOD environment and risk management. The other eight evaluators have more than five years' experience in information security management, risk management and

cybersecurity. The rationale behind selecting evaluators from BOYD security and cyber security is to evaluate our proposed framework from both prospective.

## 7.3 Evaluation Briefing Session:

Owing to the need to isolate the evaluators because of the COVID-19 Coronavirus the briefing session was conducted online. The purpose of the session was to explain the objectives of the evaluation and the process for verifying the research framework, together with an overview of the framework workflow and associated parameters. A discussion of each stage took place to give the evaluators a complete understanding of the proposed framework and the results generated. The purpose of the evaluation briefing session was to:

- Allow the researcher to explain all the concepts and objectives of the evaluation stage.
- Allow the evaluator to understand their role and to clarify any points made by the researcher.
- Give the evaluators detailed description of framework components and its functioning.
- Allow the researcher to discuss the checklist questions for the evaluation.

## 7.4 Evaluation Parameters:

Framework Flow: This gives a structure of the proposed solution and the flow of the data and shows the sequence and relationship between different entities in the framework. It also highlights the role of each component in the framework and relationships between various components of the framework.

Risk Sources: This parameter is to specify the scope of possible risks that could occur. The sources will be input to the framework and will be used for risk prediction. In this research the MDM event logs and function logs from business systems are used as risk sources. Different kind of risk were explained and how they can occur and can be identified

User privacy/ethics: Any proposed solutions should take into account the privacy of the personal data held on the smart devices belonging to BYOD users, as well as ethics considerations in context of Omani culture. Privacy concerns were given due consideration in context of Omani culture.

Classifications: The input datasets should be analysed to predict to whether events are normal or malicious. Machine learning component is responsible for taking various actions as input and classify them as normal and abnormal event

Risk Accountability: Even though the users accessing the system have already been authenticated the framework should consider the accountability for any risks detected. This should include ethics issues, responsibility for risk and the authorities who need to be notified.

Risk Audit: This step measures the effectiveness of the risk treatments and responses. The proposed framework should create notifications and store the classifications results and any required actions in the risk database for reporting purposes.

Risk Performance: This is the need to evaluate the proposed solution in terms of services, actions, as well as time and risk reduction to a previously determined level.

All of these parameters are used to construct the evaluation questions and evaluate the proposed BYOD risk management framework.

## 7.5 Evaluation Questionnaire:

A checklist was created and distributed to evaluators. The checklist included the main evaluation parameters which were framework flow sequences, risk accountability, risk sources, risk performance, classifications, and risk audit. The main concepts and acronyms used in the evaluation checklist were as follows:

- MDM: Mobile device Management system.
- Function log: This contains log records which have been extracted from the e-services and databases of organizations.
- BYOD: Bring your own device.

Table 7.1: evaluation checklist questions

| | | | |
|---|---|---|---|
| **1. Do you think the framework covers risks of the BYOD environment?** | Yes | No | Comment |
| **2. Does the framework accommodate all security characteristics (confidentiality, integrity and availability)?** | | | |
| **Risk Accountability:** | | | |
| **3. Do you agree that the framework enhances the security accountability?** | | | |
| **4. Do you think that the proposed framework will enable faster detection of the risks and their associated responsibility?** | | | |
| **Risk Resources:** | | | |
| **5. Does the proposed BYOD risk management framework match the organisation processes and policies for BYOD adoption?** | | | |
| **Risk Performance:** | | | |
| **6. In your opinion, does the proposed framework enhance the risk detection** | | | |

| | | | |
|---|---|---|---|
| **performance of the risk management process?** | | | |
| **7. Do you think using MDM and the function logs in this framework has enhanced risk management performance?** | | | |
| **8. Do you agree that BYOD risk management has covered all the risks factors of BYOD environment and policies?** | | | |
| **Classifications:** | | | |
| **9. Do you think the classification method used is the best solution for the detection of malicious activities in BYOD scenarios?** | | | |
| **10. Do you think the classification attributes are accurate and clear?** | | | |
| **User privacy/Ethics** | | | |
| **11. Do you think the proposed framework adequately considers the privacy requirements of the owner of the smart device?** | | | |
| **12. Do you agree that the notification generated by the** | | | |

| | | | |
|---|---|---|---|
| **framework ensures compliance with ethical and legal factors?** | | | |
| **Risk Audit** | | | |
| **13. Do you think the proposed framework adequately audits and documents risks?** | | | |

The evaluation checklist questions have been designed to achieve the objectives of this research and to measure the accuracy of the proposed framework. The evaluators will answer the questions in Boolean mode by replying Yes/No. and they can add their comments and feedback if required. The Boolean mode was used to simplify the evaluation process and reduce the time taken for evaluation. A detailed analysis of the checklist used for the evaluation is provided in section 7.5

## 7.6 Evaluator's answer analysis

The evaluation checklist was sent to the researcher by email. The data was extracted and analysed using Microsoft excel spreadsheets. Closed questions with yes/no answers were used and evaluators could add their feedback if they want to. The responses to the questions were as follows:

**Question 1: Do you think the framework covers the internal and external risks of BYOD?**

All evaluators agreed that the proposed framework of BYOD risk management is able to accommodate the risks associated with BOYD environment. This indicates the proposed framework give due consideration to BOYD risks.

**Question 2: Does the framework accommodates all security characteristics (confidentiality, integrity, and availability)?**

All evaluators agreed that the proposed framework supported all functionality required of the security triangle which were confidentiality, Integrity, and availability.

**Question 3: Do you agree that the framework enhances the security accountability?**

All evaluators agreed that accountability in terms of ethics considerations together with the associated responsibilities, and authorities was maintained by the proposed framework.

**Question 4. Do you think that the proposed framework will enable faster detection of the risks and their associated responsibility?**

All evaluators agreed that the framework would enable faster detection of risks and their associated responsibility as framework uses both MDM and functional logs.

**Question 5. Does the proposed BYOD risk management framework match the organisation processes and policies for BYOD adoption?**

All evaluators agreed that the framework covers organisation processes and policies for BYOD adoption this adding strength to the proposed work to generate the accurate and suitable risk detection.

**Question 6. In your opinion, does the proposed framework enhance the risk detection and prediction performance of the risk management process?**

All evaluators agreed that risk detection and prediction could be enhanced due to use of both MDM and function long.

**Question 7. Do you think using MDM and functions logs in this framework enhanced risk management performance?**

All evaluators agreed that incorporating the MDM and functions logs enhanced risk management performance.

**Question 8. Do you agree that BYOD risk management covered all the risks factors of BYOD environment and policies?**

Nine of the ten evaluators agreed that all the risk factors and policies of the BYOD environment were covered by the framework. After discussion with the one evaluator who disagreed it transpired that unexpected risks and unimplemented policies were being considered which was not really about the proposed framework performance.

**Question 9. Do you think the classifications method used is the best option for detection of malicious activities in BYOD scenarios?**

Nine of the ten evaluators agreed that the classification system used was the best option. Discussion with the one evaluator who did not agree showed that the reason for disagreement was not related to the classification method but that the evaluator did not agree that certain activities were malicious.

**Question 10. Do you think the classification attributes were accurate and clear?**

Eight out of ten of the evaluators agreed that the classification attributes were accurate and clear. Discussion with the three who disagreed showed a misunderstanding of the background work that was performed.

**Question 11: Do you think the proposed framework adequately considers the privacy requirements of the owner of the smart device?**

Nine out of ten evaluators agreed that privacy requirements were adequately considered. The evaluator who disagreed said that there was no notice or step in the framework stating a privacy level. Discussion showed that the proposed framework determines the user permissions and notifies th user as appropriate which maintains the privacy.

**Question 12: Do you agree that the notifications generated by the framework ensures compliance with ethical and legal factors?**

All evaluators agreed that ethical and legal factors were complied with.

**Question 13: Do you think the proposed framework adequately audits and documents risks?**

All the evaluators agreed that the framework adequately audits and documents risks.

**Summary of evaluation question results**

The core function of the proposed framework is its ability to predict/detect the BYOD risks using MDM and functions logs, so it was necessary to evaluate framework performance in term of the normal and abnormal events classification. The results from question 5 and 6 show that all the evaluators agreed that the framework performance in this respect was satisfactory. This is a great result which confirms the accuracy of the framework and its components.

## Comments and feedback analysis:

The following comments and feedback were received from the evaluators:

- The solution requires all organisations to adopt MDM

This evaluator stated that the proposed solution was only applicable if the MDM system has been installed in the organisations. An online discussion was conducted to understand and explain the feedback. However, Oman is moving into Smart City solutions, so organisations can now start building their smart connections using BYOD technology. Therefore, the proposed framework will be highly applicable now and in the coming years.

- Add policy management to framework and perform audit of logs.

Although the evaluators suggested adding policy management for BYOD in the proposed framework. MDM already applies policies for smartphone users. Also access control policies have been applied to different levels of the network.

- Update framework regularly to enhance risk management

Regular updates were needed to the framework to enhance risk management. This also has been considered during the structuring of the framework, by repeatedly extracting the logs from the sources and applying the classifications, as well as recording the risks in the database.

- The solution required backup servers to be used.
- MDM Logs and function logs should be available to support and enhance risk management and provide security for the system. Also, the notification procedure should be enhanced by providing a technique to confirm the identity of the user, such as a one-time password (OTP) to complete the processes.
- However, all evaluators were completely satisfied with the framework architecture, and agreed that the proposed framework would enhance the BYOD risk management experience if adopted by Omani organisations.

## 7.7 Prototype Development

After carrying out user evaluation it was decided to develop a prototype system. I will use Support Vector Machine (SVM) for the classification purpose as our problem is concerned with binary classification. The code for the classification is presented in Appendix D.

SVM is supervised machine learning algorithm, and it is used both for classification and regression problem. Here SVM will be used for classification purpose.

The dataset comprises of four features and a target. This data has two classes known as normal or malicious. We build the model to classify the type of events related to normal and malicious classes.

In the model building we use dataset of normal and abnormal events. This dataset is obtained from both BOYD log file and server log files and data is labelled manually. Participants were also involved in labelling of the data, where they confirmed normal and abnormal events. The reason behind involving participants to label the data is accommodate participant view of what is normal and what is malicious activity. Omani organisations were not willing to share their BOYD log files due security and privacy constraints. To my knowledge no organisation in the world had made BOYD log files available publicly. To address the issue of non-availability of the log files, I generated BOYD log files by simulating the various BOYD action in order to acquire required data for the training and test purpose. I have extracted the features from log file entries and created data set without labelling the instances class. The data file was then given to participants, and they were asked to label data instances as normal and malicious. Final dataset was formed after combing the data labelled by the participants and it was then used for model training and testing.

We divide the dataset into training set and test set in order to understand model performance. In the next section we will discuss machine different learning libraries and select a machine learning library to be used in the prototype implementation.

### 7.7.1 Machine Learning Libraries

There is a number of open source libraries available for machine learning. These libraries have been implemented in different programming languages such as Python, Java, R, C++ and GO languages. Following machine learning libraries were considered to be used in the implementation of the proposed framework.

1. KerasKeras is a popular neural network library. It has been integrated into TensorFlow as a one of its core libraries. It has been used many neural network applications.
2. PyTorch is considered as one of widely used python libraries in machine learning. It has been used in deep learning applications. PyTorch has also extension in C++ and C.
3. Scikit-Learn is an active python library for machine learning and it provides algorithms for classification, regression and clustering etc. The feature of this library is its flexibility, and its integration ability with other machine learning libraries. Scikit-Learn uses libraries such as NumPy, SciPy and Pandas.
4. Weka is a machine learning package and it is implemented in Java. Weka is open-source software and provide implementation of different machine learning algorithm.
5. Python-anywhere is other well-known python platform which can easily be used in cloud environment. This tool can be integrated with other machine learning softwares and provides support for running applications in cloud environment .
6. AWS Marketplace is a platform which contain thousands of software's and libraries to develop machine learning models and solutions. This platform can be used for cloud based machine learn classifications as it provides extensive catalogue that includes hundreds of services.

Weka tool has been chosen for the implementation of the prototype as it is free open source and provide a set machine learning algorithms and it is compatible with all operating systems environments. I have integrated Weka library in NetBeans integrated development environment to embed Weka in Java environment and use it as a Java library.

### 7.7.2 Evaluating the Model

Evaluation is carried out to understand how accurately the model can predict the normal and abnormal events. The accuracy of the model is calculated by comparing actual test set value and predicted values.

The model has achieved overall classification accuracy of 96.5% and for further evaluation, we also check precision and recall of the model.

The common performance measurement parameters of the model accuracy are as follows.

True Positive (TP): The model correctly predicts positive class

True Negative (TN): The model correctly predicts negative class

False Positive (FP): The model incorrectly predicts positive class

False Negative (FN): The model incorrectly predicts negative class

True Positive Rate (TPR) = TP / P

False Positive Rate (FPR) = FP / N

False Negative Rate (FNR) = FN / P

We calculate precision and recall as follow

Precision = TP/ (TP+FP)

Recall = TP/ (TP+FN)

F-Measure: It is harmonic mean of precision and recall. It provides a single score to address the concerns of precision and recall in a single number.

Detailed class accuracy is show in table 7.2 below

Table7.2: Class accuracy

| Class | TPR | FPR | Precision | Recall | F-Measure | ROC Area | PRC Area |
|---|---|---|---|---|---|---|---|
| Normal | 0.98 | 0.06 | 0.96 | 0.98 | 0.97 | 0.93 | 0.93 |
| Malicious | 0.93 | 0.014 | 0.97 | 0.93 | 0.95 | 0.95 | 0.90 |

**Confusion Matrix**

The confusion matrix is a numerical presentation of the findings of classifications results. Each column in this table shows the level of classifications accuracy for each class as well as the false classifications of the same class as well. The primary structure of the confusion matrix contains cells organised in two columns and two rows. These cells represent the results as the true positive, true negative, false positive and false negative as shown below.

