TOWARDS A UNIFIED FRAUD MANAGEMENT AND DIGITAL FORENSIC FRAMEWORK FOR MOBILE APPLICATIONS

by

RUDY KATLEGO BOPAPE

submitted in accordance with the requirements for
the degree of

MASTER OF SCIENCE

in the subject

COMPUTING

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF. ERNEST KETCHA NGASSAM

2015

DECLARATION

Student number: 47220295

I declare that *Towards a Unified Fraud Management and Digital Forensic Framework for Mobile Applications* is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I have not previously submitted this work, or part of it, for examination at UNISA for another qualification or at any other higher education institution.

SIGNATURE DATE

DEDICATION

I dedicate this dissertation to my daughter, Atlegang Bopape and my son, Leago Bopape.

ACKNOWLEDGEMENTS

First and foremost, I would like to praise and thank God Almighty, whose many blessings have made me who I am today and have seen me complete this research successfully.

I am grateful to Prof. Ernest Ketcha Ngassam for having accepted to be my supervisor. His patience, guidance and efforts have not gone unoticed or unappareciated. He has gone beyond the role of an advisor to assume the role of an academic mentor and father, making an effort to push me, to explain difficult concepts and impart his wealth of knowledge onto me.

I wish to thank my beloved husband, Lebogang Bopape, who has fully supported me throughout my academic journey. I thank you for your patience, for your words of encouragement and for believing in me when I did not. I love you dearly, I appreciate you and I thank God for you.

A special and warm thank you to my parents, Neville and Joan Kekana, whose role in supporting my education was nothing less than fundamental. From my earliest days of school, their sacrifice, time, money and effort enabled me to reach goals that even I doubted at times. I am especially grateful to my father, Neville, for always teaching me the importance of education.

Mokgona Nyamane, my sister, I thank you for selflessly offering to take the pressure off me of being a mom and a student, especially on those weekends when I needed some time off to study.

My good friend and mentor Bessy Mahopo; a special heartfelt thank you for your unwavering support and love when I needed it most. Your constant encouragement to go one step further and patience are always an inspiration to me.

Finally, I am grateful to my extended family and friends whose encouraging words kept me going even in the toughest of times.

ABSTRACT

Historically, progress in technology development has continually created new opportunities for criminal activities which, in turn, have triggered the need for the development of new security-sensitive systems. Organisations are now adopting mobile technologies for numerous applications to capitalise on the mobile revolution. They are now able to increase their operational efficiency as well as responsiveness and competitiveness and, most importantly, can now meet new, growing customers' demands.

However, although mobile technologies and applications present many new opportunities, they also present challenges. Threats to mobile phone applications are always on the rise and, therefore, compel organisations to invest money and time, among other technical controls, in an attempt to protect them from incurring losses. The computerisation of core activities (such as mobile banking in the banking industry, for example) has effectively exposed organisations to a host of complex fraud challenges that they have to deal with in addition to their core business of providing services to their end consumers. Fraudsters are able to use mobile devices to remotely access enterprise applications and subsequently perform fraudulent transactions. When this occurs, it is important to effectively investigate and manage the cause and findings, as well as to prevent any future similar attacks. Unfortunately, clients and consumers of these organisations are often ignorant of the risks to their assets and the consequences of the compromises that might occur. Organisations are therefore obliged, at least, to put in place measures that will not only minimise fraud but also be capable of detecting and preventing further similar incidents.

The goal of this research was to develop a unified fraud management and digital forensic framework to improve the security of Information Technology (IT) processes and operations in organisations that make available mobile phone applications to their clients for business purposes. The research was motivated not only by the increasing reliance of organisations on mobile applications to service their customers but also by the fact that digital forensics and fraud management are often considered to be separate entities at an organisational level.

This study proposes a unified approach to fraud management and digital forensic analysis to simultaneously manage and investigate fraud that occurs through the use of mobile phone applications. The unified Fraud Management and Digital Forensic (FMDF) framework is designed to (a) determine the suspicious degree of fraudulent transactions and (b) at the same time, to feed into a process that facilitates the investigation of incidents.

A survey was conducted with subject matter experts in the banking environment. Data was generated through a participatory self-administered online questionnaire. Collected data was then presented, analysed and interpreted quantitatively and qualitatively. The study found that there was a general understanding of the common fraud management methodologies and approaches throughout the banking industry and the use thereof. However, while many of the respondents indicated that fraud detection was an integral part of their processes, they take a rather reactive approach when it comes to fraud management and digital forensics. Part of the reason for the reactive approach is that many investigations are conducted in silos, with no central knowledge repository where previous cases can be retrieved for comparative purposes. Therefore, confidentiality, integrity and availability of data are critical for continued business operations.

To mitigate the pending risks, the study proposed a new way of thinking that combines both components of fraud management and digital forensics for an optimised approach to managing security in mobile applications. The research concluded that the unified FMDF approach was considered to be helpful and valuable to professionals who participated in the survey. Although the case study focused on the banking industry, the study appears to be instrumental in informing other types of organisations that make available the use of mobile applications for their clients in fraud risk awareness and risk management in general.

Keywords

Fraud management; digital forensics; mobile applications; mobile devices; threats; frameworks; process models; paradigms

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation or Acronym	Description
AICPA	American Institute of Certified Public Accountants
CBR	Case-based Reasoning
DF	Digital Forensic
DFRWS	Digital Forensic Research Conference
EBR	Experience-based Reasoning
EIDIP	Enhanced Digital Investigation Model
FFML	Financial Fraud Modelling Language
FM	Fraud Management
FMDF	Fraud Management and Digital Forensic
FMS	Fraud Management System
FT	Forensic Technology
GPS	Global Positioning System
IT	Information Technology
KB	Knowledge Base
MMS	Multimedia Messaging Service
NSMP	Noise-suppressed Similarity Measure to Profile
OBSP	Objectives-based Sub-phases
SMS	Short Messaging Service
UMP	User Mobility Profile
CIMA	Chartered Institute of Management Accountants
IDIP	Integrated Digital Investigation Model
EIDIP	Enhanced Integrated Digital Investigation Model

Table 0.1: List of abbreviations and accronyms

1. INTRODUCTION AND BACKGROUND TO THE STUDY

1.1. INTRODUCTION

The ability of an organisation to fulfil its mission depends on the meaningful and productive use of its assets (Anderson & Choobineh, 2008). Mobile applications are now common assets used by many organisations for their core services to reach a broader audience and fulfil their missions in service delivery. These applications are exposed and subject to fraud risks, and their survival depends on the quality and effectiveness of the overall fraud management strategy that the organisation implements.

The concept of fraud management comprises a number of steps, of which prevention and detection are the most important and focal ones. Fraud prevention for mobile applications refers to application policies and procedures as well as communication that, when used in a combined approach, are able to stop fraud from occurring. Fraud detection, on the other hand, focuses on activities and techniques that promptly and timely recognise whether fraud has occurred or is occurring. While prevention techniques do not ensure that fraud will not be committed, they are the first line of defence in minimising fraud risk.

It is important to note that no system of internal control can provide absolute assurance against fraud. There needs to be a stream that defines the investigation process as well as a corrective action process (Jonkers, 2010). This is where digital forensics plays a crucial role. Forensic Technology (FT) can help capture, secure and deal with substantial volumes of mobile device information and recover hidden or lost data. Furthermore, it provides the tools and knowledge to analyse data and fits the results into meaningful fraud assessment reports. With such an integrated framework in place, it will be possible to improve the chances of loss recovery while minimising any exposure to litigation and damage to reputation. Furthermore, not only will such framework preserve evidence but it will also maintain confidence in users and mitigate losses.

The purpose of this study is to propose a unified framework for managing fraud and digital forensics for enterprises' mobile applications. The framework encompasses all aspects of fraud prevention, deterrence, detection, examination, investigation as well as reporting for the better management of any possible fraud incident that concerns the use of a mobile application.

This chapter serves as an introduction to the research study. It aims to put the research into perspective by highlighting the need for organisations to be proactive in addressing fraud risks that often affect their revenue and their reputational brand. A preliminary literature review provides the background of the study, and it briefly examines previous works on fraud management and digital forensics. Such a preliminary review is intended to inform the reader of the various fraud management and digital forensic frameworks, methodologies and approaches in use today as well as their merits and demerits as applied in various organisational contexts.

The chapter then elucidates the motivation, research context and the problem statement of this research study. Research objectives which guide this study are stated immediately after the problem statement. Methodologies, research strategy and data collection techniques to be adopted in the study are then also briefly discussed. This chapter also examines research ethics in order to inform the readers about how the respondents would be protected during data collection. The overall layout of the dissertation is then also provided in order to guide the reader on the number of chapters that constitute the dissertation and what each chapter covers. The chapter will then conclude by giving a detailed discussion of the research methodology, namely, the reason for conducting the research, the process followed through the research design, the choice of a research strategy, which data generation method was used, as well as the type of data analysis to be conducted. A summary of the chapter is provided in the chapter's conclusion section.

1.2. KEY CONCEPTS AND TERMS

In recent years, investigations of crimes committed by means of telecommunication technologies have become a burden to investigators, from both forensic and prevention perspectives. Computer crime investigation units across organisations are increasingly inundated with reports of various types of online fraud, such as phishing, targeted malware attacks, Trojans as well as insider threats, with mobile fraud being the most prevalent. As an illustration, during 2009, online banking grew with an estimated five million net new households banking online and/or via a mobile device. It is estimated that telecommunications fraud as a whole costs industries around $30 to $50 billion per annum, with mobile fraud costing about $300 billion per year (Burge & Shawe-Tyalor, 2001). In most cases, fraud is noticed very late, if noticed at all.

1.2.1. Mobile devices

Mobile communication is a subset of telecommunications where communication (data, voice and image) is conducted using a mobile device that is regarded as the basic communication instrument. A mobile device can be characterised as a pocket-sized computing device that has a display screen with a miniature keyboard and/or a touch input. These types of devices are seen as an extension to personal computers in the sense that they are capable of hosting a broad range of capabilities for both business (for example, e-mail, banking and e-commerce) and private use (for example, telephone and SMS). A perpetrator uses such a device to remotely connect to an enterprise application and commit a crime by fraudulently using the functionalities of the application. The fraudulent use of the application is done by providing ‘stolen’ credentials for authentication or by accessing unauthorised aspects of the application.

1.2.2. Mobile applications

Mobile applications are software that are either native to the mobile phone, such as games and calendars, or are accessed remotely through a web browser. Their role is to perform a range of tasks aimed at achieving mobile phone users' needs. These applications vary from communication applications, such as e-mail and social networking clients, to productivity applications, such as banking and financial services. Moreover, mobile devices provide users with an opportunity to store information at various storage facilities in 'the cloud', provided that the user has the appropriate credentials to do so. This represents a value-added service to mobile users who are willing to pay a fee, to be able to walk, talk and work freely and efficiently anywhere and at any time. Because of its valuable importance, as well as the critical nature of transactions that can be made via mobile phones (and therefore mobile applications), mobile data communication is subject to fraud and criminal intent.