Table 7.3: confusion matrix résulte components

| | Positive | Negative |
|---|---|---|
| True | True/Positive | True/ negative |
| False | False/Positive | False/Negative |

Table 7.4 the values of these cells are calculated as below

| | |
|---|---|
| True positive | TP= $\frac{Tp}{Tp+Fn}$ |
| True negative | TN= $\frac{Tn}{Tn+FP}$ |
| False negative | FN=$\frac{FN}{FN+TP}$ |
| False positive | FP= $\frac{FP}{FP+TP}$ |

Confusion matrix of SVM is shown in the table 7.5 below

Table 7.5 Confusion matrix

| 321 | Predicted: Normal | Predicted: Malicious |
|---|---|---|
| **Actual: Normal** | **207** | **3** |
| **Actual: Malicious** | **7** | **104** |

### 7.7.3 Comparison of Algorithms

It was also decided to compare the performance of the performance of SVM with SimpleLogistic and Multilayer Perceptron classifiers. Simple Logistic is used for building linear logistic regression models and MultilayerPerceptron uses backpropagation to learn a multi-layer perceptron to classify instances. All of these three algorithms have 96% accuracy. This could be due to fact that data set contains no missing value and class labelling is done by participants. The table 7.6 and table7.7 shows the detail of class accuracy of the SimpleLogistic and MultilayerPerceptron algorithm.

Table 7.6: **Class Accuracy of SimpleLogistic**

| Class | TPR | FPR | Precision | Recall | F-Measure | ROC Area | PRC Area |
|---|---|---|---|---|---|---|---|
| Normal | 0.98 | 0.06 | 0.96 | 0.98 | 0.97 | 0.93 | 0.93 |
| Malicious | 0.93 | 0.014 | 0.97 | 0.93 | 0.95 | 0.93 | 0.90 |

**Table 7.7: C5lass Accuracy of MultilayerPerceptron**

| Class | TPR | FPR | Precision | Recall | F-Measure | ROC Area | PRC Area |
|---|---|---|---|---|---|---|---|
| Normal | 0.98 | 0.06 | 0.96 | 0.98 | 0.97 | 0.98 | 0.98 |
| Malicious | 0.93 | 0.014 | 0.97 | 0.93 | 0.94 | 0.98 | 0.97 |

### 7.7.3.1 Receiver Operating Characteristic Curve

Knowledge flow was constructed to get receiver operating characteristic (ROC) curve. KnowledgeFlow environment provided by Weka, and it allows data and classification models flow through a diagram. KnowledgeFlow enables users to select various components from tool bar and place them on canvas and connect and configure them to create a knowledge flow for processing of data and its analysis. Figure 7.1 show the knowledge flow diagram.

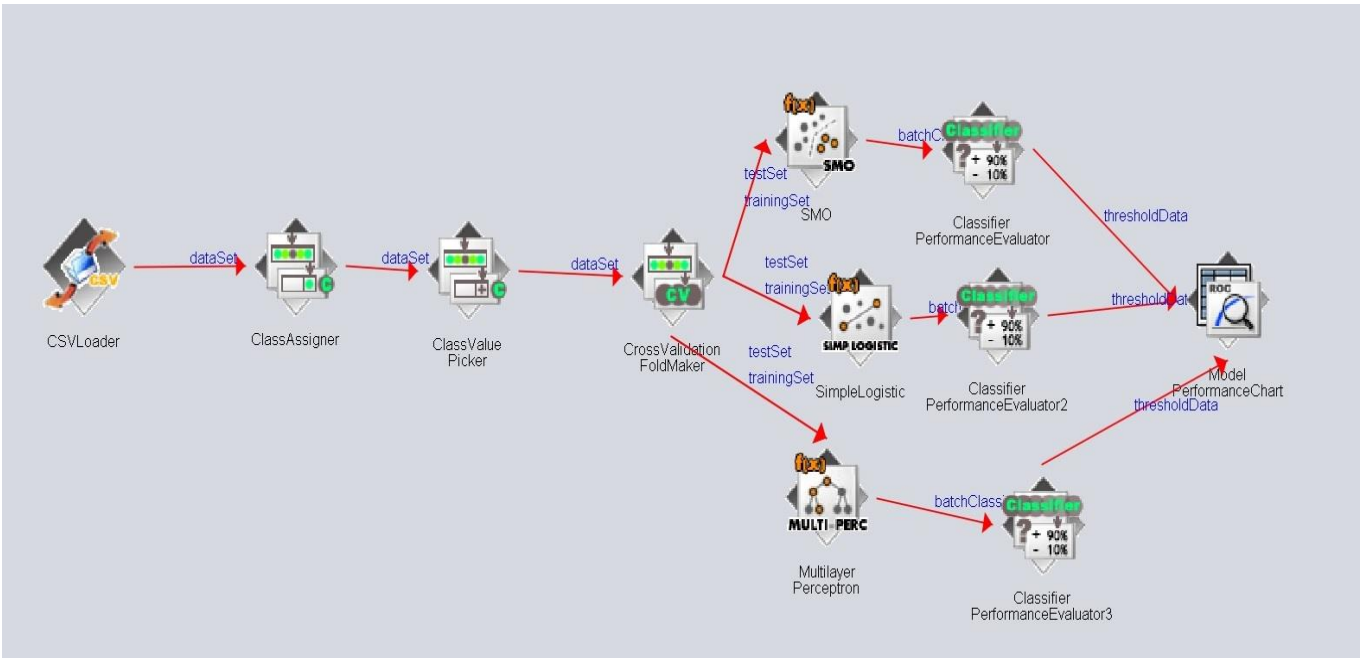



Figure 7.1: Knowledge Flow Diagram

The figure 7.1 includes classifiers; SMO, SimpleLogistic and MultilayerPerceptron. Evaluation of these classifier has been carried out using 10-fold cross-validation technique. Multiple ROC curves were obtained by running the knowledge flow diagram and these ROC curves are shown in Figure 7.2

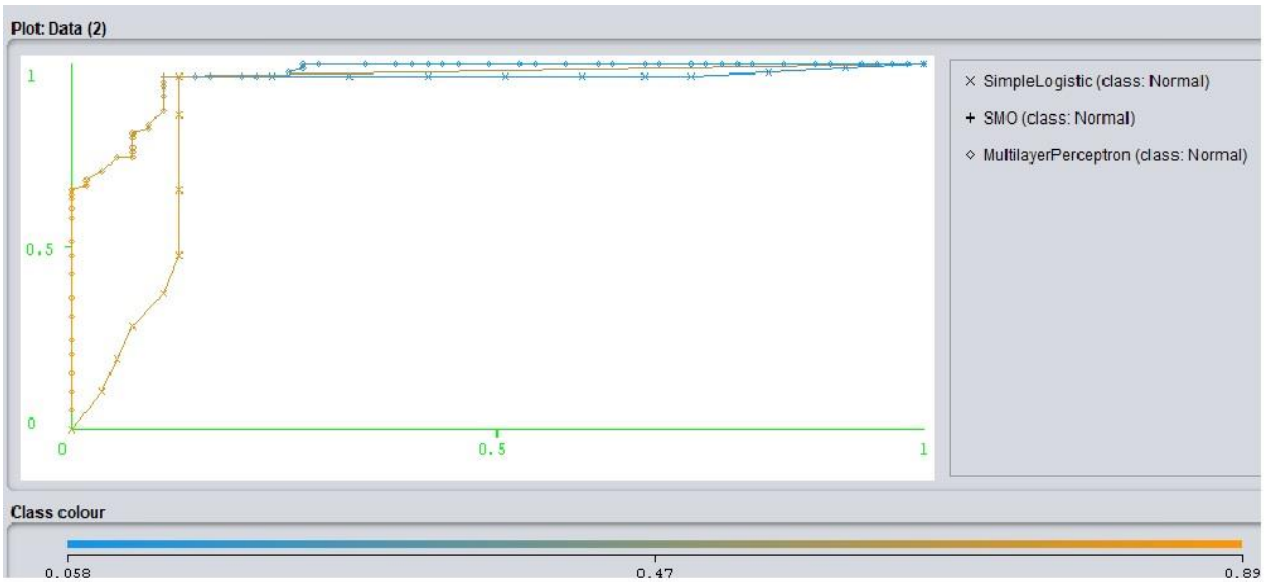



Figure 7.2: ROC Curves

### Notification Generation

The notification generation was carried out by notification component once an instance is classified as abnormal. In order to test notification component malicious and normal instances were created using Weka API and Java environment and results of classification were sent to notification generation components. All notifications were sent to administrator. Currently notifications convey information in textual format, but these remedial actions/plans could be implemented in real world environment to deal with abnormal events without human intervention.

## 7.8 Conclusion:

The evaluation of framework focus both on participant's evaluation and development of the prototype.

The participants' evaluation showed that the proposed BYOD risk management framework could be employed for efficient detection of risks. The participants also acknowledged that the proposed framework provided ideal ability for auditing. The evaluation process was conducted online due to the need to isolate the evaluators because of the COVID-19 Coronavirus outbreak. A briefing session was given to the evaluators, giving opportunity for discussion if required. The evaluators were provided with a checklist containing 12 questions which covers the following parameters: risk sources, framework flow, user privacy/ethics, classifications, risk accountability, risk audit and risk performance.

The result of the evaluation proved effectiveness of the use of MDM log and function event-logs in the BYOD risk management framework for detecting and predicting risks and the ability of the framework to maintain user privacy and ethics considerations.

Also, porotype system was developed for the framework evaluation and application of SVM has shown the accuracy of 96%. SimpleLogistic and MultilayerPerceptron algorithms were also used in comparison with SVM and both SimpleLogistic and MultilayerPerceptron have also shown accuracy of 96%.

The next chapter will present the research conclusions and recommendations for future work

# Chapter 8: Conclusions and future work

## 8.1 Introduction

The chapter conclude the research and highlights the future research directions. The thesis contributions and summary are given in section 8.2, the limitations of the research in 8.3, future directions and recommendations in 8.4, and the reflections of the researcher in 8.5.

## 8.2 Thesis Contributions and Summary

This research focuses on Bring Your Own Device (BYOD) security threats and risk management for Omani organisations. Oman is moving towards "Smart City" infrastructure. The Smart City initiative started in the city of Al Duqum in 2018, and it will move to other cities such as Sohar in 2022 and Matrah in 2025 as part of the Oman Vision 2040. BYOD is at the heart of the Oman 2040 vision in relation to smart cities and location independent working. Survey of different Omani organisation was carried out in order to understand the problem from these organisations point of view. Our research attempts to make a contribution to BYOD risk management. The BYOD risk-management framework has been proposed focusing on the risks associated with using personal devices on company networks. The goal of the proposed framework is to enable Omani organisations to address the security and privacy issues of the BYOD environment and provide increase level of trust in using BOYD devices. The challenges that exist in the existing BYOD environment and the limitation of the existing frameworks have been highlighted and this research attempts to address these with the proposed framework. The main gaps identified by the secondary and primary research were personal security to protect user devices and the data, together with data leakage which causes business data stored in personal devices to be exposed to unauthorised persons. Detecting the risks from BYOD devices was considered a challenge in BYOD environment. Further challenges and risks have been discussed in literature review chapter 3 and analysis chapter in chapter 5.

The contribution of the research is integrating different event logs and using machine learning to t classify detected events as normal or malicious. This goal was achieved using the MDM and functions log used as the dataset for SVM algorithms to generate the predictions.

Evaluation was carried out by involving participants from Omani organisations and developing a prototype. The evaluation showed that the proposed BYOD risk-management framework was efficient in detecting and predicting risks. The evaluation process was conducted online due to the need to isolate the evaluators because of the COVID-19 Coronavirus outbreak. A briefing session was given to the evaluators, giving opportunity for discussion of required. The evaluators were provided with a checklist containing 12 questions which covered the following parameters: risk sources, framework flow, user privacy/ethics, classifications, risk accountability, risk audit and risk performance.

The evaluators approved the use of MDM and function event-logs in the BYOD risk-management framework for detecting and predicting risks and the ability of the framework to maintain user privacy and ethics considerations. The prototype evaluation has shown that model is 96% accurate in predicting malicious events.

## 8.3 Limitations

This section is about highlighting the limitations of the proposed framework which should be considered when assessing the findings of this research. They include the following:

MDM itself can perform different management and security services but still needs multi-layered security support. These layers would consist of firewalls, IPS, access-list and IDS. MDM can provide user-profile management and application restrictions, but comprehensive traffic filtering requires other countermeasures. The proposed framework does not take into account firewalls IDS or other network related concerns.

The constant changing of threats in the BYOD environment has limited the functionality of proposed solutions. Even while evaluating the output of this work, improvements integrating Artificial Intelligent (AI) in smart devices have been introduced. This will bring other challenges managing access control and security accountability in the future for organisations adopting BYOD.

Currently offline data is used for the prototype development. There could be performance issues/response time issue in real-time environment.

## 8.4. Future Direction and Recommendation

The proposed risk-management framework has the ability to predict and identify security risks and generate suitable mitigation and prevention notifications. The novelty of the proposed framework is to make timely decisions and generate an effective action plan based on the classifier output and the current security policies for risk management in organisations. The action plan will either mitigate or avoid the risk.

It is desirable to integrating the framework with online traffic provides scope for improvement because currently it is functioning offline.

The researchers should take care regarding the improvement of integrating artificial intelligence (AI) in smart devices as mentioned above. This will keep bringing challenges in managing the access control and security accountability for the organisations adopting BYOD.

The proposed framework was only tested with a limited amount of data. As data become bigger and more extensive, including various data types generated from smart devices which contain IoT connections. It will bring new challenges of performance and accuracy. A more effective and automated remedial/mitigation component could be implemented that should take into account root cause of the abnormal event and organisational policy concerning security and privacy. Blockchain technology could be explored when non-repudiation is an important concern in BOYD environment.

## 8.5 Researcher Reflection

I started my PhD journey derived from my passion for starting and continuing my education. Moreover, the research topic was already investigated in 2012/2013 when I was doing my masters degree. Then I published a research paper in the IEEE conference in Malaysia which was

subsequently cited in 29 publications. The paper was about implementing BYOD solutions. (The passions to improve BYOD's security and privacy was with me, so when I started my PhD in 2015, I followed what was interesting to me and chose that as my topic.

The PhD journey was completely different from the taught courses. Each phase of the PhD acted as a separate study and a new learning phase. The most challenge phase was to come up with a credible framework for security and privacy of the BOYD environment.

To deeply understand the MDM functionality, I joined a MobileEngin workshop in London in 2018, where MDM opportunity and challenges were discussed by the industry experts and group discussions were taken place.

During my PhD journey I have make research papers contributions in reputable international conferences and my contributions were published in 2019 and 2020 got a high level of interaction with other researchers and there were more than 360 downloads and many citations for these papers. This proves the increased focus of the researcher in BYOD domain and the impact of the proposed solutions. List of publication is provided in this thesis

# References


1. Agudelo, C. A., Bosua, R., Ahmad, A., and Maynard, S. B. (2016) 'Mitigating Knowledge Leakage Risk in Organizations through Mobile Devices: A Contextual Approach'
2. Agudelo, C. A., Bosua, R., Ahmad, A., and Maynard, S. B. (2016) 'Understanding Knowledge Leakage & BYOD (Bring Your Own Device): A Mobile Worker Perspective'. *ArXiv Preprint arXiv:1606.01450*
3. Agudelo, C. A., Bosua, R., Ahmad, A., and Maynard, S. B. (2016) 'Understanding Knowledge Leakage & BYOD (Bring Your Own Device): A Mobile Worker Perspective'. *ArXiv Preprint arXiv:1606.01450*
4. Akujuobi, C., Ampah, N., and Sadiku, M. N. (eds.) (2007) *Consumer Electronics, 2007. ISCE 2007. IEEE International Symposium on*. 'Application of Wavelets and Self-Similarity to Enterprise Network Intrusion Detection and Prevention Systems': IEEE
5. Aldini, A., Seigneur, J., Ballester Lafuente, C., Titi, X., and Guislain, J. (2017) 'Design and Validation of a Trust-Based Opportunity-Enabled Risk Management System'. *Information & Computer Security* 25 (1), 2-25
6. Al-Janabi, M., Quincey, E. d., and Andras, P. (eds.) (2017) *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*. 'Using Supervised Machine Learning Algorithms to Detect Suspicious URLs in Online Social Networks': ACM
7. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., and Shamshirband, S. (2017) 'Survey of Main Challenges (Security and Privacy) in Wireless Body Area Networks for Healthcare Applications'. *Egyptian Informatics Journal* 18 (2), 113-122
8. Andrea, I., Chrysostomou, C., and Hadjichristofi, G. (eds.) (2015) *2015 IEEE Symposium on Computers and Communication (ISCC)*. 'Internet of Things: Security Vulnerabilities and Challenges': IEEE
9. Anwar, Z., Bibi, N., and Afzal, H. (eds.) (2019) *2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*. 'Mining Mobile Security Concerns and their Solutions': IEEE
10. Armando, A., Costa, G., Verderame, L., and Merlo, A. (2014) 'Securing the" Bring Your Own Device" Paradigm'. *Computer* 47 (6), 48-56
11. Armstrong, C. J. (ed.) (2009) *IFIP World Conference on Information Security Education*. 'An Approach to Visualising Information Security Knowledge': Springer

12. Arthur, J. 'Fighting Information Risk and Security'. *IS Practices for SME Success Series*, 15
13. Assing, D. and Calé, S. (2013) *Mobile Access Safety: Beyond BYOD.*: John Wiley & Sons
14. Atallah, È., Bonnefoi, P., Burgod, C., and Sauveron, D. (eds.) (2006) *Proceedings of the Seventh Edition of e-Smart Conference, Nice, France (September 2006)*. 'Mobile Ad Hoc Network with Embedded Secure System'
15. Balachandran, A., Voelker, G. M., and Bahl, P. (2005) 'Wireless Hotspots: Current Challenges and Future Directions'. *Mobile Networks and Applications* 10 (3), 265-274
16. Barreno, M., Nelson, B., Joseph, A. D., and Tygar, J. D. (2010) 'The Security of Machine Learning'. *Machine Learning* 81 (2), 121-148
17. Bartens, Y., De Haes, S., Lamoen, Y., Schulte, F., and Voss, S. (eds.) (2015) *System Sciences (HICSS), 2015 48th Hawaii International Conference on*. 'On the Way to a Minimum Baseline in IT Governance: Using Expert Views for Selective Implementation of COBIT 5': IEEE
18. Bell, M. (2013) 'Considerations when Implementing a BYOD Strategy'. *IS Practices for SME Success Series* 1 (1)
19. Bello, A. G., Murray, D., and Armarego, J. (2017) 'A Systematic Approach to Investigating how Information Security and Privacy can be Achieved in BYOD Environments'. *Information & Computer Security* 25 (4), 475-492
20. Birchall, A. (2014) 'Caught in the Web'. *Management Today* (Jul 2014), 34
21. Blum, A. L. and Langley, P. (1997) 'Selection of Relevant Features and Examples in Machine Learning'. *Artificial Intelligence* 97 (1-2), 245-271
22. Boadi, P. M., Zhou, S., and Kagalidis, I. (eds.) (2018) *International Conferences on WWW/Internet, ICWI 2018 and Applied Computing 2018*. 'Towards a Novel Byod Vulnerability Metrics Taxonomy for Organisations': IADIS Press
23. Boehmer, W. (ed.) (2009) | *2009 International Conference on Availability, Reliability and Security*. 'Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001': IEEE
24. Bohn, H., Bobek, A., and Golatowski, F. (eds.) (2006) *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on*. 'SIRENA-Service Infrastructure for Real-Time Embedded Networked Devices: A Service Oriented Framework for Different Domains': IEEE
25. Brand, J. C., Renen, K., and Rudman, R. (2015) 'Proposed Practices to Mitigate Significant Mobility Security Risks'

26. Breier, J. and Branišová, J. (2017) 'A Dynamic Rule Creation Based Anomaly Detection Method for Identifying Security Breaches in Log Records'. *Wireless Personal Communications* 94 (3), 497-511
27. Brown, W. and Nasuti, F. (2005) 'What ERP Systems can Tell Us about Sarbanes-Oxley'. *Information Management & Computer Security* 13 (4), 311-327
28. Caldwell, C., Zeltmann, S., and Griffin, K. (eds.) (2012) *Competition Forum*. 'BYOD (Bring Your Own Device)': American Society for Competitiveness
29. Campbell, P. L. (2005) *A CobiT Primer*.: United States. Department of Energy
30. Campbell, P. L. (2005). *A Cobit Primer.*
31. Carter, E. and Hogue, J. (2006) *Intrusion Prevention Fundamentals*.: Pearson Education India
32. Chapelle, O., Scholkopf, B., and Zien, A. (2009) 'Semi-Supervised Learning'. *EEE Transactions on Neural Networks* 20 (1), 542-542.
33. Chen, H., Li, J., Hoang, T., and Lou, X. (2013) 'Security Challenges of BYOD: A Security Education, Training and Awareness Perspective'
34. Chen, Y., You, W., Lee, Y., Chen, K., Wang, X., and Zou, W. (eds.) (2017) *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 'Mass Discovery of Android Traffic Imprints through Instantiated Partial Execution': ACM
35. Chu, X., Ouyang, W., Li, H., and Wang, X. (eds.) (2016) *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 'Structured Feature Learning for Pose Estimation'
36. Conti, M. and Giordano, S. (2014) 'Mobile Ad Hoc Networking: Milestones, Challenges, and New Research Directions'. *IEEE Communications Magazine* 52 (1), 85-96
37. Cramer, D. (2003) *Advanced Quantitative Data Analysis*.: McGraw-Hill Education (UK)
38. Creswell, J. W. and Poth, C. N. (2017) *Qualitative Inquiry and Research Design: Choosing among Five Approaches*.: Sage publications
39. Dahbur, K., Mohammad, B., and Tarakji, A. B. (eds.) (2011) *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications*. 'A Survey of Risks, Threats and Vulnerabilities in Cloud Computing'
40. Dalvi, N., Domingos, P., Sanghai, S., and Verma, D. (eds.) (2004) *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. 'Adversarial Classification': ACM
41. Dannewitz, C., Kutscher, D., Ohlman, B., Farrell, S., Ahlgren, B., and Karl, H. (2013) 'Network of Information (Netinf)–an Information-Centric Networking Architecture'. *Computer Communications* 36 (7), 721-735

42. De, A. K., Garg, S., Singhal, D. K., Malik, H., Mukherjee, A., Jena, M. K., Kumar, S., Kaushik, J. K., Mohanty, A. K., and Das, B. C. (2013) 'Derivation of Goat Embryonic Stem Cell-Like Cell Lines from in Vitro Produced Parthenogenetic Blastocysts'. *Small Ruminant Research* 113 (1), 145-153
43. Demontis, A., Melis, M., Biggio, B., Maiorca, D., Arp, D., Rieck, K., Corona, I., Giacinto, G., and Roli, F. (2017) 'Yes, Machine Learning can be More Secure! a Case Study on Android Malware Detection'. *IEEE Transactions on Dependable and Secure Computing*
44. Devos, J. and Van de Ginste, K. (eds.) (2014) *Proc. 8th European Conference on IS Management and Evaluation, Ghent*. 'A Quest for Theoretical Foundations of COBIT 5'
45. Dhingra, M. (2016) 'Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)'. *Procedia Computer Science* 78, 179-184
46. Dhingra, M. (2016) *Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)* [online]. available from <http://www.sciencedirect.com/science/article/pii/S1877050916000326>
47. Do, H. H. and Rahm, E. (2000) 'On Metadata Interoperability in Data Warehouses'. *Technischer Report*, 1-2000
48. Doargajudhur, M. S. and Dell, P. (2019) 'Impact of BYOD on Organizational Commitment: An Empirical Investigation'. *Information Technology & People*
49. Downer, K. and Bhattacharya, M. (eds.) (2015) *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*. 'BYOD Security: A New Business Challenge': IEEE
50. Driscoll, D. L. (2011) 'Introduction to Primary Research: Observations, Surveys, and Interviews'. *Writing Spaces: Readings on Writing* 2, 153-174
51. Earley, S., Harmon, R., Lee, M. R., and Mithas, S. (2014) 'From BYOD to BYOA, Phishing, and Botnets'. *IT Professional* (5), 16-18
52. Ekelhart, A., Fenz, S., and Neubauer, T. (eds.) (2009) *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*. 'Aurum: A Framework for Information Security Risk Management': IEEE
53. Eslahi, M., Naseri, M. V., Hashim, H., Tahir, N., and Saad, E. H. M. (eds.) (2014) *Computer Applications and Industrial Electronics (ISCAIE), 2014 IEEE Symposium on*. 'BYOD: Current State and Security Challenges': IEEE
54. Eslahi, M., Salleh, R., and Anuar, N. B. (eds.) (2012) *2012 IEEE International Conference on Control System, Computing and Engineering*. 'Bots and Botnets: An Overview of Characteristics, Detection and Challenges': IEEE
55. Ezrahovich, A. Y., Vladimirtsev, A. V., Livshitz, I. I., Lontsikh, P. A., and Karaseva, V. A. (eds.) (2017) *" Quality Management, Transport and Information Security, Information*

*Technologies"(IT&QM&IS), 2017 International Conference*. 'Risk-Based Thinking of ISO 9001: 2015—The New Methods, Approaches and Tools of Risk Management': IEEE

56. Finkelstein, A., Biton, R., Puzis, R., and Shabtai, A. (2017) 'Classification of Smartphone Users using Internet Traffic'. *ArXiv Preprint arXiv:1701.00220*
57. Frias-Martinez, V., Stolfo, S. J., and Keromytis, A. D. (eds.) (2008) *Computer Security Applications Conference, 2008. ACSAC 2008. Annual*. 'Behavior-Profile Clustering for False Alert Reduction in Anomaly Detection Sensors': IEEE
58. Fussell, L. and Field, S. (eds.) (2005) *18th International Conference on Systems Engineering (ICSEng'05)*. 'The Role of the Risk Management Database in the Risk Management Process': IEEE
59. Ganiyu, S. O. and Jimoh, R. G. (2018) 'Characterising Risk Factors and Countermeasures for Risk Evaluation of Bring Your Own Device Strategy'. *International Journal of Information Security Science* 7 (1), 49-59
60. Garba, A. B., Armarego, J., and Murray, D. (2015) 'A Policy-Based Framework for Managing Information Security and Privacy Risks in BYOD Environments'. *International Journal of Emerging Trends & Technology in Computer Science* 4 (2), 189-198
61. Gas, B. (2010) 'Self-Organizing Multilayer Perceptron'. *IEEE Transactions on Neural Networks* 21 (11), 1766-1779
62. Ghosh, A., Gajar, P. K., and Rai, S. (2013) 'Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies'. *Journal of Global Research in Computer Science* 4 (4), 62-70
63. Goeschel, K. (ed.) (2016) *Southeastcon, 2016*. 'Reducing False Positives in Intrusion Detection Systems using Data-Mining Techniques Utilizing Support Vector Machines, Decision Trees, and Naive Bayes for Off-Line Analysis': IEEE
64. Gola, J., Webel, J., Britz, D., Guitar, A., Staudt, T., Winter, M., and Mücklich, F. (eds.) (2019). '2019. Objective Microstructure Classification by Support Vector Machine (SVM) using a Combination of Morphological Parameters and Textural Features for Low Carbon Steels'. held Computational Materials Science
65. Gupta, A., Anpalagan, A., Carvalho, G. H., Guan, L., and Woungang, I. (2019) 'Prevailing and Emerging Cyber Threats and Security Practices in IoT-Enabled Smart Grids: A Survey'. *Journal of Network and Computer Applications*
66. Haider, S. K., Jin, C., Ahmad, M., Shila, D., Khan, O., and van Dijk, M. (2017) 'Advancing the State-of-the-Art in Hardware Trojans Detection'. *IEEE Transactions on Dependable and Secure Computing*
67. Hall, D. 'The Threat from Inside'. *IS Practices for SME Success Series*, 35