Deployment of mobile technologies can present a significant amount of risk to the overall enterprise security position. Mobile devices and applications have numerous vulnerabilities that are susceptible to malicious attacks as well as non-malicious internal threats. From the type of network the mobile devices use to the threat of data loss, mobile devices have no shortage of inherent risk (ISACA, 2010). For example, fraudsters are able to obtain a smartphone and send an anonymous e-mail to a user, claiming to be from a recognised organisation in order to mislead the recipient into revealing sensitive information for use in identity theft. The recipient is told to visit a website where they are asked to enter sensitive information such as passwords and banking details. In this whole process, the user is without knowledge that confidential information is being submitted to fraudsters. A fraudster then logs on to a mobile application, for example, internet banking, and is able to transact without the user's consent. Thus, in essence, fraudsters make use of the same tools and technology that drive and build the business to their own advantage. This type of fraud is noticed late, if at all, and when it is, there should be measures that are put in place at enterprise level to manage and investigate the incident.

1.2.3. Fraud management

Telecommunications fraud management deals with detecting, managing and investigating any attempt to steal by deception or to deliberately abuse services offered via telecommunications (Bihina Bella, Eloff & Olivier, 2009). A fraud management framework identifies and acts against a potential known fraudulent behaviour. In the case of a fraud incident perpetrated using a mobile device through a banking application, the fraud management approach would first collect fraud data from the device, such as (a) the date and time the fraud took place, (b) the transactions and (c) the account number involved. The next step would be to process collected data for analysis and, finally, to apply a set of rules based on the characteristics of a known fraud type. This set of rules can then be used in future to detect similar fraud used through the same modus operandi and raise an alert. In essence, a fraud management approach involves monitoring and managing any mobile fraud incident.

1.2.4. Digital forensics

Because mobile devices carry details about communication, online activities and the whereabouts of an individual at specific times, it is possible to acquire and examine the data on the device to investigate how the fraud occurred. For this, digital forensics methods are used that focus on what happens after fraud and whose role is also to attempt to discover what actions may have occurred to cause it. Vacca (2002) describes digital forensics as the preservation, extraction and analysis of evidence where the documentation of digital evidence is stored as data or magnetically encoded information. For any mobile fraud incident, the data inherent in the device are acquired and analysed. From captured data, an expert investigator would be able to analyse data such as the date and time the fraud occurred, the modus operandi used to gain access to the device and its application, as well as the details of the transaction's history.

For any transaction to be secured over a mobile network through the use of a mobile device, it should consist of independent and modular processes. First, there is a need for identification; a mobile device and application users should be allowed to send their unique identification information, e.g. a user ID (for instance, to a server network), for verification in order to gain access to a mobile banking application. Secondly, the mobile application should be able to authenticate the transaction from users via an identification process or cryptographic mechanism. The transaction is then performed on the mobile application which carries the responsibility of ensuring that the requested transaction is performed under a secure environment. In cases where there is identity theft as described earlier, it is easy for this supposed secure transaction to be conducted by an attacker without the knowledge of the legitimate user. When this happens, there needs to be a seamless process that investigates the cause and finds better ways to manage similar type of fraud in the future. It would be ideal to have a single solution that performs both the tasks of fraud management and digital forensic approaches combined – a solution which offers the capability of monitoring and detecting fraud on one side, and then automatically conduct an investigation to identify the root cause on the other side. This study serves to propose a mind shift towards a unified fraud management and digital forensic framework that has not been presented in previous research.

1.3. PROBLEM STATEMENT

Mobile devices are continuously evolving and have went on to become more powerful when compared to how powerful personal computers were in the mid to late 1990s. They offer users convenience and portability and nowadays provide more than just the telephony service they were originally designed for. Such an increased adoption has created an ideal platform for fraudsters to attack, and these attacks are expected to proliferate in the same way that they have with personal computers. A fraudster is able to use a mobile device to access a remote application in order to participate in online fraud. Mobile applications (commonly called ‘apps’) provide enhanced convenience and functionality. Developers have created a myriad of mobile applications for various uses and activities, which further contributes to the proliferation of mobile adoption. Anyone can potentially develop and distribute mobile applications with little oversight, making apps a potential attack vector for cybercriminals. For example, compared to about a year ago, today’s mobile banking scene faces a greater threat of malware and viruses attacking mobile phones, especially with more users conducting transactions on their handsets. Malware is software that has been developed to execute malicious intent on a mobile device. Research has shown that in Europe and the USA, there has been an increase in the number of malware attacks that target financial institutions (Eschelbeck, Gerhard, 2014).

By far, the worst drawback of mobile fraud has to do with the financial loss that this incurs. When money is lost, financial strain is felt by an individual, a group, an organisation and even society. Another effect is that of a psychological nature. This type of fraud is a personal violation, and although there is no physical injury, the victim still finds the betrayal to be as severe as an injury.

Against this background, there needs to be a mechanism to put together a model to monitor mobile applications against fraud risk, such that if an attack occurs, this will be traceable back to the fraudster. This explains the need to undertake a search towards producing a unified fraud management and digital forensic framework for mobile applications. Such a framework will not only assist in curbing the frequency of these attacks that occur in mobile applications but will also help in proactively gathering evidence for further investigation.

1.4. RESEARCH OBJECTIVES

The main objective of this research is

to develop a unified fraud management and digital forensic framework for mobile applications.

To achieve this, the following sub-objectives need to be accomplished:

- **Sub-objective 1:** Investigate mobile applications, their architecture and threat landscape.
- **Sub-objective 2:** Explore and analyse the advantages and limitations of existing fraud management approaches with regard to mobile applications.
- **Sub-objective 3:** Explore and analyse the advantages and limitations of existing digital forensic approaches concerning mobile applications.
- **Sub-objective 4:** Conceptualise a preliminary fraud management and digital forensic framework for mobile applications.

1.5. RESEARCH QUESTIONS

The following is the primary research question which this study aims to address:

> *How can a framework for fraud management and digital forensic be developed to simultaneously minimise the vulnerability of mobile applications and proactively trigger the forensic process when a fraud occurs?*

The following are the derived secondary research questions:

- **Research Question 1:** What is the threat faced by mobile applications with regard to their architecture?
- **Research Question 2:** What is state-of-the-art fraud management with respect to mobile applications?
- **Research Question 3:** What is state-of-the-art digital forensic as regards mobile applications?
- **Research Question 4:** How can a unified fraud management and digital forensic framework be developed for mobile applications?

Although this might often not be the case in many studies, there is a direct mapping between research objectives and identified research questions. While the first three research questions will be answered through a literature review, it should be noted that the identification of the threats landscape of mobile applications based on their architecture will be one of the first contributions of this study. With reference to second and third research questions, an understanding of the literature on fraud management and digital forensics will enable the alignment of investigated approaches to the threat landscape of mobile applications which is an additional contribution. The main contribution will be that of the suggestion of the conceptual framework from the fourth research question, which will further be validated and improved based on a case study from the banking industry.

1.6. ASSUMPTIONS AND LIMITATIONS

An overview of research assumptions, delineations and limitations is outlined below.

1.6.1. Assumptions

This study assumes that

- the respondents would voluntarily participate and cooperate by providing the researcher with all vital information needed for the success of this study;
- the participants would be familiar with the research instruments to be used in this study; and
- the participants' perspectives would be meaningful, knowable and be made explicit so that they affect the success of this study positively.

1.6.2. Limitations

For the purpose of this study, the researcher will only focus on mobile applications within the banking environment. Any other forms of fraud risks outside mobile applications will not be investigated.

1.7. RESEARCH METHODOLOGY

The study will undergo a thorough literature review. First, it is necessary to understand the fraud landscape for mobile applications. Secondly, it is essential to investigate the various approaches and models used for fraud management and digital forensics respectively.

The data to be used in the literature study will be collected mainly from journal articles, conference papers, books, previous dissertations/theses and the World Wide Web (internet) in general. This literature review will answer the first three research questions.

A research methodology is a systematic way to solve a problem. It is the science of studying how research is to be carried out (Miles & Huberman, 1994). The procedures by which researchers go about their work of describing, explaining and predicting phenomena are called research methodology and are aimed at giving the work plan of the research. The results obtained from the literature review will then be used to conduct a gap analysis. Such a study will help compare the actual performance of these fraud management and digital forensic approaches respectively to potential performance that can be achieved. On conclusion of the literature study, logical argumentation will be established, which will lead to the creation of the unified FMDF framework. This will answer the fourth research question. The method to be used in the context of this research design will be through an experienced survey, which is aimed at focusing and obtaining the same kinds of data from a group of people in a standardised and systematic way (Oates, 2006). The survey will only include individuals who have had practical experience in either fraud prevention, and detection, or forensic investigations.

This section outlines the research methodology followed in this dissertation and also explores some contextual factors that affect and influence the choice of a research methodology. The use of both the quantitative and qualitative research methodology for implementing the survey strategy will be justified. The research instrument, also referred to as the data generation method, to be used in this study is also introduced.

This study intends to implement the research process suggested by Oates (2006), as shown in Figure 1.1.

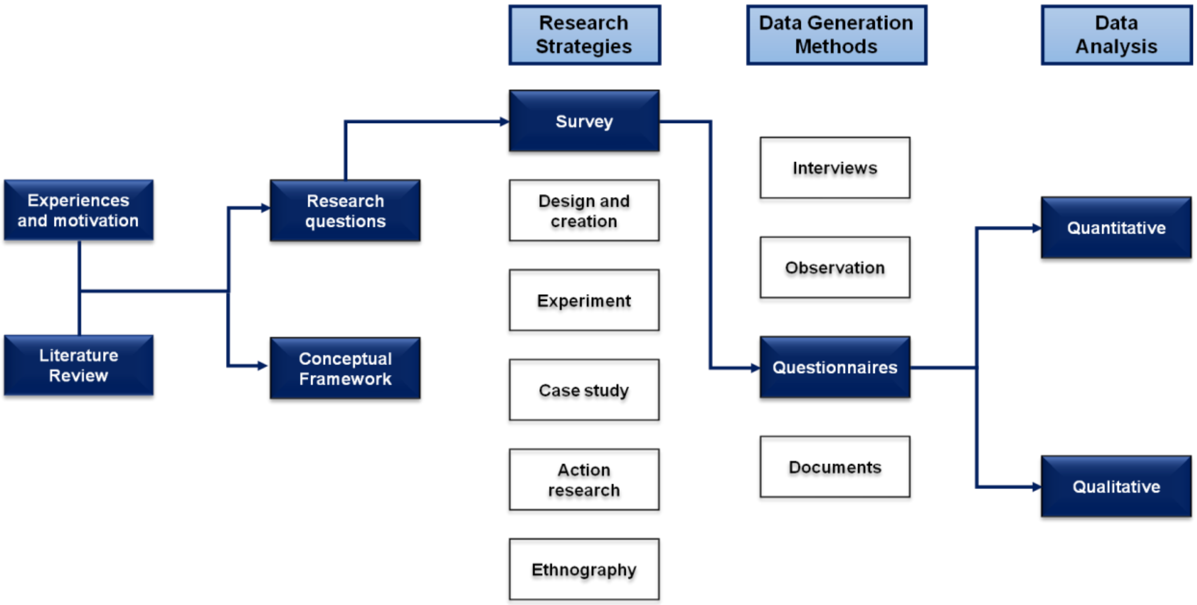


Figure 1.1 Approach of the research process
Source: (Oates, 2006)

1.7.1. Reason for conducting the research

Personal experience and motivation: The researcher's previous experience in the field of fraud management within the banking environment made it possible for some first-hand personal insight into the challenges of online fraud to be brought to the table. This served as motivation for this study regarding how the current fraud management approaches could be improved. One of these challenges included turnaround times for fraud investigations as well as the ability to link various cases to one another due to the forensic function placed separately from fraud management.