68. Harari, G. M., Müller, S. R., Aung, M. S., and Rentfrow, P. J. (2017) 'Smartphone Sensing Methods for Studying Behavior in Everyday Life'. *Current Opinion in Behavioral Sciences* 18, 83-90
69. Harris, M. A. and Patten, K. P. (2014) 'Mobile Device Security Considerations for Small-and Medium-Sized Enterprise Business Mobility'. *Information Management & Computer Security*
70. Haslum, K., Moe, M. E., and Knapskog, S. J. (eds.) (2008) *Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on*. 'Real-Time Intrusion Prevention and Security Analysis of Networks using HMMs': IEEE
71. He, X., Chomsiri, T., Nanda, P., and Tan, Z. (2014) 'Improving Cloud Network Security using the Tree-Rule Firewall'. *Future Generation Computer Systems* 30, 116-126
72. Hernandez, A. and Choi, Y. (2014) 'Securing BYOD Networks: Inherent Vulnerabilities and Emerging Feasible Technologies'
73. Herrera, A. V., Ron, M., and Rabadão, C. (eds.) (2017) *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*. 'National Cyber-Security Policies Oriented to BYOD (Bring Your Own Device): Systematic Review': IEEE
74. Hoo, K. J. S. (2000) *How Much is enough? A Risk Management Approach to Computer Security*.: Stanford University Stanford, Calif
75. Horvitz, E. and Mulligan, D. (2015) 'Policy Forum. Data, Privacy, and the Greater Good'. *Science (New York, N.Y.)* 349 (6245), 253-255
76. Hovav, A. and Putri, F. F. (2016) *This is My Device! Why should I Follow Your Rules? Employees' Compliance with BYOD Security Policy* [online]. available from <http://www.sciencedirect.com/science/article/pii/S1574119216300724>
77. Howard, F. (2008) 'Modern Web Attacks'. *Network Security* 2008 (4), 13-15
78. Huang, Z., Zavarsky, P., and Ruhl, R. (eds.) (2009) *2009 International Conference on Computational Science and Engineering*. 'An Efficient Framework for IT Controls of Bill 198 (Canada Sarbanes-Oxley) Compliance by Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002': IEEE
79. Ingrams, A. (2015) 'Mobile Phones, Smartphones, and the Transformation of Civic Behavior through Mobile Information and Connectivity'. *Government Information Quarterly* 32 (4), 506-515
80. Ismail, K. A., Singh, M. M., Mustaffa, N., Keikhosrokiani, P., and Zulkefli, Z. (2017) 'Security Strategies for Hindering Watering Hole Cyber Crime Attack'. *Procedia Computer Science* 124, 656-663
81. Jain, A. K. and Shanbhag, D. (2012) 'Addressing Security and Privacy Risks in Mobile Applications.'. *IT Professional* 14 (5), 28-33

82. Jakhale, A. (ed.) (2017) *Computational Intelligence in Data Science (ICCIDS), 2017 International Conference on*. 'Design of Anomaly Packet Detection Framework by Data Mining Algorithm for Network Flow': IEEE
83. Jans, M., Lybaert, N., and Vanhoof, K. (2010) 'A Framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: The IFR² Framework'
84. Jennex, M. and Durcikova, A. (eds.) (2014) *System Sciences (HICSS), 2014 47th Hawaii International Conference on*. 'Integrating IS Security with Knowledge Management: Are we Doing enough to Thwart the Persistent Threat?': IEEE
85. Jones, J. (2012) 'Beginner's Guide to BYOD (Bring Your Own Device)'. *Retrieved February* 9, 2014
86. Jordan, M. I. and Mitchell, T. M. (2015) 'Machine Learning: Trends, Perspectives, and Prospects'. *Science (New York, N.Y.)* 349 (6245), 255-260
87. Kaur, R. (2014) 'Control Issues and Mobile Devices'
88. Kellner, A., Horlboge, M., Rieck, K., and Wressnegger, C. (eds.) (2019) *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. 'False Sense of Security: A Study on the Effectivity of Jailbreak Detection in Banking Apps': IEEE
89. Ko, R. and Choo, R. (2015) *The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues*.: Syngress
90. Kołcz, A. and Teo, C. H. (eds.) (2009) *CEAS'09: Sixth Conference on Email and Anti-Spam*. 'Feature Weighting for Improved Classifier Robustness'
91. Krombholz, K., Hobel, H., Huber, M., and Weippl, E. (eds.) (2013) *Proceedings of the 6th International Conference on Security of Information and Networks*. 'Social Engineering Attacks on the Knowledge Worker': ACM
92. Lalanne, V., Munier, M., and Gabillon, A. (eds.) (2013) *Social Computing (SocialCom), 2013 International Conference on*. 'Information Security Risk Management in a World of Services': IEEE
93. Larrocha, E. R., Minguet, J. M., Díaz, G., Castro, M., and Vara, A. (eds.) (2010) *Education Engineering (EDUCON), 2010 IEEE*. 'Filling the Gap of Information Security Management Inside ITIL®: Proposals for Posgraduate Students': IEEE
94. Layland, R., Wexler, J., Datoo, A., George, A., Rege, O., Marshall, J., Herrema, J., and Duckering, B. (2012). *The 2011 Mobile Device Management challenge—defusing Mobile Anarchy in the Enterprise.Network World and Robin Layland Present*
95. Leavitt, N. (2013) 'Today'. *Computer* (11), 16-19

96. Lee, J., Park, S., and Yoon, H. (eds.) (2015) *2015 Second International Conference on Computing Technology and Information Management (ICCTIM)*. 'Security Policy Based Device Management for Supporting various Mobile Os': IEEE
97. Liu, X., Qian, F., and Qian, Z. (eds.) (2017) *Network Protocols (ICNP), 2017 IEEE 25th International Conference on*. 'Selective HTTPS Traffic Manipulation at Middleboxes for BYOD Devices': IEEE
98. Lounsbury, J. (2013) 'Application Security: From Web to Mobile. Different Vectors and New Attacks'. *Security in Knowledge*, 2-30
99. Lowd, D. and Meek, C. (eds.) (2005) *Proceedings of the Eleventh ACM SIGKDD International Conference on Knowledge Discovery in Data Mining*. 'Adversarial Learning': ACM
100. Madani, H., Siddiqui, S., Azizullah, F., and Ashraf, A. (2014). *Method and Apparatus for Dynamic Tunneling*
101. Madzima, K., Moyo, M., and Abdullah, H. (eds.) (2014) *2014 Information Security for South Africa*. 'Is Bring Your Own Device an Institutional Information Security Risk for Small-Scale Business Organisations?': IEEE
102. Magruder, J. S., Lewis, S. X., Burks, E. J., and Smolinski, C. (2015) 'Bring Your Own Device (BYOD)--Who is Running Organizations?'. *Journal of Accounting & Finance (2158-3625)* 15 (1)
103. Manikandan, S. and Manimegalai, R. (2012) 'Survey on Mobile Ad Hoc Network Attacks and Mitigation using Routing Protocols'. *American Journal of Applied Sciences* 9 (11), 1796
104. Mansfield-Devine, S. (2012) *Interview: BYOD and the Enterprise Network* [online]. available from <http://www.sciencedirect.com/science/article/pii/S1361372312700313>
105. Matos, A., Romao, D., and Trezentos, P. (eds.) (2012) *Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on*. 'Secure Hotspot Authentication through a Near Field Communication Side-Channel': IEEE
106. Matulevicius, R., Mayer, N., and Heymans, P. (eds.) (2008) *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*. 'Alignment of Misuse Cases with Security Risk Management': IEEE
107. Mavroforakis, M. E. and Theodoridis, S. (2006) 'A Geometric Approach to Support Vector Machine (SVM) Classification'. *IEEE Transactions on Neural Networks* 17 (3), 671-682
108. Mitchell, R. and Chen, I. (2013) 'Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems'. *IEEE Transactions on Reliability* 62 (1), 199-210

109. Moin, A. H. and Khansari, M. (eds.) (2010) *IFIP International Conference on Open-Source Systems*. 'Bug Localization using Revision Log Analysis and Open Bug Repository Text Categorization': Springer
110. Montes de Oca, M., Lopez Varela, M. V., Laucho-Contreras, M. E., Casas, A., Schiavi, E., Rey, A., Silva, A., and en nombre del equipo del estudio PUMA (2017) 'Classification of Patients with Chronic Obstructive Pulmonary Disease According to the Latin American Thoracic Association (ALAT) Staging Systems and the Global Initiative for Chronic Obstructive Pulmonary Disease (GOLD)'. *Archivos De Bronconeumologia* 53 (3), 98-106
111. MOROLONG, M., GAMUNDANI, A., and SHAVA, F. B. (eds.) (2019) *2019 IST-Africa Week Conference (IST-Africa)*. 'Review of Sensitive Data Leakage through Android Applications in a Bring Your Own Device (BYOD) Workplace': IEEE
112. Morrow, B. (2012) 'BYOD Security Challenges: Control and Protect Your most Sensitive Data'. *Network Security* 2012 (12), 5-8
113. Nagamalla, V. and Varanasi, A. (eds.) (2017) *Information Communication and Embedded Systems (ICICES), 2017 International Conference on*. 'A Review of Security Frameworks for Internet of Things': IEEE
114. Nam, T. and Pardo, T. A. (eds.) (2011) *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times*. 'Conceptualizing Smart City with Dimensions of Technology, People, and Institutions'
115. Nguyen, H. D., McLachlan, G. J., and Wood, I. A. (2016) 'Mixtures of Spatial Spline Regressions for Clustering and Classification'. *Computational Statistics & Data Analysis* 93, 76-85
116. Nickel, M., Murphy, K., Tresp, V., and Gabrilovich, E. (2016) 'A Review of Relational Machine Learning for Knowledge Graphs'. *Proceedings of the IEEE* 104 (1), 11-33
117. Oktavia, T., Tjong, Y., and Prabowo, H. (eds.) (2016) *2016 International Conference on Information Management and Technology (ICIMTech)*. 'Security and Privacy Challenge in Bring Your Own Device Environment: A Systematic Literature Review': IEEE
118. Ortbach, K., Brockmann, T., and Stieglitz, S. (2014) 'Drivers for the Adoption of Mobile Device Management in Organizations'
119. Palanisamy, R., Norman, A. A., and Mat Kiah, M. L. (2020) 'BYOD Policy Compliance: Risks and Strategies in Organizations'. *Journal of Computer Information Systems*, 1-12
120. Park, K. and Lee, H. (eds.) (2001) *ACM SIGCOMM Computer Communication Review*. 'On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets': ACM

121. Patel, A., Taghavi, M., Bakhtiyari, K., and JúNior, J. C. (2013) 'An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review'. *Journal of Network and Computer Applications* 36 (1), 25-41
122. Pell, L. (2013) 'BYOD Implementing the Right Policy'. *University of Derby, UK*, 95-98
123. Petrov, D. and Znati, T. (eds.) (2018) *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*. 'Context-Aware Deep Learning-Driven Framework for Mitigation of Security Risks in BYOD-Enabled Environments': IEEE
124. Pozza, G. (2014) 'Beyond BYOD: Can I Connect My Body to Your Network'
125. Radovanović, D., Radojević, T., Lučić, D., and Šarac, M. (eds.) (2010) *MIPRO, 2010 Proceedings of the 33rd International Convention*. 'IT Audit in Accordance with Cobit Standard': IEEE
126. Rahm, E. and Do, H. H. (2000) 'Data Cleaning: Problems and Current Approaches'. *IEEE Data Eng.Bull.* 23 (4), 3-13
127. Ratchford, M., Wang, P., and Sbeit, R. O. (2018) 'BYOD Security Risks and Mitigations'. in *Information Technology-New Generations*. ed. by Anon: Springer, 193-197
128. Ratchford, M. M. and Wang, Y. (eds.) (2019) *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*. 'BYOD-Insure: A Security Assessment Model for Enterprise BYOD': IEEE
129. Retnowardhani, A., Diputra, R. H., and Triana, Y. S. (2019) 'Security Risk Analysis of Bring Your Own Device (BYOD) System in Manufacturing Company at Tangerang'. *Telkomnika* 17 (2), 753-762
130. Rhodes, C. and Bettany, A. (2016) 'Managing Windows Updates with Intune'. in *Windows Installation and Update Troubleshooting*. ed. by Anon: Springer, 167-184
131. Rhodes, K. L. and Kunis, B. (2011) 'Walking the Wire in the Wireless World: Legal and Policy Implications of Mobile Computing'. *J.Tech.L.& Pol'y* 16, 25
132. Rhodes, K. and Kunis, B. (2011).
133. Rhodes-Ousley, M. (2013) *Information Security: The Complete Reference*.: McGraw Hill Education
134. Rivera, S., Lagraa, S., Nita-Rotaru, C., Becker, S., and State, R. (eds.) (2019) *2019 IEEE Security and Privacy Workshops (SPW)*. 'Ros-Defender: Sdn-Based Security Policy Enforcement for Robotic Applications': IEEE
135. Roberts, L. G. and Wessler, B. D. (eds.) (1970) *Proceedings of the May 5-7, 1970, Spring Joint Computer Conference*. 'Computer Network Development to Achieve Resource Sharing': ACM
136. Romer, H. (2014) 'Best Practices for BYOD Security'. *Computer Fraud & Security* 2014 (1), 13-15

137. Saha, A. and Sanyal, S. (2015) 'Review of Considerations for Mobile Device Based Secure Access to Financial Services and Risk Handling Strategy for CIOs, CISOs and CTOs'. *ArXiv Preprint arXiv:1502.00724*
138. Sahd, L. and Rudman, R. J. (2017) 'Best Practices Mobile Technology Risk Assessment and Control Checklist'. *Southern African Journal of Accountability and Auditing Research* 19 (1), 129-145
139. Salle, M. and Rosenthal, S. (eds.) (2005) *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*. 'Formulating and Implementing an HP IT Program Strategy using CobiT and HP ITSM': IEEE
140. Samal, B., Behera, A. K., and Panda, M. (eds.) (2017) *Sensing, Signal Processing and Security (ICSSS), 2017 Third International Conference on*. 'Performance Analysis of Supervised Machine Learning Techniques for Sentiment Analysis': IEEE
141. Samaras, V., Daskapan, S., Ahmad, R., and Ray, S. K. (eds.) (2014) *Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian*. 'An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD': IEEE
142. Sathya, G. and Vasanthraj, K. (eds.) (2013) *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*. 'Network Activity Classification Schema in IDS and Log Audit for Cloud Computing': IEEE
143. Sato, Y., Fukuda, I., and Fujita, T. (2013) 'Deployment of OpenFlow/SDN Technologies to Carrier Services'. *IEICE Transactions on Communications* 96 (12), 2946-2952
144. Scarfo, A. (ed.) (2012) *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on*. 'New Security Perspectives Around BYOD': IEEE
145. Shakshuki, E. M., Kang, N., and Sheltami, T. R. (2013) 'EAACK—a Secure Intrusion-Detection System for MANETs'. *IEEE Transactions on Industrial Electronics* 60 (3), 1089-1098
146. Shi, S., Wang, Q., Xu, P., and Chu, X. (eds.) (2016) *2016 7th International Conference on Cloud Computing and Big Data (CCBD)*. 'Benchmarking State-of-the-Art Deep Learning Software Tools': IEEE
147. Shila, D. M., Shen, W., Cheng, Y., Tian, X., and Shen, X. S. (2017) 'AMCloud: Toward a Secure Autonomic Mobile Ad Hoc Cloud Computing System'. *IEEE Wireless Communications* 24 (2), 74-81
148. Shiomi, Y., Nishiuchi, H., and Yoshii, T. (2015) 'Mode Classification for Mixed Traffic Flow Based on Smartphone Data'. *Journal of the Eastern Asia Society for Transportation Studies* 11, 1970-1981