Literature review: Academic books, journal articles and conference papers that have already been written on the topic have been reviewed. By studying the literature, the researcher gained an understanding of previous work that was done before in both the fraud management and digital forensic fields. This knowledge allowed the researcher to decide on what topics remain to be addressed. Various frameworks, approaches and models were critically evaluated in order to discover themes that linked various authors and literature. The literature review also aided in providing a conceptual framework of the research discussed in the next section.

1.7.2. Research design

Research questions: A set of research questions discussed in Chapter 1 of the study were developed based first on the set of objectives to be achieved. Secondly, they were based on suggestions in the reviewed literature of where more research and investigation were required.

Conceptual framework: Miles and Huberman (1994:18) describe a conceptual framework as something that "*explains either graphically, or in narrative form, the main things to be studied – the key factors, concepts or variables – and the presumed relationship among them"*.

The conceptual framework of this study aims to make explicit the structure of thinking about the research topic and process undertaken and the structure/content for the whole study based on literature and personal experience (Vaughan, 2008). In this study, the conceptual framework is developed after the literature review and provides the structure/content for the whole study based on literature and personal experience as described in the previous section. The framework is suggested based on gap analysis form various topics in the literature and further improved based on the analysis of participants' feedback.

1.7.3. Research strategy

The strategy used in the context of this study is an experienced survey, which is aimed at focusing on obtaining the same kind of data from a group of people in a standardised and systematic way (Oates, 2006). The survey only included people who have had practical experience in either fraud prevention, and detection, or forensic investigations. This was done to ensure that competent respondents were able to contribute new ideas and to ensure a representation of different types of experience (Kothari, 2004). A survey research design was chosen because it best served to answer the questions and the purposes of this study. A survey research is one in which a group of people or items are studied by collecting and analysing data from only a few people or items considered to be representative of the entire group. In other words, only a part of the population is studied, and findings from this are expected to be generalised to the entire population (Kothari, 2004).

1.7.4. Data generation method

Survey research uses questioning as a strategy to elicit information from subjects in order to determine characteristics of selected populations on one or more variables. The chosen data generation method is a questionnaire, and the following rationale is given:

- A questionnaire allows the gathering of data from any part of the world through the use of existing technology.
- The standardised wording of a questionnaire reduces interference in subject responses.
- In addition to the standardised wording, the structure of questions allows for higher reliability in data than is practically possible in an interview, for example.
- The questionnaire may be completed at the respondent's convenience.

1.7.5. Data analysis

This study mostly used quantitative design, as well as qualitative design, which, when combined, are referred to as 'mixed methods'. Mixed methods is a procedure for collecting, analysing and mixing both quantitative and qualitative data at some stage of the research process within a single study in order to understand a research problem more completely (Creswell, 2002). The rationale for mixing is that neither quantitative nor qualitative methods are sufficient by themselves to capture details and challenges of the current fraud and forensic landscape. When used in combination, quantitative and qualitative methods complement each other and allow for a more complete analysis of the study (Tashakkori & Teddlie, 2003).

Quantitative data analysis: In quantitative research, reliance in only placed on numerical data, and it uses claims for developing knowledge, such as cause-and-effect thinking, reduction to specific variables, hypotheses and questions, use of measurement and observation, and the test of theories (Degu & Yigzaw, 2006). Further, variables to investigate and choose instruments will be determined, which will yield highly reliable and valid scores.

Qualitative data analysis: Alternatively, qualitative research is an inquiry process of understanding where the researcher develops a complex, holistic picture as well as reports the views of respondents (Creswell, 2002). In qualitative research, data analysis is based on the feedback that the participants perceive for their world and ultimately produces an understanding of the problem based on multiple contextual factors (Miller & Creswell, 2000).

Mixed methods approach: In a mixed methods approach, the analysis involves mixing methods, approaches, concepts or language into a single study (Onwuegbuzie & Combs, 2011). The approaches and units of analysis used are those which are most appropriate for finding an answer to their research questions (Tashakkori & Teddlie, 2009). An advantage of this approach is that quantitative and qualitative methods are compatible; thus, both numerical and text data, collected sequentially or concurrently, can help better understand the research problem.

1.8. ETHICAL CONSIDERATIONS

As this study required the participation of human respondents, specifically fraud and forensic professionals, certain ethical issues were addressed. A consideration of these ethical issues was necessary for the purpose of ensuring the privacy as well as the safety of the participants. Among the significant ethical issues that were considered in the research process were consent and confidentiality. To secure the consent of the selected participants, all important details of the study were communicated to the respondents, including the research aim and purpose. By explaining these important details, the respondents were able to understand the importance of their role in the completion of the research. The respondents were also advised that they could withdraw from the study even during the process. With that said, the participants were not forced to participate in the research. The confidentiality of the participants was also ensured by not disclosing their names or personal information in the research. Only relevant details that helped in answering the research questions were included. Furthermore, the research will record data accurately and fully. Data will not be manipulated into a suitable form for the research. The research will be open and honest about results obtained, without any falsification or fabrication. Wherever necessary, full credit will be given to original authors or material consulted and/or cited in this dissertation, with enough information provided in the reference list for further reading.

1.9. RESEARCH STRUCTURE

This dissertation is organised into seven chapters. Each chapter discusses important aspects of the research study. The outline of the research is depicted diagrammatically in Figure 1.2.

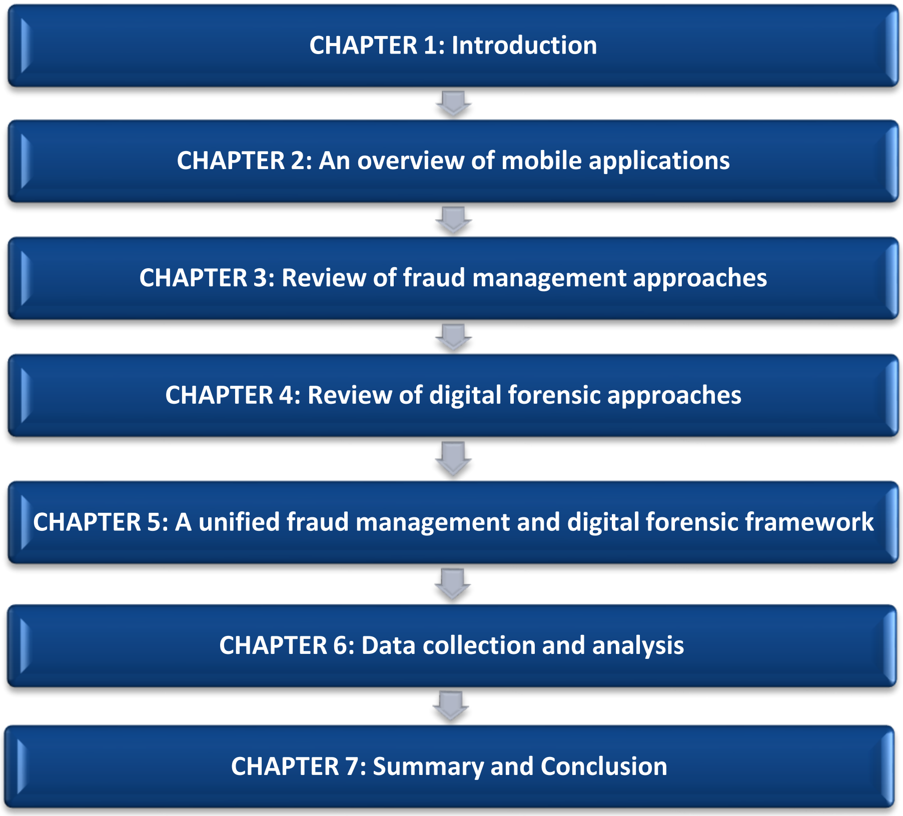

CHAPTER 1: Introduction
CHAPTER 2: An overview of mobile applications
CHAPTER 3: Review of fraud management approaches
CHAPTER 4: Review of digital forensic approaches
CHAPTER 5: A unified fraud management and digital forensic framework
CHAPTER 6: Data collection and analysis
CHAPTER 7: Summary and Conclusion

Figure 1.2: Research structure

Chapter 1 – Introduction: This chapter introduces the research and places it into perspective by addressing key aspects, namely, research background, context, motivation, statement of the problem, objectives, assumptions, delimitations, limitations, and research ethics. The chapter also gives the outline of the research. Chapter 1 also discusses the methodology, research strategy, design, data collection, and analysis techniques and tools. The survey research methodology has been discussed from both theoretical and practical views. This chapter also justifies the qualitative and quantitative research methodology, strategy, design, and data collection techniques and analysis.

Chapter 2 – An overview of mobile applications: This chapter answers the first research question. It gives an examination of scholarly work focusing on the development of mobile applications. The objective of the chapter is to briefly explore and characterise mobile applications as well as identify the various challenges faced by their usage from a fraud perspective.

Chapter 3 – Review of fraud management approaches: This chapter answers the second research question. It takes the reader through a number of existing frameworks and models that have been researched and used for fraud management. Each framework/model or approach studied is evaluated by highlighting its strengths and weaknesses.

Chapter 4 – Review of digital forensic approaches: Chapter 4 provides an answer to research question three. It is a detailed examination of scholarly work focusing on existing digital forensic approaches. Similar to Chapter 3, each framework, model or approach is studied and evaluated using a brief benefit and gap analysis.

Chapter 5 – Unified fraud management and digital forensic framework: The crux of this research study is presented in this chapter. Based on the research, a framework to simultaneously manage and investigate fraud that occurs through the use of mobile applications is presented. The framework is designed to determine the suspicious degree of fraudulent transactions and at the same time to feed into a process that facilitates the investigation of incidents.

Chapter 6 – Data collection and analysis: Chapter 6 describes the process undertaken to formulate the questionnaire used as a data generation method as well as to provide questions related to the framework for its validation and improvement. A rigorous analysis of data is carried out using narrations and constant comparison methods. Trends and themes are identified and discussed. Results are presented following each data analysis technique. Data is presented, analysed and interpreted qualitatively and quantitatively.

Chapter 7 – Conclusion: This chapter discusses research findings and then states conclusions from these findings. The research contribution is reflected on and recommendations for further studies are given. The chapter also summarises the outcome of the study. The reader is reminded of the initial objectives, and then the outcome of the study is compared with those objectives to ascertain whether they have all been met.

1.10. CONCLUSION

The objective of this chapter is to serve as an introduction to the research study by highlighting the need for organisations to be proactive in addressing fraud risks that often affect their revenue and their reputational brand. A preliminary literature review was provided followed by the motivation, research context and the problem statement of this research study. Methodologies, research strategy and data collection techniques to be adopted in the study are also briefly discussed. The research methodology used in this dissertation has been implemented according to the research process suggested by Oates (2006). Table 1.1 is a summary of important components of the research methodology used.

Research methodology	This dissertation
Research strategy	Survey
Data generation method	Questionnaire
Data analysis	Mixed methods approach

Table 1.1: Components of the research methodology

The objective of this chapter was to present the research methodology used for the gathering and analysis of the data for this study. The approach is taken from both the qualitative and quantitative perspectives. Through academic research, a survey methodology was identified as one of the most applicable research designs with the use of a questionnaire as the most suitable survey tool. The questionnaire was developed to determine whether the critical success factors identified through the literature review in Chapters 2, 3 and 4 of the study are indeed critical and important to the adoption of the proposed unified fraud management and digital forensic approach. The chapter that follows will provide an overview of mobile applications.

2. AN OVERVIEW OF MOBILE APPLICATIONS

2.1. INTRODUCTION

In recent years, mobile technologies and applications have become pervasive, seeping into every aspect of people's personal and professional lives. Research shows that users are now spending 2 hours and 42 minutes per day on mobile devices as of March 2014, which is up from 2 hours and 38 minutes in the preceding year (Khalaf, 2014); mobile application usage accounts for 2 hours and 19 minutes of that time spent. Such findings tell a clear story that applications, which were considered a mere trend a few years ago, are now dominating the mobile industry that was inherently conceived for mere communication.

Organisations throughout are adopting mobile technologies for numerous applications to capitalise on the mobile revolution. This means that they are now able to increase their operational efficiency as well as responsiveness and competitiveness, and most importantly, meet new growing customers' demands. For example, businesses are able to offer banking and travel services that are unique to the user's requirements. Although mobile technologies and applications present many new opportunities, they also present development and implementation challenges. There are many ways the mobile channel benefits both businesses and consumers; for example, the ability to initiate a transaction from anywhere, and easier ways to make payment are just a handful of examples of how the mobile channel adds value. In each year of the Mobile Payments & Fraud Report (Kount, 2015), respondents were asked to rank the four primary areas where they see mobile providing the most value from most to least important. These four primary sources of value were as follows:

- **Convenience:** making it quick and easy to pay from a mobile device
- **Opportunity:** increasing leads and sales generation into all channels
- **Conversion:** generating up-sell opportunities and location-based promotions
- **Loyalty:** increasing consumer loyalty, leading to higher retention and lifetime value

The preceding chapter provided an introduction and background to the study. The objective of this chapter is to explore and characterise mobile applications as well as identify the various challenges faced by their usage from a fraud risk perspective. In doing so, an answer it being provided to the first research question of this study, which is: “What is the threat landscape of mobile applications with regard to their architecture?” The chapter forms the basis for the justification of the need to suggest a unified fraud management and forensic model for mobile apps, which is the main contribution of this research. Section 2.2 provides an overview of mobile applications as they are known today. The section goes into details about the growing trends in mobile applications, including the diversity of application types, their impact on the enterprise and consumer. In addition to the overall trend analysis, Section 2.3 goes on to study the architecture of a mobile application as well as the threat landscape associated with each layer identified. In Section 2.4, key scenarios where mobile apps are used for fraudulent activities are identified.

2.2. MOBILE APPLICATIONS

Mobile applications, often referred to as mobile apps, are software designed to run on smartphones, tablet computers, and other mobile devices. They support a much wider range of activities than desktop applications and leverage information about a user’s environment to provide novel capabilities such as context awareness (Kim & Gelog, 2013). Their wide use is due to the richness of their functionalities, including user interfaces for basic services such as messaging telephony, as well as advanced services such as mobile payments and mobile transactions for applications in the banking industry (Kirubakaran & Karthikeyani, 2013). Because of their reliance on mobile technologies for performance, mobile applications are somewhat architecturally different from their desktop counterparts as discussed in the following subsection.

2.2.1. Characteristics of mobile applications

Besides the fact that mobile applications are designed to run on mobile devices, they have a range of common characteristics identified from the literature and summarised as follows:

Connectivity: Some mobile applications may require network connectivity (mostly internet) to operate effectively. This allows user-specific information or notifications, such as software upgrades, to be pushed to the application as and when they are available, rather than being actively called (Radia, et al., 2012). Natchetoi (2008) refers to this as proactive data feeding, which is the ability to store and retrieve server information even when the connection is down. With the growing number of apps on tablets and smartphones, this push functionality becomes critical to providing end users with up-to-date enterprise information and services.

Convenience and simplicity: Mobile applications are mostly identified by their convenience. They operate on devices with limited form factors (e.g. small screen size) and can adapt easily to the physical mobile device's resolution (Teng & Helps, 2010). This means that the information architecture and the overall usability must be implemented with care to create a fitting and simple interaction flow that is able to properly portray the offerings of a business. The user interface of an application will have a huge effect on how easy it is to use regardless of the device being used. Although bigger screens are becoming popular nowadays, the screen sizes of mobile devices are still small compared to computers and notebooks. Organisations now ensure that navigating and manipulating their app on any device is effortless; otherwise, users will look for an alternative mechanism that can provide something better.

Supported devices: There are hundreds of different mobile devices, with varied vendors, with different software features and hardware components. Organisations design their applications to be compatible with most devices in order to provide a consistent user experience across platforms (Sangwhan, et al., 2009).

Security: One of the most important issues in every business context is security, which consists of many facets. For example, Guo, et al. (2011) note the importance of ensuring that the data transferred over the network is encrypted through the carrier network. As some applications sync data with online, web-based applications, the storage of this data on the server must also be secured. Another facet can be that of the protection of the device itself. Organisations would want to ensure that no one but the legitimate user can access the application and the sensitive data associated with it. The research touches on the concept of fraud management and digital forensics, in Chapters 3 and 4.

Context aware: The increase of powerful mobile devices provides a great opportunity for context-aware mobile applications to become mainstream (Paspallis & Papadopoulos, 2013). Dey (2001) describes the term context aware as any information that can be used to characterise the situation of an entity. For example, applications are able to derive the location of a person, their type of connectivity, and nearby devices. This feature might not make sense for every application but can be useful in creating a good experience for the user.

Reachability: Reachability covers a more social attribute given by the nature of mobile applications themselves. A good application can be used anywhere, at any time. The same is true of applications where reachability is understood as availability in terms of updated and recent information and continuous usefulness. Examples of this attribute include actual content around the clock, time-aware options or even context sensitivity (Paspallis & Papadopoulos, 2013) as described in the characteristic above.

Speed: Since mobile apps are supposedly designed for use in mobile devices, good mobile apps should be fast and reliable. Their processes are normally executed with very little lag time, providing quick and seamless usage.

The success of a mobile application is best judged based on how well it performs a valuable task in terms of realising its functionality (i.e. it is useful) and in aligning with a business or consumer purpose or goal; how well it uses technology to deliver high quality and good performance; and how well it is accepted by users as being user-friendly, secure, powerful, and satisfactory to use. Successful mobile applications are useful, deliver excellent performance, and are easy to use while providing a relatively secure model for usage (Radia, et al., 2012). The aforementioned attributes may be general features and characteristics but play a vital role in mobile applications. Almost every software service provider can offer application development services, but only a few mature companies seriously care about these characteristics and features to give the ultimate mobile app to the end user.

Mobile applications essentially can be viewed as an extension of existing distributed computing types which just add mobility to host systems. The next section of the chapter describes the type of mobile applications and their use. The purpose of the section is not to identify the best approach, but rather to discuss the inherent benefits and limitations that each mobile application carries.

2.2.2. Types of mobile applications

When developing mobile applications, two main alternatives exist regarding implementation technology; either an organisation goes for native applications, or they deliver a mobile web in the form of web apps. Furthermore, there is a third type of app that is referred to as a hybrid application. Each approach carries inherent benefits and limitations, and some of the differentiating factors are further discussed in the subsections that follow.

2.2.2.1. Native applications

A native application is developed for a specific platform with predefined device models and a set range of operating system versions. These are applications that are downloaded onto a mobile device and run as a standalone application. Native applications can interface with the device’s native features, information and hardware such as the camera, for example (Granlund, et al., 2013). Limitations include the fact that users of native apps are required to manually download and install software updates. Native applications are typically more expensive to develop because they support multiple devices. Moreover, supporting these different platforms with multiple code bases accounts for a higher cost in maintenance. Native apps typically perform faster than mobile web applications and can be found in app stores. The app store approval process of a native application helps assure users of the quality and safety of the application (Bettini & Price, 2011).

2.2.2.2. Web applications

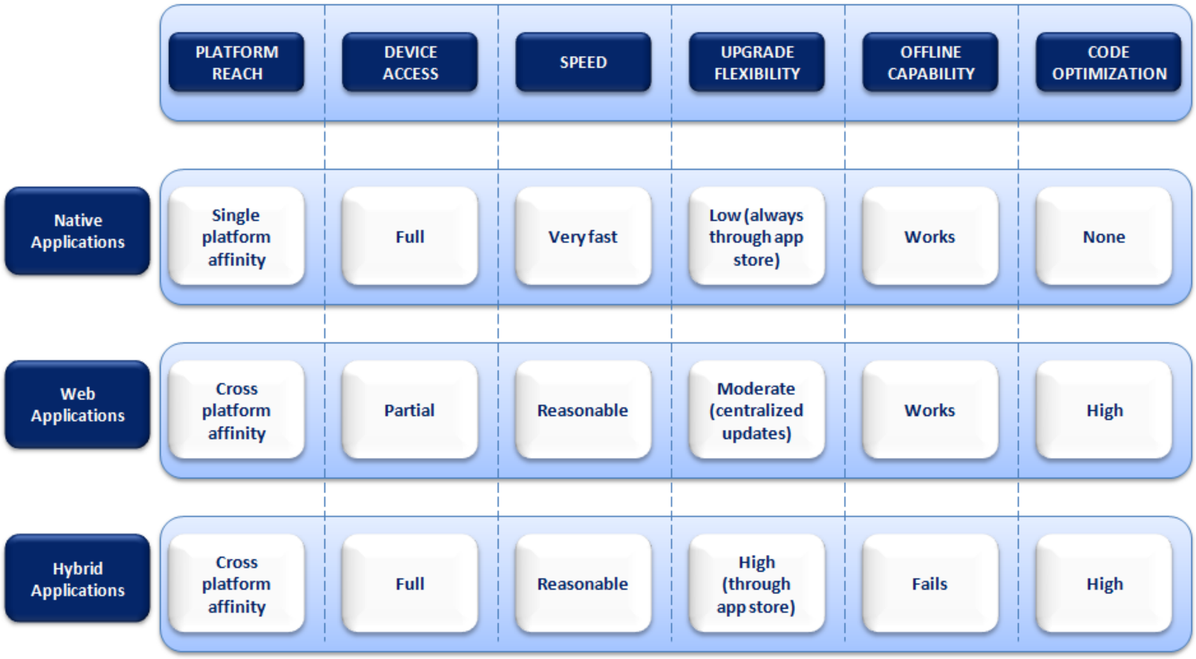
A web application, on the other hand, is developed using web technologies, thus accessible from a mobile web browser independent of device model or operating system (Granlund, et al., 2013). These are applications that are accessed through a mobile device’s web browser. The capability of a mobile web application allows it to access a limited amount of the device’s native features and information (e.g. orientation, geolocation, and media). Software updates/upgrades are made to the web server without user intervention (Park, et al., 2009). Similarly to native applications, web applications that support multiple web browsers may also result in higher development costs. Mobile web apps are also strong in the sense that they have a common base across all platforms. Unlike native applications, web app users do not have to go through a store to download or access the application, and these apps can be released in any form and at any time without approval.