149. Siboni, S., Shabtai, A., and Elovici, Y. (2018) 'An Attack Scenario and Mitigation Mechanism for Enterprise BYOD Environments'. *ACM SIGAPP Applied Computing Review* 18 (2), 5-21
150. Singh, M. M., Chan, C. W., and Zulkefli, Z. (2017) 'Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm'. *International Journal of Advanced Computer Science and Applications* 8 (2), 53-62
151. Singh, N. (2012) 'BYOD Genie is Out of the bottle–"Devil Or Angel"'. *Journal of Business Management & Social Sciences Research* 1 (3), 1-12
152. Singhal, S. and Jena, M. (2013) 'A Study on WEKA Tool for Data Preprocessing, Classification and Clustering'. *International Journal of Innovative Technology and Exploring Engineering (IJItee)* 2 (6), 250-253
153. Sitnikova, E. and Asgarkhani, M. (eds.) (2014) *2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*. 'A Strategic Framework for Managing Internet Security': IEEE
154. Spoorthi, V. and Sekaran, K. C. (eds.) (2014) *Networks & Soft Computing (ICNSC), 2014 First International Conference on*. 'Mobile Single Sign-on Solution for Enterprise Cloud Applications': IEEE
155. Stiawan, D., Abdullah, A. H., and Idris, M. Y. (eds.) (2010) *Education Technology and Computer (ICETC), 2010 2nd International Conference on*. 'The Trends of Intrusion Prevention System Network': IEEE
156. Suchacka, G., Skolimowska-Kulig, M., and Potempa, A. (2015) 'Classification of E-Customer Sessions Based on Support Vector Machine.'. *Ecms* 15, 594-600
157. Sultana, A. and Jabbar, M. (eds.) (2016) *Applied and Theoretical Computing and Communication Technology (iCATccT), 2016 2nd International Conference on*. 'Intelligent Network Intrusion Detection System using Data Mining Techniques': IEEE
158. Susanto12, H., Almunawar, M. N., and Tuan, Y. C. (2011) 'Information Security Management System Standards: A Comparative Study of the Big Five'. *International Journal of Electrical Computer Sciences IJECSIJENS* 11 (5), 23-29
159. Tang, O. and Musa, S. N. (2011) 'Identifying Risk Issues and Research Advancements in Supply Chain Risk Management'. *International Journal of Production Economics* 133 (1), 25-34
160. Tanimoto, S., Yamada, S., Iwashita, M., Kobayashi, T., Sato, H., and Kanai, A. (eds.) (2016) *Consumer Electronics, 2016 IEEE 5th Global Conference on*. 'Risk Assessment of BYOD: Bring Your Own Device': IEEE

161. Tu, C. Z., Adkins, J., and Zhao, G. Y. (2019) 'Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory'. *Journal of the Midwest Association for Information Systems| Vol* 2019 (1), 11
162. Tuch, H., Laplace, C., Barr, K. C., and Wu, B. (eds.) (2012) *ACM SIGPLAN Notices*. 'Block Storage Virtualization with Commodity Secure Digital Cards': ACM
163. Tuttle, B. and Vandervelde, S. D. (2007) 'An Empirical Examination of CobiT as an Internal Control Framework for Information Technology'. *International Journal of Accounting Information Systems* 8 (4), 240-263
164. Utter, C. J. and Rea, A. (2015) 'The" Bring Your Own Device" Conundrum for Organizations and Investigators: An Examination of the Policy and Legal Concerns in Light of Investigatory Challenges'. *Journal of Digital Forensics, Security and Law* 10 (2), 4
165. Veljkovic, I. and Budree, A. (2019) 'Development of Bring-Your-Own-Device Risk Management Model: A Case Study from a South African Organisation'. *The Electronic Journal of Information Systems Evaluation* 22 (1), 1-14
166. Vignesh, U. and Asha, S. (2015) 'Modifying Security Policies Towards BYOD'. *Procedia Computer Science* 50, 511-516
167. Vignesh, U. and Asha, S. (2015) *Modifying Security Policies Towards BYOD* [online] . available from <http://www.sciencedirect.com/science/article/pii/S1877050915005244>
168. Von Solms, B. (2005) 'Information Security Governance: COBIT Or ISO 17799 Or both?'. *Computers & Security* 24 (2), 99-104
169. Wang, R. W. (2013) 'Mobile Devices and Control Issues' Wang, Y., Wei, J., and Vangury, K. (eds.) (2014) *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*. 'Bring Your Own Device Security Issues and Challenges': IEEE
170. Watson, B. and Zheng, J. (eds.) (2017) *Proceedings of the SouthEast Conference*. 'On the User Awareness of Mobile Security Recommendations': ACM
171. Weber, L. (2014) . *Addressing the Incremental Risks Associated with Adopting a Bring Your Own Device Program by using the COBIT 5 Framework to Identify Keycontrols*
172. Williams, G. P. (2012) 'Cost Effective Assessment of the Infrastructure Security Posture'
173. Yamin, M. M. and Katt, B. (eds.) (2019) *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*. 'Mobile Device Management (MDM) Technologies, Issues and Challenges'
174. Yang, T. A., Vlas, R., Yang, A., and Vlas, C. (eds.) (2013) *2013 International Conference on Social Computing*. 'Risk Management in the Era of Byod: The Quintet of Technology Adoption, Controls, Liabilities, User Perception, and User Behavior': IEEE

175. Zefferer, T. and Teufl, P. (eds.) (2013) *2013 International Conference on Security and Cryptography (SECRYPT)*. 'Policy-Based Security Assessment of Mobile End-User Devices an Alternative to Mobile Device Management Solutions for Android Smartphones': IEEE
176. Zulkefli, Z., Singh, M. M., and Malim, Nurul Hashimah Ahamed Hassain (eds.) (2015) *International Conference on Computational Science and its Applications*. 'Advanced Persistent Threat Mitigation using Multi Level Security–Access Control Framework': Springer
177. Oktavia, T. and Prabowo, H., 2016, November. Security and privacy challenge in Bring Your Own Device environment: A Systematic Literature Review. In *2016 International Conference on Information Management and Technology (ICIMTech)* (pp. 194-199). IEEE.
178. Akande, A.O. and Tran, V.N., 2021. Predicting Security Program Effectiveness in Bring-Your-Own-Device Deployment in Organizations.
179. Rivera, D., George, G., Peter, P., Muralidharan, S. and Khanum, S., 2013. Analysis of security controls for BYOD (bring your own device). minerva-access.unimelb.edu.au
180. Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X., 2021. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, p.102248.
181. Zahadat, N., Blessner, P., Blackburn, T. and Olson, B.A., 2015. BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, pp.81-99.
182. Marilyn, L., Odendahl & Indiana, 2014. *'Bring your own device' creates privacy issues for employees.* [Online]
Available at: http://www.ibj.com/articles/49128-bring-your-own-device-creates-privacy-issues-for-employees
[Accessed 1 12 2015].
183. Vinh, T.L., Cagnon, H., Bouzefrane, S. and Banerjee, S., 2020. Property-based token attestation in mobile computing. *Concurrency and Computation: Practice and Experience*, *32*(1), p.e4350.
184. Gudo, M. and Padayachee, K., 2015, September. SpotMal: A hybrid malware detection framework with privacy protection for BYOD. In *Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists* (pp. 1-6).
185. Muhammad, M.A., Ayesh, A. and Wagner, I., 2019, July. Behavior-Based Outlier Detection for Network Access Control Systems. In *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems* (pp. 1-6).
186. Scarfò, A., 2013, March. All silicon data center, the energy perspectives. In *2013 27th International Conference on Advanced Information Networking and Applications Workshops* (pp. 1617-1622). IEEE.

187. Matulevičius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P. and Genon, N., 2008, June. Adapting secure tropos for security risk management in the early phases of information systems development. In *International Conference on Advanced Information Systems Engineering* (pp. 541-555). Springer, Berlin, Heidelberg.
188. Marchand, C., Aubert, A. and Bossuet, L., 2017, September. On the security evaluation of the ARM TrustZone extension in a heterogeneous SoC. In *2017 30th IEEE International System-on-Chip Conference (SOCC)* (pp. 108-113). IEEE.
189. Raj, U. and Catherine, M.S., 2015. Certificate based hybrid authentication for bring your own device (BYOD) in Wi-Fi enabled environment. *International Journal of Computer Science and Information Security*, *13*(12), p.41.
190. Pradip Kumar Sharma, Jong Hyuk Park, 2018 Blockchain based hybrid network architecture for the smart city, Future Generation Computer Systems,Volume 86, ,Pages 650-655, ISSN 0167-739X,
191. Sengan, S., Subramaniyaswamy, V., Nair, S.K., Indragandhi, V., Manikandan, J. and Ravi, L., 2020. Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. *Future generation computer systems*, *112*, pp.724-737.
192. Elbasiony, R.M., Sallam, E.A., Eltobely, T.E. and Fahmy, M.M., 2013. A hybrid network intrusion detection framework based on random forests and weighted k-means. *Ain Shams Engineering Journal*, *4*(4), pp.753-762.
193. Martin, V., Cao, Q., Benson, T. (2017). Fending off IoT-hunting attacks at home networks. CAN 2017 - Proceedings © 2021 JDFSL Page 15 JDFSL 2021 of the 2017 Cloud-Assisted Networking Workshop, Part of CoNext 2017. https://doi.org/10.1145/3155921.3160640
194. Asante, A. and Amankona, V., 2021. DIGITAL FORENSIC READINESS FRAMEWORK BASED ON HONEYPOT AND HONEYNET FOR BYOD. *Journal of Digital Forensics, Security and Law*, *16*(2), p.2.
195. Palanisamy, R., Norman, A.A. and Mat Kiah, M.L., 2020. BYOD policy compliance: Risks and strategies in organizations. *Journal of Computer Information Systems*, pp.1-12.
196. Hovav, A. and Putri, F.F., 2016. This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, *32*, pp.35-49.
197. Ali, M.D. and Kaur, D., 2020. Byod cyber forensic eco-system. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, *11*(9).
198. Dušanka, D., Darko, S., Srdjan, S., Marko, A. and Teodora, L., 2017. A comparison of contemporary data mining tools. In XVII International Scientific Conference on Industrial Systems (pp. 150-155).

199. AI-Qershi, F., AI-Qurishi, M., Rahman, S. M. M. & AI-Amri, A., 2014. Android vs. iOS: The Security Battle. s.l., World Congress on Computer Applications and Information Systems (WCCAIS).
200. Le, D.-N.et al., 2018. chapter 14. In: CYBERSECURITY IN PARALLEL AND DISTRIBUTED COMPUTING. s.l.:A JOHN WILEY & SONS, INC., PUBLICATION.
201. Aickelin, U. and Dasgupta, D., 2005. Artificial immune systems. In *Search methodologies* (pp. 375-399). Springer, Boston, MA.
202. Chanal, P.M., Kakkasageri, M.S. and Manvi, S.K.S., 2021. Security and privacy in the internet of things: computational intelligent techniques-based approaches. In *Recent Trends in Computational Intelligence Enabled Research* (pp. 111-127). Academic Press.
203. Brown James and Leander Jamal 2017 **An Evolutionary Approach to Cyber Security: Protecting Mobile Devices and Networks,** North Carolina Agricultural and Technical State University. ProQuest Dissertations Publishing, 2017. 10267464.
204. Watkins, A., and Boggess, L. (2002). "A new classifier based on resource limited artificial immune systems," in IEEE World Congress on Computational Intelligence, 1546–1551.
205. Al-Enezi, J.R., Abbod, M.F. and Alsharhan, S., 2010. Artificial immune systems-models, algorithms and applications.

# Appendix A

This table analysis available in chapter 5 which is analysis chapter. This table represent the risk management steps which Widley used in participated organizations.