2.2.2.3. Hybrid applications

A hybrid approach combines native development with web technology (IBM, 2012). Hybrid applications are written with the same technology used for websites and mobile web implementations, and they are hosted or run inside a native container on a mobile device. This means that the software runs on a device’s internal software but utilises web connectivity to accomplish certain tasks, such as syncing contacts across devices.

One of the advantages of these app types is that a mobile web developer can put the application – making it accessible – and make it a native application that can be installed or purchased by the end user. One of the more popular hybrid applications in use today is the LinkedIn mobile application.

Figure 2.1 depicts a graphical representation of the differences between the three types of applications discussed.



	PLATFORM REACH	DEVICE ACCESS	SPEED	UPGRADE FLEXIBILITY	OFFLINE CAPABILITY	CODE OPTIMIZATION
Native Applications	Single platform affinity	Full	Very fast	Low (always through app store)	Works	None
Web Applications	Cross platform affinity	Partial	Reasonable	Moderate (centralized updates)	Works	High
Hybrid Applications	Cross platform affinity	Full	Reasonable	High (through app store)	Fails	High

Figure 2.1: Native vs. Web vs. Hybrid applications
Source: Cavazza (2011) and IBM (2012)

Although hybrid applications may appear to be the ideal situation, they may become cumbersome and may create more overheads for developers. They may also create performance bottleneck depending on the type of application to be developed. In general, native apps are best suited for applications that make extensive use of mobile device native features (e.g. battery, geolocation, and camera). Web applications, on the other hand, are best suited for those applications that require a limited use of mobile device features. These applications, for example, make use of cloud-based enterprise data for service provisioning with very few or even no mobile device feature use. Finally, the hybrid type is good when combining both: developing an application that uses mobile device features and also enterprise cloud functionalities.

2.2.3. Categories of mobile applications

According to research, the number of smartphones in use worldwide exceeded the one billion unit mark for the first time ever in the third quarter of 2012 (Kirubakaran & Karthikeyani, 2013), and it was estimated that the next billion in smartphone usage might be achieved in less than three years, by 2015[1]. Mobile applications such as Short Messaging Service (SMS) and Multimedia Messaging Service (MMS) clients and browsers come preinstalled on mobile devices. While these were initially developed mostly in the entertainment sector, they are now touching more critical domains which will be explored in more detail below.

Retail: Retail businesses are building mobile applications that do more than just display products for sale. The applications are built to shape the in-store experience, empower purchasing processes, and create interesting and dynamic ways to interact with the customer. Furthermore, these are mobile applications that help retailers operate their businesses.

Media: Media type applications are those communication channels through which news, entertainment, education, data, or promotional messages are disseminated. These software programs are used to create multimedia works, including both artistic and commercial works. Examples of these types of applications include magazines, newspapers, graphics/image viewers, and audio/video players.

Finance: Personal finance apps extract real-time data from financial service providers such as banks, investment houses, lenders, and credit card companies, and have the ability to depict an accurate portrait of the user’s finances on the fly.

[1] At the time of writing this dissertation the estimate was achieved as per (Statista, 2016).

Social: Mobile apps are also very prominent in social networking, where they foster collaboration with other enterprises or individuals of interest. These apps allow device users to access their favourite social media sites where they can post updates and view their friends' activities. These apps offer personalisation for users accessing information and applications, thus enhancing user satisfaction.

Productivity: Another common type of mobile application can be broadly categorised as organisation-based. These apps allow users to handle meetings and appointments through calendar programs, take notes through word processor apps, and write out memos such as shopping lists. Notable applications of this type include calendars, calculators, address books, task managers as well as file managers.

Further categories of mobile applications can extend to travel, where one can make airport bookings, for example; education mobile apps, where lessons are available through these apps; and even healthcare applications that allow patient records and notes to be viewed and managed. Figure 2.2 takes a closer look at mobile application categories and which ones remained popular during the research period. Social messaging apps grew to 28% of time spent on a mobile device, which indicates the broader shift to sharing within small, more private messaging applications (Khalaf, 2014). Entertainment (including YouTube) and utility apps are at 8% each, while productivity apps doubled at 4% usage. The overall usage of mobile devices for the year 2013 was through applications (86%), while a normal browser was only utilised by 14% of the sample size. For the purpose of this study, the research will only focus on the use of mobile banking applications from a security perspective.

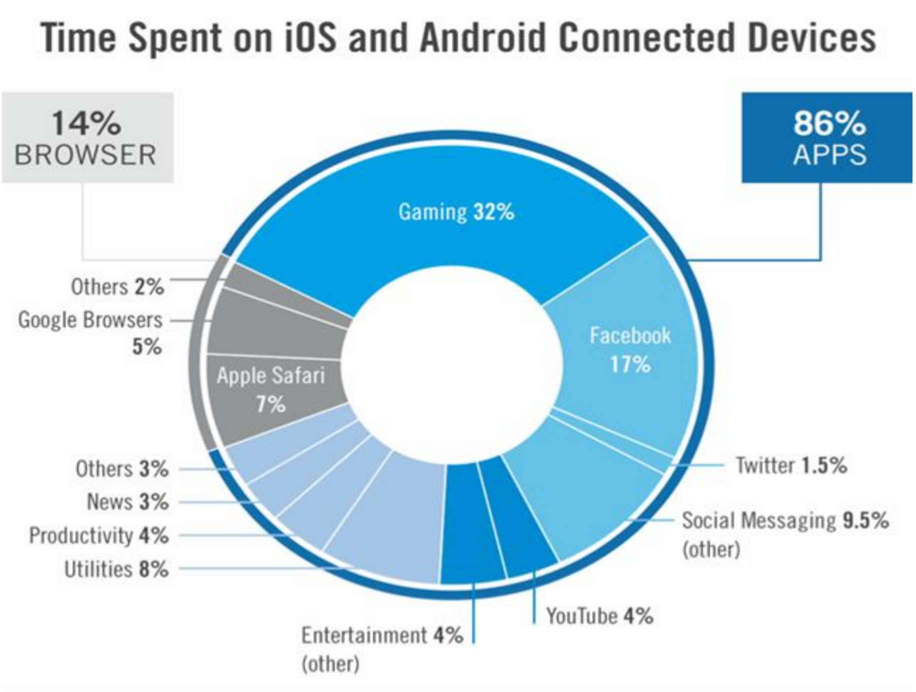


Figure 2.2: Time spent on iOS and Android mobile devices
Source: (Khalaf, 2014)

It is clear from Figure 2.2 that organisations face a strong demand for innovative mobile applications to dramatically improve customer engagement. Additionally, the demand is growing for mobile versions of existing desktop and web-based applications. In response to this, enterprises are seen embarking on several mobile application development projects. One of the first steps for development of any mobile application is selecting the right client architecture. A mobile application will normally be structured as a multi-layered application consisting of various layers. The next section of the study explores this in more detail.

2.3. MOBILE APPLICATION ARCHITECTURE

From a technology perspective, mobility shifts the global computing infrastructure from static, homogenous desktop computing to highly dynamic, heterogeneous, resource-constrained handheld and wearable computing (Kim & Gelog, 2013). Mobile applications have grown to support a much wider range of activities than desktop applications and are built to either extend an existing business system or interface with it. This new computing context demands entirely new software architectural paradigms that address the challenges of mobile application fraud. A mobile application will normally be structured as a multi-layered system consisting of a user interface, a business layer, and data layers. Figure 2.3 illustrates a common mobile application architecture with components grouped by areas of concern.

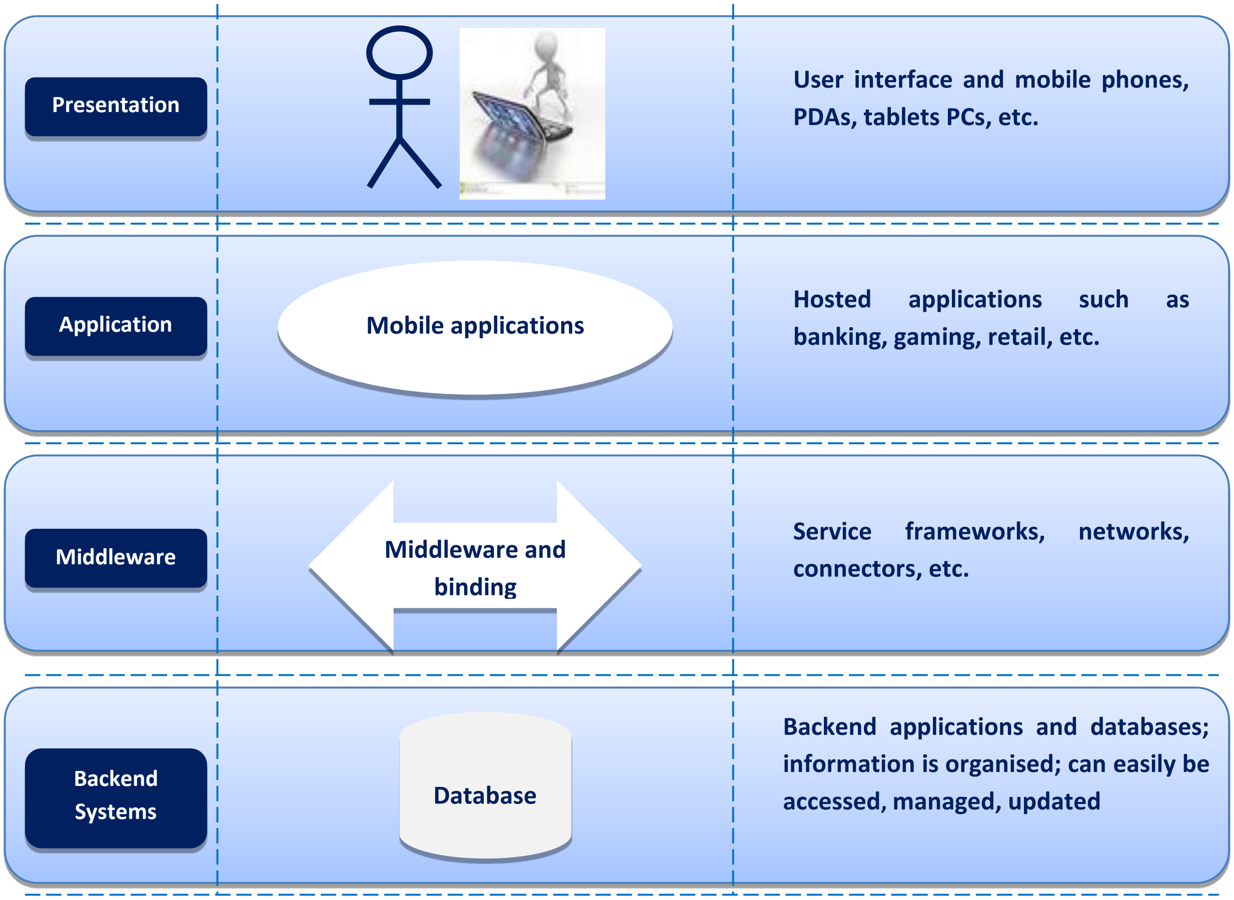

Presentation
User interface and mobile phones, PDAs, tablets PCs, etc.
Application
Mobile applications
Hosted applications such as banking, gaming, retail, etc.
Middleware
Middleware and binding
Service frameworks, networks, connectors, etc.
Backend Systems
Database
Backend applications and databases; information is organised; can easily be accessed, managed, updated

Figure 2.3: Mobile application architecture
Source: Unhelkar and Murugesan (2010)

2.3.1. The presentation layer

The presentation layer represents the user interface in mobile devices. It is fundamentally the medium by which end users access the entire system in order to undertake some business-related tasks/activities. Various such medium can be used to access the entire system within an organisation. A simple example of the presentation layer with reference to the banking industry is the interface by which end users operate to undertake internet banking transactions. Upon installing and registering for the usage of such internet banking application, an invocation of the application through the device provides an interface whereby the user can perform a range of activities, mostly those of invoking their transactional requests/queries for further processing by a layer down the hierarchy.

2.3.2. The application layer

The application layer represents the hosted application, such as banking, which is intended to support the main functionalities of the existing system by allowing accessibility via a mobile device. The layer holds a range of functionalities geared at catering for end users’ needs depending on the intended transactional request of the user. In the banking industry, typical features and services available in this layer include, but not limited to, balance enquiry, viewing statements, transfer of money between accounts, making payments to beneficiaries, and purchases of prepaid airtime and electricity (Njenga & Ndlovu, 2012).

2.3.3. The middleware layer

It represents service frameworks and network connectors. This layer of the architecture provides data transformation and is the central point of communication between a device and the corresponding backend resources (legacy systems, third-party systems or databases). Additionally, the middleware may provide security enforcement mechanisms in order to ensure that services requested at the application layer warrant the necessary authorisation. It is thus comprised of functionalities for challenging end users while accessing certain backend services. In addition to the foregoing, requests to the backend are also managed by the middleware layer in order to ensure that appropriate queries/requests are channelled to relevant backend services. In other words, the middleware layer binds the application to the content and leads to a more consistent way of handling the information (Unhelkar & Murugesan, 2010).

2.3.4. The backend systems layer

This layer represents the backend applications and databases where the actual data is stored. These systems perform the core functions of organisations' operations and contain core information and business rules. The information layer is responsible for manifesting a unified representation of the information aspect of an organisation (such as metadata, master data, and structured data) as provided by its applications (in this case mobile) and systems (The Open Group, 1995).

Although mobile devices are quickly evolving due to technological breakthroughs, they are still highly vulnerable to a number of fraud risks which can target any layer of the architecture. A successful attack to the entire application or the layers thereof can cause immense financial, operational and reputational damage to an organisation. Some key threats are discussed below.

2.3.5. Threat landscape

The deployment of mobile technologies can present a significant amount of risk to the overall enterprise security posture. Mobile devices and applications have numerous vulnerabilities that are susceptible to malicious attacks as well as non-malicious internal threats. From the types of networks the mobile devices use to the threat of data loss, mobile devices have no shortage of inherent risks. Table 2.1 summarises the 10 top mobile risks (Kesäniemi, 2012).

#	Mobile risks	Concerned layer
1.	Insecure or unnecessary client-side data storage	Presentation, Application
2.	Lack of data protection in transit	Application, Middleware, Backend
3.	Personal data leakage	Application, Middleware, Backend
4.	Failure to protect resources with strong authentication	Presentation, Application
5.	Failure to implement least privilege authorisation policy	Backend
6.	Client-side injection	Presentation, Application
7.	Client-side denial of service	Presentation, Application
8.	Malicious third-party code	Application, Middleware, Backend
9.	Client-side buffer overflow	Presentation, Application
10.	Failure to apply server-side controls	Middleware, Backend

Table 2.1: Top 10 mobile application risks
Source: Kesäniemi (2012)

To better describe these top 10 mobile risks, each risk has been mapped to a layer of the mobile architecture where the risk is more prevalent. Over and above the above-mentioned risks, some of the key threats to mobile applications also include the following:

Physical theft: The very portability of mobile devices makes them physically easy to steal. The owner of a stolen phone could lose all the data stored on it – not only personal data but also identifiers to financial and corporate data. A sophisticated attacker can defeat most security features of mobile phones and gain access to any information stored (Ruggiero & Foote, 2011).

Phishing: This is the most familiar threat term among smartphone users. One of the primary threats of phishing is identity theft, which involves the fraudulent acquisition of sensitive personal information by sending official-looking e-mails impersonating a trustworthy sender.

Open connectivity: The number of smartphone users has increased, and with it the use of data transmission networks such as Wi-Fi, Bluetooth, and infrared. This high degree of connectivity in combination with the mobility of the device increases the attack surface and opens a whole new family of threats (DeWin, et al., 2009).

Spyware: These are software designed to collect or use private data without the knowledge or approval of the user. The common data targeted by a spyware includes phone call histories, text messages, browser history, user location and other information that could be used in committing financial fraud.

Networking exploits: Networking exploits are those that take advantage of flaws in the mobile operating system, software that operates on local or cellular networks. Once connected, they can install malicious code on a mobile device.

Trojan horses: A Trojan horse is a malicious software program (malware) that masquerades as legitimate software (Dai, et al., 2011). Malware can be installed by worms or viruses, or unknowingly by the user, thinking the software is a game or even a browser plug-in. Other types of malware may make attempts to make changes on a user's phone bill, send malicious messages to a contact list, or give the attacker control over your mobile smartphone device without a user's knowledge.

Interception: Middleware technologies have the potential to weaken applications' barrier to entry. The data in transit between the mobile device and the server of an existing system, or between two devices, may be intercepted and then gain unauthorised access to sensitive data (Gadhiya & Wandra, 2009).

Denial of service: Because of resource limitations, mobile device platforms often contain very poor process management models (DeWin, et al., 2009). Therefore, simply feeding a badly written application with corrupt data that causes it to crash or hang can often bring the whole system to a halt, forcing the user to reset its device.

Hacking: Application-specific hacks have become even smarter. Many organisations are alert to the threat posed by so-called buffer overflows, the techniques by which web servers are overloaded, causing a denial of service attack. By feeding a vulnerable application a carefully crafted input, an attacker can overwrite certain memory locations in the system. This enables the attacker to execute arbitrary code, potentially resulting in system compromise (DeWin, et al., 2009).

SQL injection: SQL injection forces a database to yield otherwise secure information by causing it to confuse classified data, such as passwords or blueprints, with information that is for public consumption, such as product details or contacts. This has a direct impact on the confidentiality, integrity and availability of the data stored in the database providing this information.

As per the threat landscape already discussed, the nature of the mobile application architecture suggests that vulnerabilities can be exploited at any layer of the architecture. While the presentation layer is mostly concerned with identity theft and access to personal historical data that resides on the device, the most common entry point of vulnerability – once the hacker has passed the presentation layer – is often at the middleware layer. In this case, since its role is to channel end users' request to the relevant backend, a middleware that is not designed to handle further security features, making use of sophisticated mechanisms (using context awareness for example), will consider any frontend request as legitimate. If this is the case, access to backend systems layer will be open to a plethora of malicious and improper use of the system and unauthorised access to corporate data. To overcome this challenge, yet another level of security can be put in place at the backend level so as to ensure that information being accessed is genuinely triggered by the authorised end user.

2.4. CONCLUSION

As mobile applications continue to take a central role in people’s lives, organisations around the world are mobilising a growing number of mission-critical services. The challenges that lie ahead of us are manifold. First, given the fact that these devices constitute a core part of people’s daily lives, and since they impact both business and personal life, information security on these devices is becoming a critical success factor. This chapter first started by introducing mobile application types as well as the common uses of these applications that are apparent in people’s today lives.

Most organisations are striving to find the optimal development approach to achieving their goals, but what many quickly come to realise is that each approach carries inherent limitations and no single approach can address all growing needs and complexities of the modern mobile enterprise. This was seen at the beginning of the chapter, where the research explored the different types of mobile applications. The chapter then went on to discuss the various layers that would exist in a typical mobile application architecture as well as the threat landscape thereof. It was discovered that many known threats to normal computers target server processes that offer a certain network service. The focus of the threats on mobile devices, therefore, shifts completely from servers to applications. From a security and fraud perspective, this means that new efforts need to be spent on preventing the success of fraudulent behaviour used through these devices. Furthermore, the close connection between mobile devices and their users and the system to which they are connecting should warrant more research on improving fraud detection and, in particular, the prevention thereof.

Having answered the first research question in this chapter and being equipped with knowledge on the threat landscape of mobile applications aligned to their generic architecture, the next two chapters will focus on exploring fraud management and digital forensic approaches with regard to mobile applications.

3. REVIEW OF FRAUD MANAGEMENT APPROACHES

3.1. INTRODUCTION

With the welcome growth in mobile device usage, organisations need to manage the increased risk associated with the mobile channel. Organisations looking to mitigate mobile fraud risk should address complex, cross-channel attacks and the unique challenges presented by the mobile channel, as discussed in Chapter 2. Fraud is a pervasive corporate problem that affects organisations of all sizes around the world. The cost of fraud can be very high, both from actual money lost and the consequent erosion of public confidence from a reputational risk point of view.

The general practice of fraud management is about fraud prevention, detection, examination and investigation. These are all well-defined disciplines; however, all these features seldom exist in entirety in the current fraud management models in order to succeed. A number of surveys have documented the increasing incidence and cost of fraud against organisations (Litan, 2011). In addition to the financial cost incurred by the victims, the cost of fraud includes reputational and financial costs arising out of litigation against enterprises that fail to detect fraud. No single layer of fraud prevention is enough to keep determined fraudsters out of critical systems or applications. While absolute proof of mobile application fraud may be difficult to obtain, there are many measures that can be used to track user accounts or profiles so that potentially fraudulent activities can be flagged and investigated further.