Table A.1: Risk management steps which widley used in participated organizations.

| What are the risk management steps used to control BYOD risk in your organisation | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Participant** | Risk assessment | Risk Analysis | Risk Plan | Disaster recovery | Risk treatment | Risk identification | IT reaction |
| **1** | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| **2** | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| **3** | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| **4** | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| **5** | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| **6** | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| **7** | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| **8** | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| **9** | | | | | | | |
| **10** | | | | | | | |
| **11** | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **12** | | | | | | | |
| **13** | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| **14** | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| **15** | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| **16** | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| **17** | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| **18** | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **19** | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| **20** | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| **21** | 1 | 0 | 0 | 1 | 0 | 0 | 1 |

The analysis of table A.2 is available in chapter 5. This part of survey 1

Table A.2: which shown the used countermeasures.

| TParticipant | MDM | Network Segregation, | policy | Encryption | VPN access | Applications restrictions |
|---|---|---|---|---|---|---|
| **1** | 1 | 1 | 1 | 1 | 0 | 0 |
| **2** | 0 | 0 | 1 | 0 | 0 | 0 |
| **3** | 0 | 1 | 1 | 1 | 0 | 0 |
| **4** | 0 | 1 | 0 | 0 | 0 | 0 |
| **5** | 1 | 1 | 1 | 1 | 1 | 0 |
| **6** | 0 | 0 | 1 | 0 | 1 | 0 |
| **7** | 0 | 0 | 1 | 0 | 1 | 0 |
| **8** | 0 | 1 | 0 | 0 | 1 | 0 |
| **9** | 0 | 1 | 0 | 0 | 0 | 1 |
| **10** | 0 | 0 | 1 | 1 | 0 | 0 |
| **11** | 0 | 0 | 0 | 0 | 1 | 0 |
| **12** | 0 | 1 | 1 | 0 | 0 | 0 |
| **13** | 0 | 0 | 0 | 0 | 1 | 0 |
| **14** | 0 | 0 | 0 | 1 | 0 | 0 |
| **15** | 0 | 1 | 1 | 1 | 0 | 0 |
| **16** | 1 | 1 | 1 | 1 | 1 | 0 |
| **17** | 1 | 1 | 1 | 1 | 1 | 0 |
| **18** | 1 | 0 | 0 | 0 | 0 | 0 |
| **19** | 0 | 1 | 0 | 0 | 1 | 0 |
| **20** | 1 | 1 | 1 | 1 | 1 | 0 |
| **21** | 1 | 1 | 1 | 1 | 1 | 0 |
| | **MDM** | **Network Segregation,** | **policy** | **Encryption** | **VPN access** | **Applications restrictions** |

**Table A.3: Which of the following activities consume a significant amount of your time? - Security management**

| Participant | Security Incident response management | Security operations | Software development | Vulnerability assessment | penetration testing | searching new technologies and Security solutions | Provide advice on security to customer |
|---|---|---|---|---|---|---|---|
| **1** | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| **2** | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| **3** | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| **4** | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| **5** | 1 | 0 | 0 | 0 | | 0 | 1 |
| **6** | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| **7** | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| **8** | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| **9** | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| **10** | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| **11** | 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| **12** | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| **13** | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| **14** | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| **15** | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| **16** | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **17** | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| **18** | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| **19** | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| **20** | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **21** | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

# Appendix B Progressing report

This appendix to show the progressing done every year of the research. The comments have been given by DoS and progressing panel.

| Year | Milestone Achievements |
|---|---|
| 2016 | • This is first stage where the first drafts of research proposal have been formatted and taking the approvals of DoS.<br>• Completed three online research and development modules, Research Communication, Managing Doctorate and Research Methods, Document management. Through this year a literature review has been structured. |
| 2017 | • Detailed literature review has been done which covered the research domain. The litterer review covered the BYOD security risks and threats. Moreover, it cover the comparative between different frameworks.<br>• Structuring the methodology chapter draft 1<br>• *There are two initial data sets have been gathered through two surveys.*<br>• *MDM system demonstration configured to generate the events log.* |
| 2018 | • *Remaining data set gathered through MDM system*<br>• *Publish two research work one in conference and other in journal*<br>• *Datasets collected and cleansing*<br>• Intelligent Risk management framework for BYOD is paper published in IEEE |

| | |
|---|---|
| | • The Proposed Framework start structured and developed.<br>• The stages and phased pf the framework workflow is designed. |
| 2019 | • IEEE ICBDSC 2019 in Muscat Oman, which about integrating the blockchain in higher education.<br>• Framework chapter drafted<br>• Integrated the MDM events log files with function log files<br>• BYOD security and risk challenges in Oman Organisations is paper presented in ICEBE in China. |
| 2020 | • *Update Literature review*<br>• *Updated framework chapter*<br>• Updated Analysis chapter<br>• Drafted tools chapter |
| 2021 | • *In this stage moving to write up stage where the thesis chapters are drafted as versions, review and updated* |

# Appendix C: MDM Configuration

This appendix demonstrating the MDM steps discussed in chapter 2.

Figure C.1: MDM dashboard.