The foregoing chapter provided an overview of mobile applications. The primary objective of this third chapter is to explore the literature on various fraud management models for mobile applications within the current body of knowledge. The review seeks to extract and study advantages and limitations of the models explored. The chapter is structured as follows: Section 2 of the chapter provides a definition and an overview of fraud and the fraud management lifecycle. The third section of the chapter then provides a review of existing fraud management models, frameworks and approaches as well as their advantages and disadvantages by grouping them through similar use. The last section will then produce a summary of the findings considered to be aligned to the mobile application architecture presented in Chapter 2.

3.2. OVERVIEW OF FRAUD

As discussed in the previous chapters, methods of attempting fraud are ever changing with the advances in technology adoption by organisations. All organisations are subject to fraud risks. Various frauds have led to the downfall of entire organisations, massive investment losses, and erosion of confidence in capital markets, which has negatively had an impact on their reputation. Searching for predefined patterns no longer assists in finding previously undiscovered knowledge about fraud. As a result, fraud detection methods and systems are continuously developing in order to stop criminals from adapting to their strategies. To understand the intricacies that come with detecting fraud through mobile applications, it is essential to understand the concept of fraud management and what fraud management models and approaches aim to achieve.

3.2.1. Definition of fraud

Fraud can be defined as

- any intentional act committed to secure unfair or unlawful gain (KPMG Forensic, 2006);
- any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain (Bishop, et al., 2010); and
- the use of deception to unjustly obtain a benefit (State audit institution, 2011). The benefit obtained does not always have to be money but could very well be in the form of services, information or corruption, which involves the abuse of power for personal gain.

Using the aforementioned definitions, the study identifies fraud as

any deliberate, deceitful conduct or omission designed to gain an advantage to which a person or entity is not entitled. It is the intentional use of false representations or deception to avoid an obligation or to gain an unjust advantage.

The following are examples of fraud:

- the theft or deliberate misuse of an organisation’s assets;
- the use of false statements or identity to obtain a benefit (e.g. a fraudster claiming to represent a bank); and
- the unauthorised use of an organisation’s name or authority to gain personal benefit.

Some other examples of fraud include the destruction, removal, or inappropriate use of an organisation’s records, or any other dishonest or fraudulent acts (e.g. insider trading, discrimination, and theft of competitors’ secrets).

3.2.2. The fraud triangle

The concept of a ‘fraud triangle’ was introduced in the literature by the Auditing Standards Board (American Institute of Certified Public Accountants (AICPA), 1997). It is a model for explaining the reasoning and factors behind an individual’s decision to commit fraud. The three stages are categorised by the effect on the individual and in order for fraud to occur; all three elements must be present (Cressey, 1953). Figure 3.1 depicts the fraud triangle, which describes three factors that are present in every situation of fraud.

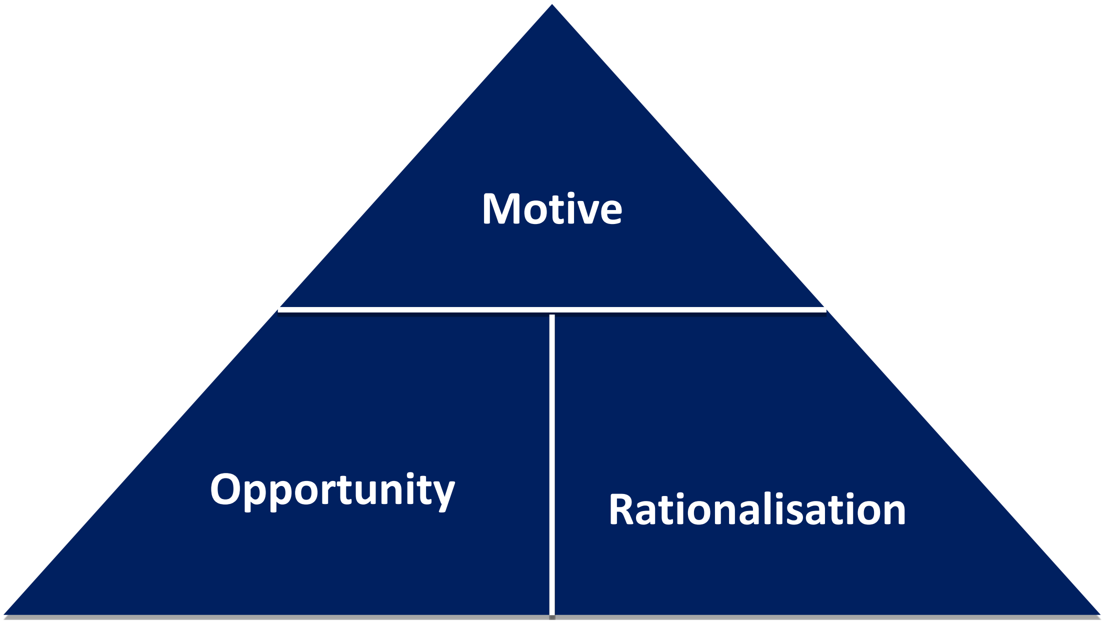


Figure 3.1: The fraud triangle
Source: Cressey (1953)

Motive, also referred to as ***pressure*****:** The first element of the fraud triangle represents the motive, that is, the reason that causes a person to commit fraud. Pressure can include almost anything, for example, a gambling debt, and most of the time comes from a significant financial need/problem. However, some frauds are committed simply out of greed alone (Lou, et al., 2009).

Opportunity: Opportunity is the situation that enables fraud to occur. Opportunity is the ability to commit fraud and defines the means and method by which the crime may be committed. Because fraudsters do not wish to be caught, they must also believe that their activities will not be detected. Opportunity is created by weak internal controls or poor oversight. Failure to establish adequate procedures to detect fraudulent activity also increases the opportunities for fraud to occur (Turner, et al., 2003). Of the three elements highlighted in Figure 3.1, opportunity is the leg that organisations have the most control over.

Rationalisation: The third element of the fraud triangle represents the mindset of the fraudster that justifies them to commit the fraud. Rationalisation involves a person reconciling his/her behaviour with the commonly accepted notions of decency and trust (Aghghaleh & Mohamed, 2014). Some common rationalisations for committing fraud are the following:

- The person believes that no help is available from outside.
- The person believes that something is owed to him/her.
- The person is unable to understand or does not care about the consequence of their actions or of accepted notions of decency and trust.

3.2.3. Fraud management lifecycle

A fraud management approach is a process of coordinated measures put in place by organisations to prevent, detect and respond to any instances of fraud (State audit institution, 2011). Although each organisation will establish its own specific procedures, effective fraud management has to start with a common understanding of the stages of the fraud management lifecycle. Therefore, a common fraud management lifecycle typically consists of the key components illustrated in Figure 3.2.

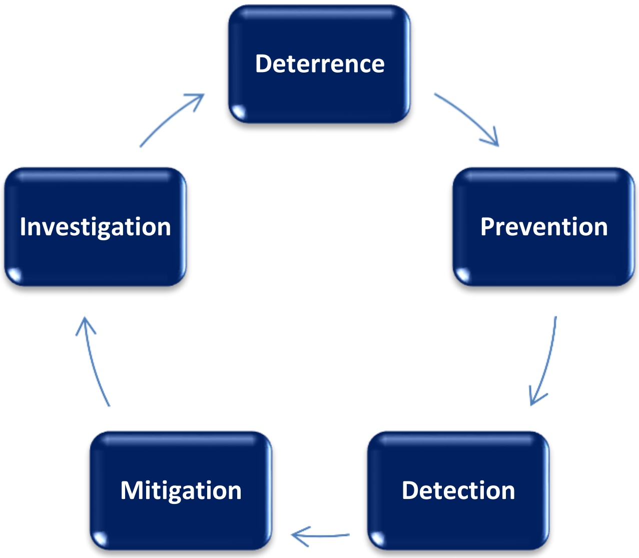


Figure 3.2: Fraud management lifecycle

Fraud deterrence: Fraud deterrence involves eliminating factors that may cause fraud, i.e. fraud deterrence is the one that stops the fraud before it happens. This first stage of fraud deterrence consists of actions and activities intended to stop or prevent fraud before it is attempted by either discouraging or making it impossible through increasing the difficulty of the fraud attempt (Wesley, 2004). Breaking the fraud triangle is the key to fraud deterrence and implies that an organisation must remove one of the elements in the fraud triangle in order to reduce the likelihood of fraudulent activities. Examples of fraud deterrence in relation to mobile applications include the use of algorithms to respond quickly, equitably, and proportionately to violations, investigating and remediating problems as and when they arise, as well as maintaining internal and external auditing processes within the entire mobile architecture value chain.

Fraud prevention: Fraud prevention means having arrangements in place that reduce the risk of fraud occurring. Many international studies (State audit institution, 2011) have shown that prevention is the most cost-effective way to prevent loss through fraud. Preventing fraudulent conduct from occurring in the first place is much better than trying to detect fraud after it has already happened. This may include putting strong control measures for authentication and authorisation when clients access services through mobile applications and ensuring the protection of information at rest as well as in transit between the various layers of the mobile architecture.

Fraud detection: This stage of the fraud management lifecycle focuses on activities and techniques that promptly recognise in a timely manner whether fraud has occurred or is occurring. The best forms of fraud detection come from aware and vigilant individuals who know where to go and what to do if fraud is suspected. Two types of fraud detection techniques exist: deductive fraud detection, which proactively searches for fraud without determining the type of fraud to look for; and inductive fraud detection, which determines the types of frauds that can occur and then queries the data set to see if they exist (Kirkos, et al., 2007).

The two fraud detection techniques, deductive and inductive, are briefly discussed below.

- A deductive fraud detection technique, for example, would analyse an organisation’s operations and use industry and knowledge to search for the highest fraud areas. As a result, specific types of frauds are identified, not just the symptoms of the fraud.
- An example of an inductive fraud detection method is data mining, which is discussed in detail in Section 3.3, which analyses data in the backend systems layer of the mobile application architecture. This data can then be used to uncover abnormal patterns in behaviour, perform trend analysis, as well as discover the relationship between various fraud types.

Fraud mitigation: Mitigation of fraud has to do with responding to the incident – either to stop losses from occurring or even delay a fraudster from continuing or completing the fraudulent activity. A fraud mitigation plan may describe the approach to controlling fraud, which includes the actions to be taken to reduce the fraud risks identified. An example of a fraud mitigation strategy is that of blocking the mobile transaction immediately and alerting the user of the action taken. This first prevents the fraudster from committing further crime and alerts the legitimate user of a problem on their account.

Fraud investigation: The process of investigation is focused on information acquisition and verification. The information gathered is either to stop fraudulent activity or to support the successful prosecution and conviction of the fraudster(s).