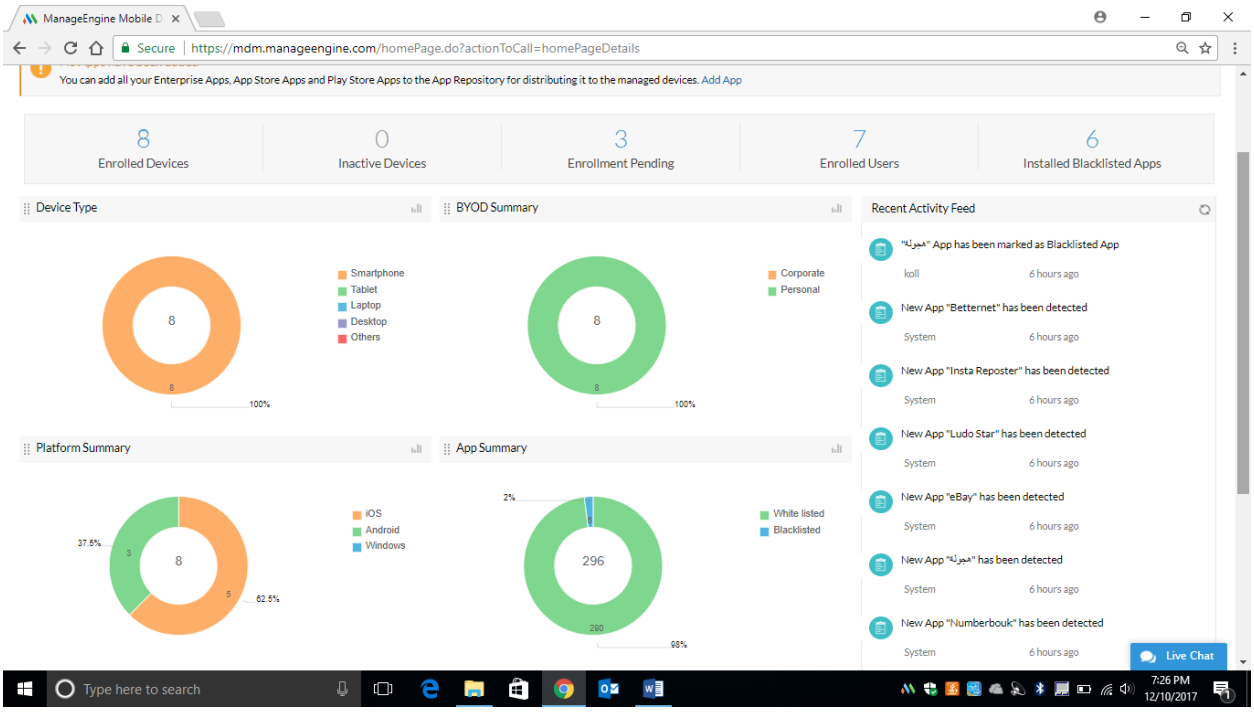


Figure C.2: Detection of white and blacklist applications in MDM

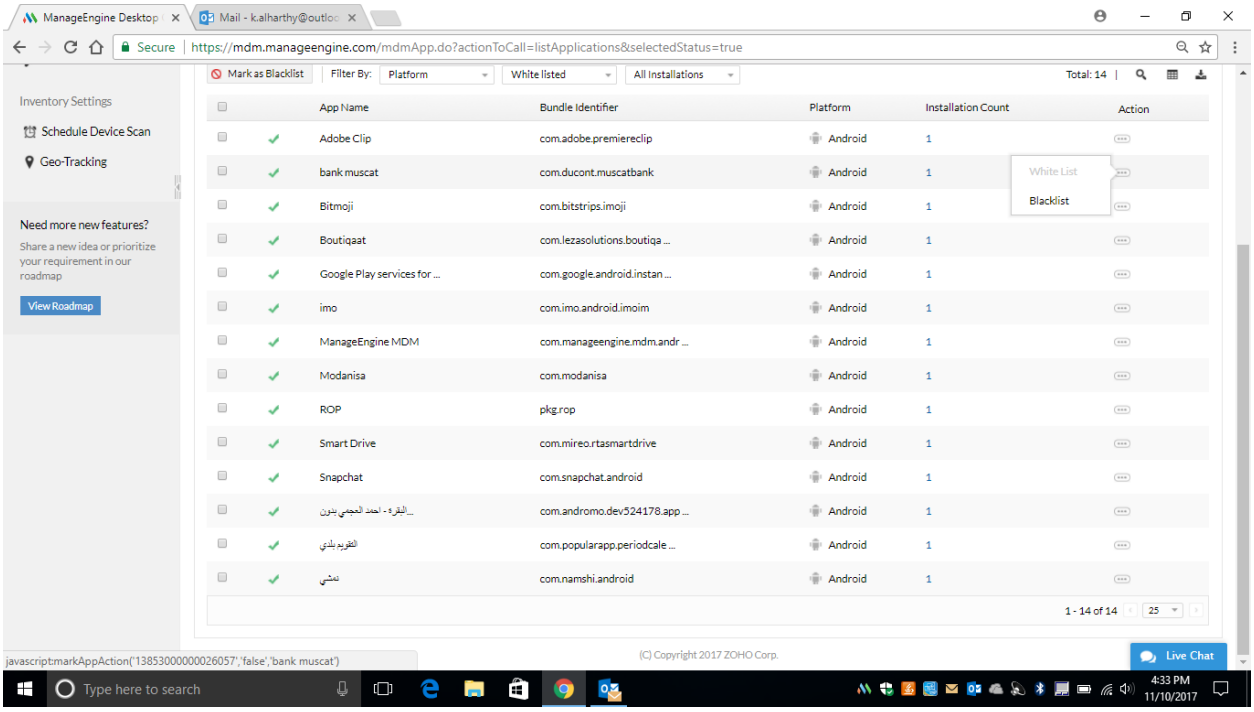



Figure C.3: enforcing passcode policy for MDM clients

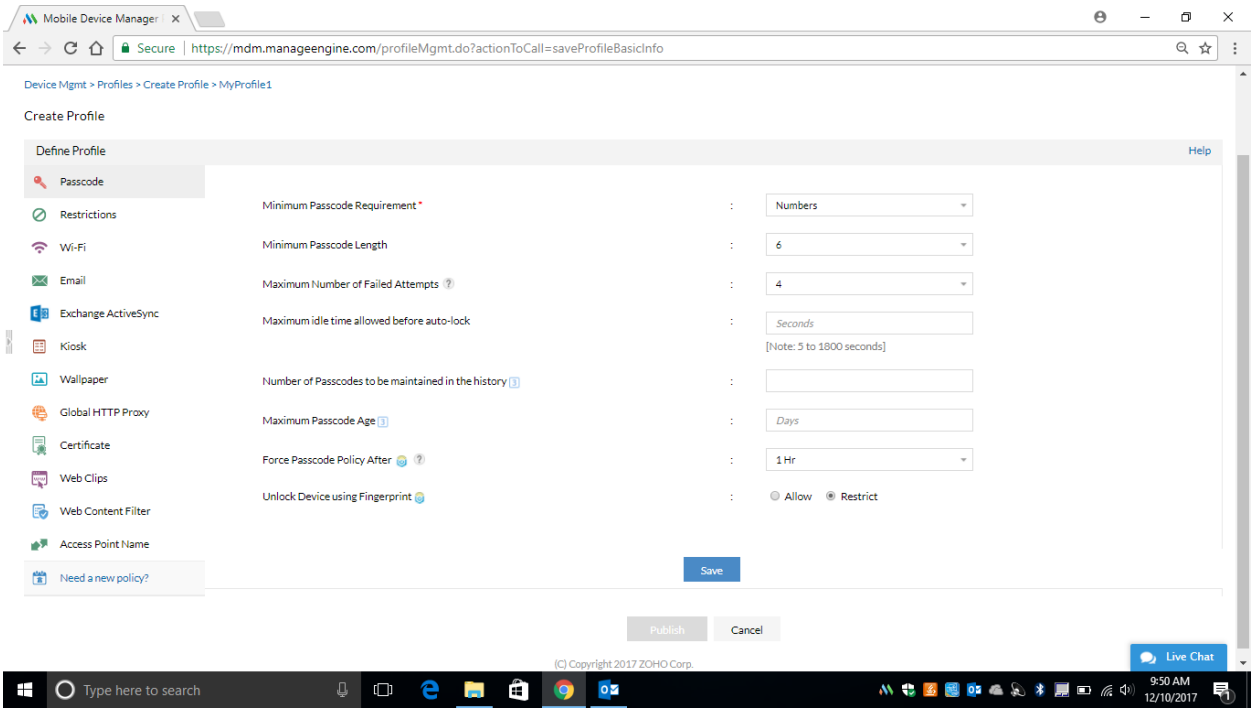


Figure C.4: Enrolement Process

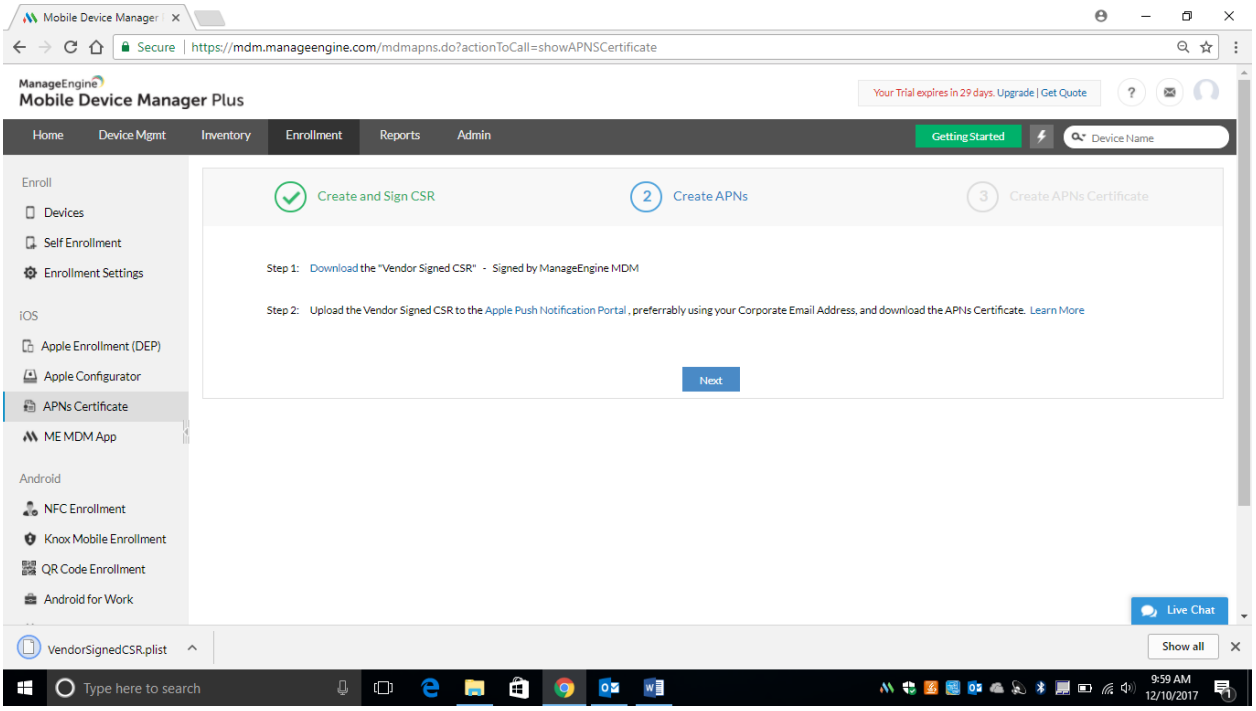


Figure C.5: iOS enronlmenet certification

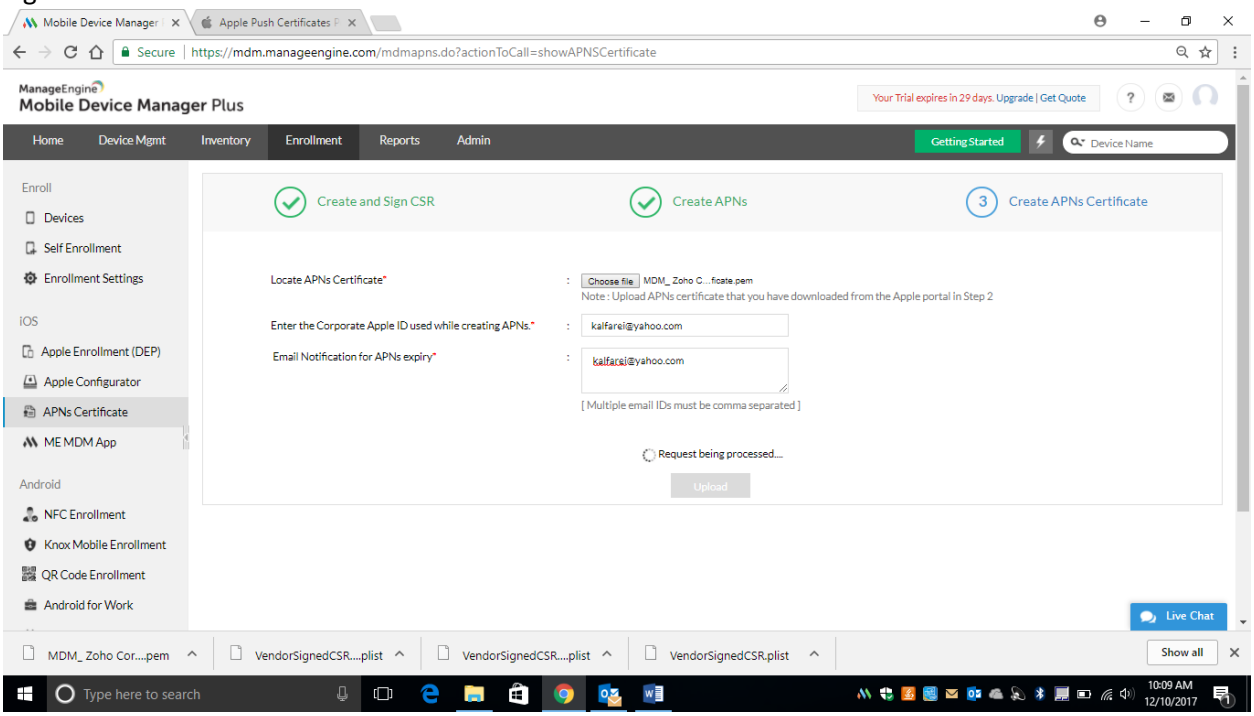



Figure C.6: iOS enronlmenet certification

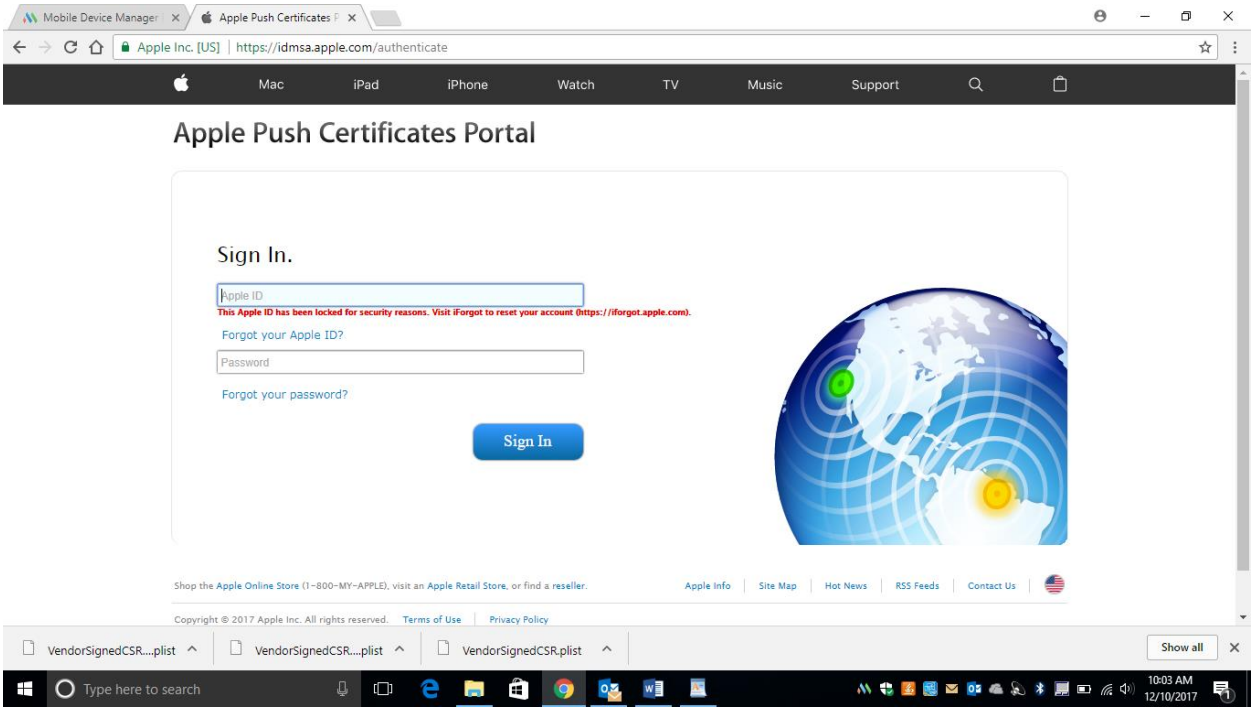


Figure C.7: Android enronlmenet

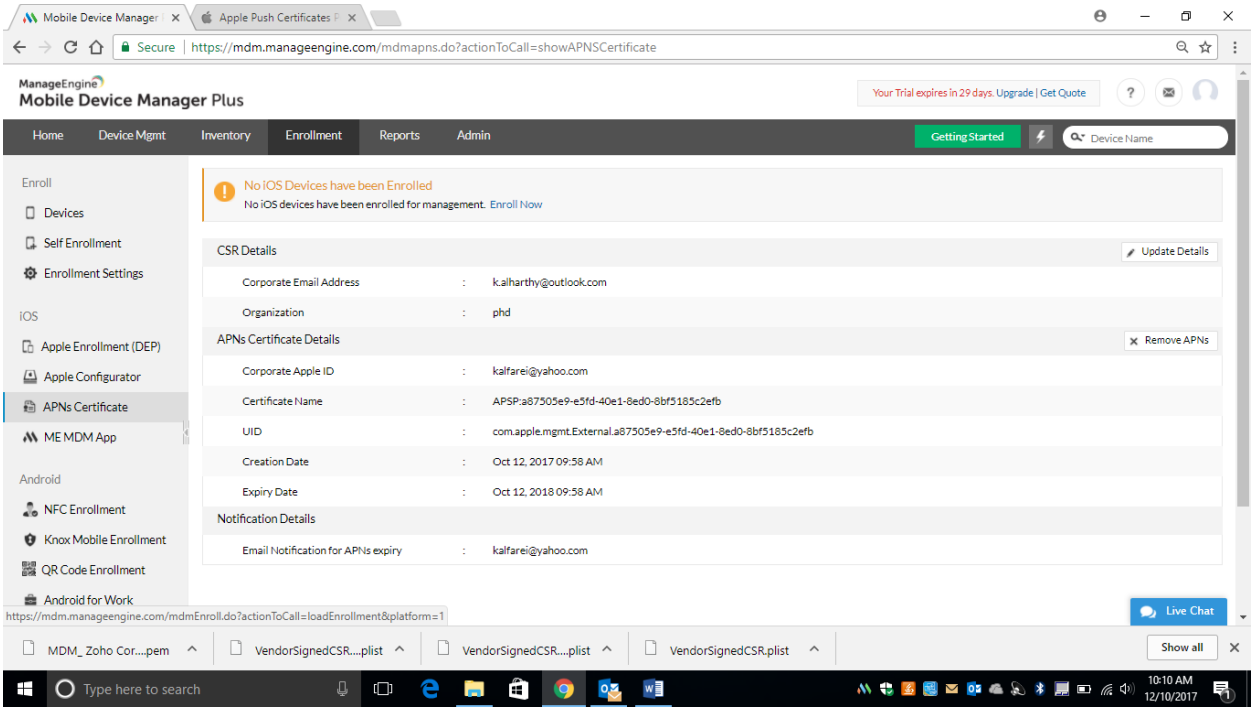



Figure C.8: admin control

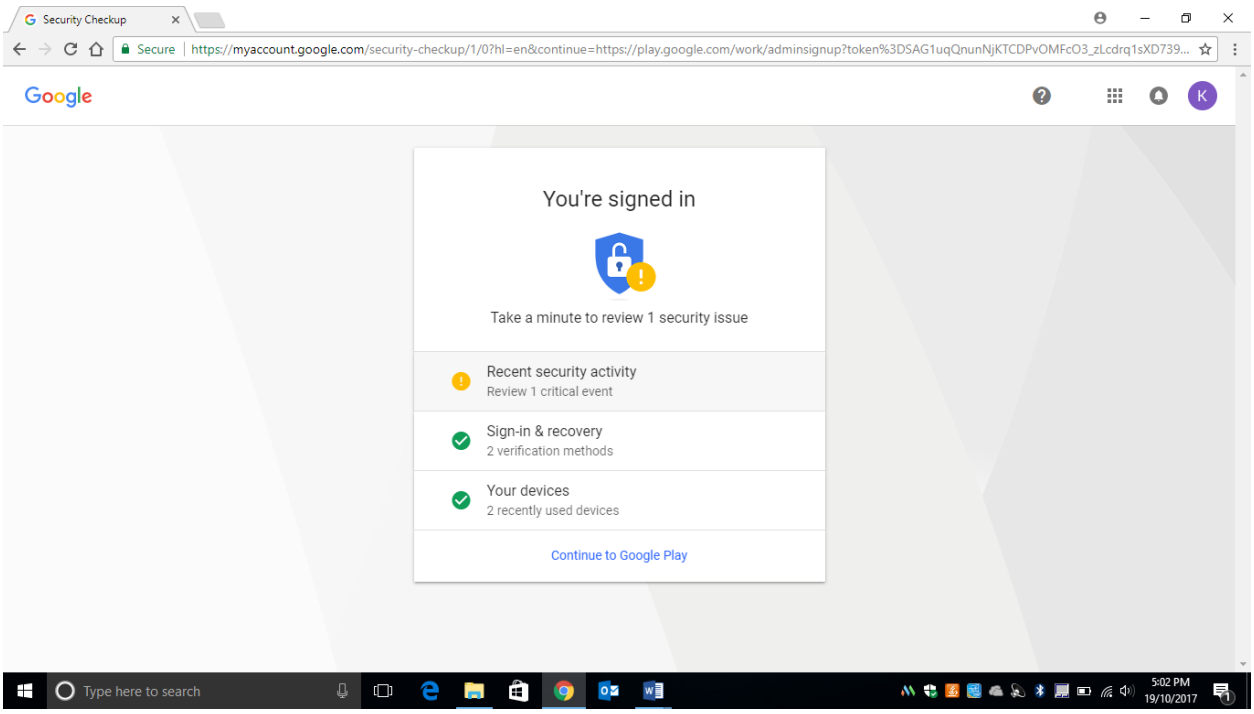


Figure C.9: setting Android for work which can be used to enforce apps

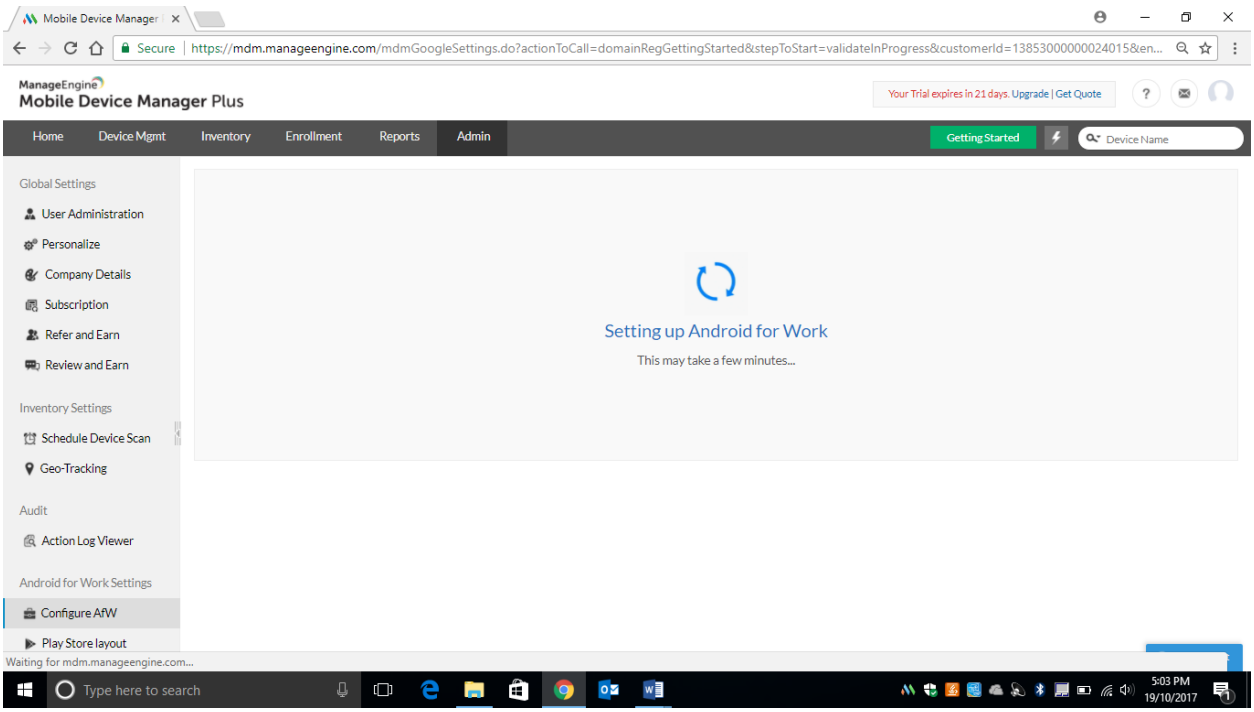


Figure C.10: Device Tracking location

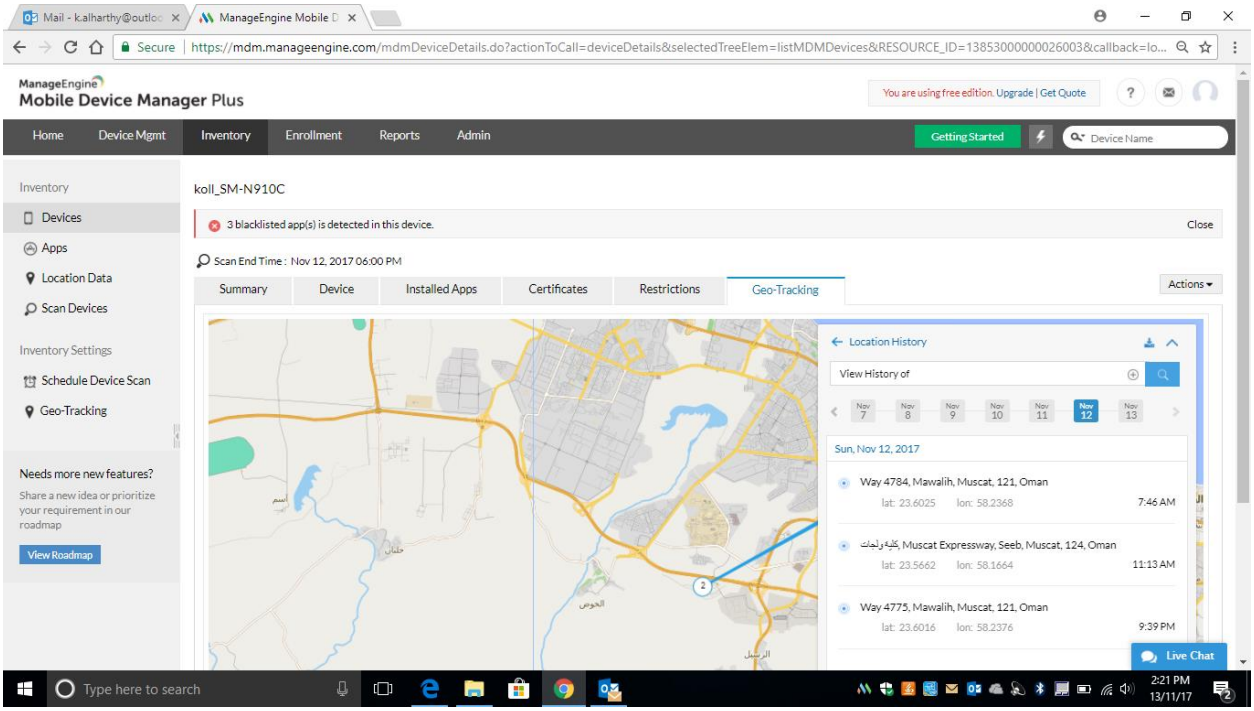



Figure C.11: Device remote access

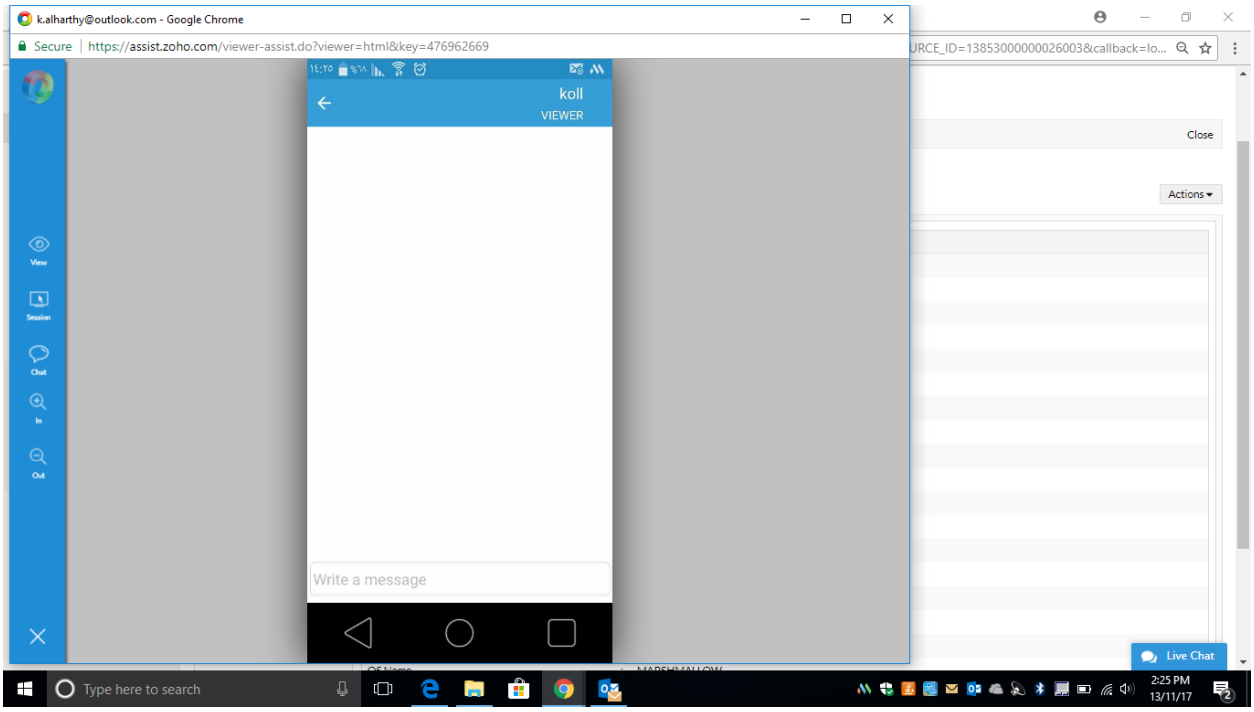
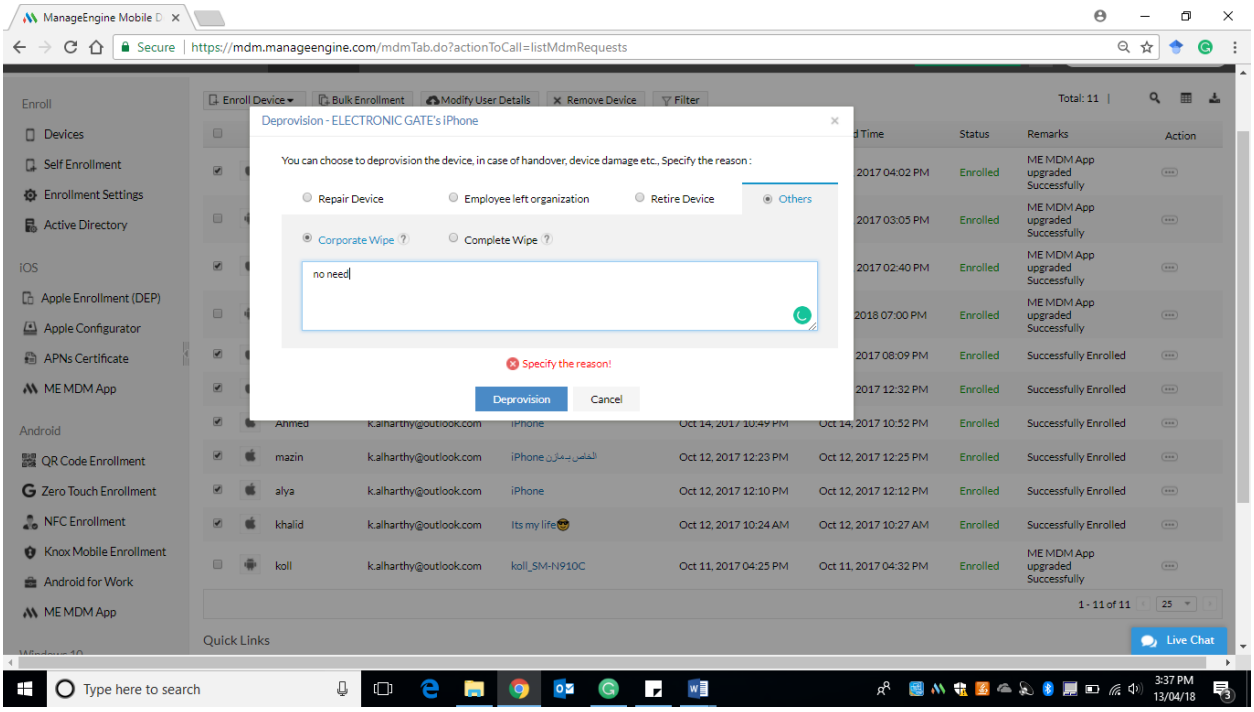


Figure C.5: Actions can be performed if the device was stolean or lost



# Appendix D: Coding snippet

This appendix presenting the print screen of the program codes.

```
package wekaclassification;
/**
 *
 * @author Khoula
 *
 */
import weka.classifiers.*;
import weka.classifiers.functions.*;
import weka.core.converters.ConverterUtils.*;
import weka.core.Instances;



public class WekaClassification {


  public static String trainingData =
"/Users/khoula/documents/NetBeansProjects/WekaClassification/dataFiles/training.csv";
   public static String testData =
"/Users/khoula/documents/NetBeansProjects/WekaClassification/dataFiles/test.csv";
```

```
package wekaclassification;
/**
 *
 * @author Khoula
 *
 */
import weka.classifiers.*;
import weka.classifiers.functions.*;
import weka.core.converters.ConverterUtils.*;
import weka.core.Instances;



public class WekaClassification {


  public static String trainingData =
"/Users/khoula/documents/NetBeansProjects/WekaClassification/dataFiles/training.csv";
   public static String testData =
"/Users/khoula/documents/NetBeansProjects/WekaClassification/dataFiles/test.csv";
```

```
    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) throws Exception {

        WekaClassification classification = new WekaClassification();
        Instances ins_train = classification.loadData(trainingData);
        Instances ins_test = classification.loadData(trainingData);

        // Training and testing of Multice
        Classifier cls = classification.buildMultiPrecepModel(ins_train);
        String s = classification.evaluateLogisticModel(cls, ins_train, ins_test);
        System.out.println( "====================== MultilayerPerceptron  Stat
====================== ");
        System.out.println(s);
        System.out.println( "====================== SVM Stat
====================== ");
       Classifier cls2 = classification.buildSVMModel(ins_train);
        String s2 = classification.evaluateSVMModel(cls, ins_train, ins_test);
        System.out.println(s2);
```

```
        System.out.println( "====================== SimpleLogistic  Stat
====================== ");
         Classifier cls3 = classification.logisticMModel(ins_train);
        String s3 = classification.evaluateLogisticModel(cls, ins_train, ins_test);
        System.out.println(s3);
    }

    public Instances loadData(String path) {
        Instances ds = null;
        try {
            ds = DataSource.read(path);// DataStore can use ARFF and CSV
            if (ds.classIndex() == -1)
            {
                ds.setClassIndex(ds.numAttributes() - 1);
            }
             }
        catch (Exception ex)
            {
            System.out.println("Data Set cant be loaded" + ex.toString());
```

```
        return ds;
    }

    public Classifier buildMultiPrecepModel( Instances ins)
    {
        MultilayerPerceptron mp = null;
        try
        {
         mp = new MultilayerPerceptron(); // Weks provided default parameters of
MultilayerPerceptron have been used
         mp.buildClassifier(ins);
        }

        catch( Exception ex)
        {
           System.out.println(" Error in creating MP model" + ex.toString());
        }
         return mp;
    }
```

```
public String evaluateMPModel(Classifier cls, Instances trainingSet, Instances testSet)
  {
  Evaluation eval = null;
  try {

     eval = new Evaluation(trainingSet);
     eval.evaluateModel(cls, testSet);
    }

  catch (Exception ex)
      {
      System.out.println(" Error in model evaluation "+ ex.toString());
  }

  return eval.toSummaryString("", true); // return some statistics
}

public Classifier buildSVMModel(Instances ins)
```

```
    SMO classifier = null;

    try{
    classifier = new SMO();

    classifier.buildClassifier(ins);
    }

    catch(Exception ex)
    {
        System.out.println(" Error in SVM Model" + ex.toString());

}
    return classifier;
}

 public String evaluateSVMModel(Classifier cls, Instances trainingSet, Instances testSet) {
    Evaluation eval = null;
    try {
```

```
        eval = new Evaluation(trainingSet);
        eval.evaluateModel(cls, testSet);
       }

    catch (Exception ex) {
         System.out.println(" Error in model evaluation "+ ex.toString());
    }

    return eval.toSummaryString("", true); // return some statistics
}

  public Classifier logisticMModel(Instances ins)
{
    Logistic classifier = null;
    try{
    classifier = new Logistic();
    classifier.buildClassifier(ins);
    }
    catch(Exception ex)
    {
```

```
            System.out.println(" Error in Logistic Model" + ex.toString());
        }
            return classifier;
        }
        public String evaluateLogisticModel(Classifier cls, Instances trainingSet, Instances
testSet)
 {
            Evaluation eval = null;
            try {
                eval = new Evaluation(trainingSet);
                eval.evaluateModel(cls, testSet);
               }
            catch (Exception ex) {
                 System.out.println(" Error in logistic model evaluation "+ ex.toString());
            }
            return eval.toSummaryString("", true); // return some statistics
        }
}
```