The fraud management lifecycle, in essence, involves developing a solution that an organisation puts in place to manage one or more fraud incidents from the beginning to the end. Research conducted (Wesley, 2004) further includes three stages in the cycle that aid the complete management and control of fraud: fraud analysis, where fraudulent events are analysed to determine the root cause of the incident; fraud policy, which consists of rules and activities to create, evaluate and communicate the deployment of guidelines and procedures to reduce the incidence of fraud; and fraud prosecution, which includes asset recovery, criminal restitution, and conviction.

Organisations strive to protect their business and their reputation through protecting their customers by taking the right measures, at the right time. The discussion that follows covers the fraud management models, approaches and frameworks found in today’s existing literature.

3.3. A REVIEW OF FRAUD MANAGEMENT APPROACHES

A survey (Drake, 2008) suggests that 70% of enterprises are currently deploying at least one mobile application and that smartphone sales accounted for 55% of overall mobile phone sales in the third quarter of 2013 (Gartner, 2013). Mobility is both an opportunity and a challenge because of a large collection of devices with an increasing number in the development of mobile applications. Considering the condition today, mobile devices have become a way of life for many people.

One of the many contributing factors to fraud exposure is that organisations unintentionally sacrifice security when they rush to market with a strategy to take advantage of current consumer shopping trends, which now are more focused on the mobile experience than ever before. For the most part, the more sophisticated organisations have made a higher level of investment and understand the basics of mobile fraud and have implemented some kind of tools or in-house processes for detecting mobile fraud. There are a significant number of fraud management (FM) approaches specifically focusing on fraud in the telecommunications world. Although these methodologies approach the subject of fraud differently, their ultimate goal is to prevent and detect fraudulent activities and, as a result, reduce risk to an acceptable level. The goal is also to protect the organisation from reputational and financial damage. Only through diligent and ongoing effort can an organisation protect itself against significant acts of fraud.

In the following subsections, some of the foregoing methodologies and frameworks used for fraud detection and their applicability to the mobile application architecture will be explored, as described in Chapter 2. The section also aims to highlight the potential benefits that can be derived and relied upon for the suggestion of a unified fraud management and digital forensic framework, discussed in Chapter 5.

3.3.1. Fraud management models through user profiling

User profiling is the process of collecting information about a user in order to construct essential information about that individual (Hasan, et al., 2013). The information in a user profile may include various attributes of a user such as geographical location, academic and professional background, interests, preferences, as well as opinions. Users often have repetitive behaviours within software applications; these behaviours can be observed and stored in their individual profiles. There are typically two broad approaches that are used to understand user needs and behaviour. The first approach uses customisation techniques, where the user explicitly selects between options to indicate demographic, geographic, and other pertinent information (Prasad Kantamneni & Narayanan, 2001). The second approach is computer-driven profiling, which is driven by a computer software model of the user through the use of data mining and collaborative filtering technologies. The basic principle is to gather information about the user through multiple techniques by analysing, for example, the pages viewed during a session, items bought, and personal data provided by a user.

Research shows that identity and data matching, another form of user profiling, are often utilised to combat fraud conducted through mobile applications (Hall, et al., 2005). An accurate client profile that provides a unique identity and a true description of its associated business activities has become an increasing concern for organisations. Hall, et al. (2005) present a framework which makes use of an instant-based learning technique.

The process consists of the following components:

- High-level mapping: The process begins with a data collection exercise of the user's geographical location for a period of three to six months.
- Feature extraction: The extraction of geographic locations is then used to create mobility sequences of the user.
- Profile definition: Once the mobility sequences have been obtained, the next step is to create the user mobility profile (UMP), which includes a unique identifier for a user and their studied behaviour.
- Classification: The final step in the intrusion detection process is the classification of a set of mobility sequences, as normal or anomalous, using a noise-suppressed similarity measure to profile (NSMP) value. If NSMP value falls within the pre-established thresholds (also stored in profile), this set of mobility sequences is considered normal, belonging to a user; otherwise, an intrusion is suspected.

A further study introduces enterprise architecture to improve profile-based identity management (Yang, et al., 2010). The framework, as illustrated in Figure 3.3, uses a consistent method that depicts characteristics of various aspects about each client (i.e. an entity) based on truthful, accurate, and sufficient information from diverse sources, and consists of six components.

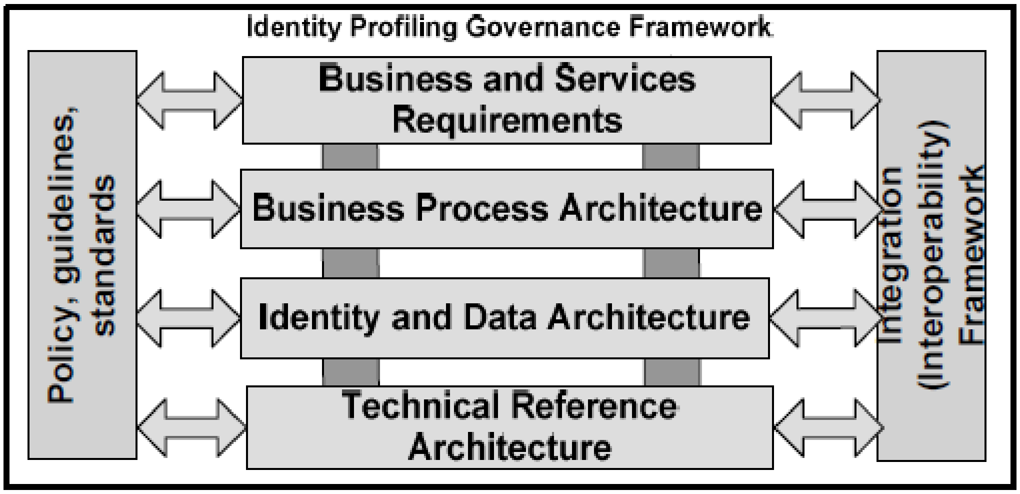

Identity Profiling Governance Framework
Policy, guidelines, standards
Business and Services Requirements
Business Process Architecture
Identity and Data Architecture
Technical Reference Architecture
Integration (Interoperability) Framework

Figure 3.3: Profile-based identity management framework
Source: (Yang, et al., 2010)

The various aspects of the framework in Figure 3.3 are elaborated below.

- Business and service requirements: The first layer of the architecture is where business rules and requirements are defined or changed to give responsiveness and agility. This function will monitor future trends in both individual and non-individual identities.

- Business process architecture: The second layer describes key business processes during client profiling activities that are defined by key departments in an organisation. For example, based on legislation, a particular rule may be created specifying that each client is dedicated a unique identity number.

- Identity and data architecture: The identity and data architecture layer is used to ensure translation of business requirements to operational processes. Data architecture describes the identity of data structures used by business application developers and support areas. It must also be able to deal with emerging and new requirements (e.g. combating new cybercrime) along with improved data and identity verification and e-fraud modelling.

- Technical reference architecture: The technical reference architecture component provides references to the existing technologies and related standards that are relevant to service providers' specific business environments.

- Policies, guidelines and standards: This component includes relevant policies, guidelines or management standards that define the appropriate behaviours that require attention.

- Integration framework: The final component ensures integration and interoperability of systems and applications. It specifies what areas/components need to be monitored, how often, where and by which business lines within the organisation.

Similarly, Compaq (2001) and Hewlett-Packard Company’s (2005) fraud management methods introduce anomaly based detection that observes and deviates from normal behaviour. Both these models employ user profiles which are built using calling patterns, frequency, and other behaviour-related information. The fraud management system (FMS) detects fraud by reading and analysing various defined streams of event information and then detects anomalies within the data in order to automatically generate alarms (Compaq, 2001). The system goes on to analyse these alarms and identify likely fraudulent behaviour. As part of its detection function, it builds individual profiles for each customer, which provide a longer-term view of how each customer uses their different services. This is used to enhance the accuracy of detection. The fraud management system detects fraud by reading and analysing the same streams of call detail records used for billing (Hewlett-Packard Company, 2005). As part of its detection function, the FMS builds usage profiles and tracks current usage at the customer or service level. Furthermore, the FMS detects anomalies within the data and automatically generates alarms that are analysed by the system to identify potentially fraudulent behaviour. The information is then presented to a fraud analyst/case manager using a graphical user interface.

Research (Prasad Kantamneni & Narayanan, 2001) describes profile-based identity on the basis that much richer user profiles can be obtained through consideration of the user’s context. This architecture is incorporated as an intermediary between the user and the application being used and uses two types of agents. The first agent is a dynamic client that resides on the user’s machine and unobtrusively studies user behaviour, while the second agent is a lookup agent which allows other applications to collaborate together and create a profile of the communities’ interests.

As can be seen in the research behaviour modelling is one of the most popular applications for fraud detection. Statistics and data mining methods have also been applied successfully to detect activities such as money laundering, e-commerce credit card fraud, telecommunications fraud and insurance fraud (Yue, et al., 2007). However, studying the behaviour of a user is not enough to mitigate this growing issue that is found in mobile application fraud. Edge, et al. (2007) propose a fraud management framework encompassing a rule-based Financial Fraud Modelling Language (FFML) for conceptual level modelling and validation of fraud policies and fraud prevention architecture based on implementing fraud policies.

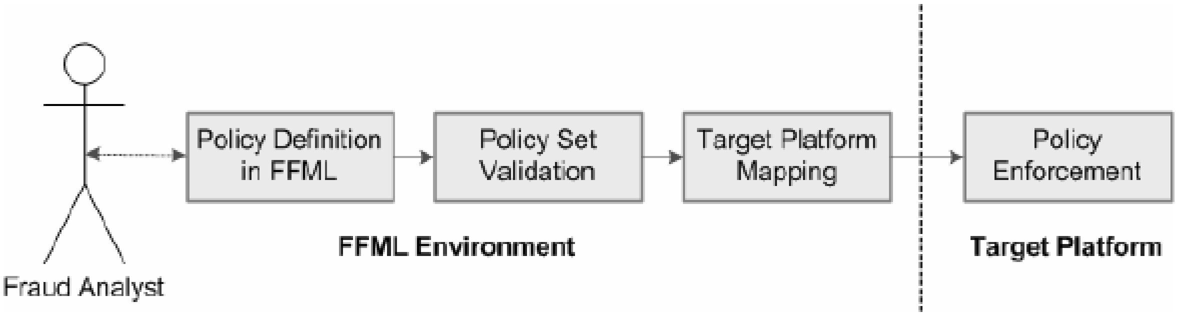


Figure 3.4: FFML Policy Processing Framework
Source: (Edge, et al., 2007)

A key element of the framework illustrated in Figure 3.4 is the attempt to detect fraud proactively, blocking transactions with suspicious click stream patterns. The framework's main function is the continuous monitoring of incoming click data which stores transactional behaviour and known fraudulent activity patterns to which preventive actions may then be initiated prior to transaction completion. The FFML language consists of language constructs that facilitate policy definition of rules, which consist of event sequences, conditional statements and action statements to formulate the rule (Edge, et al., 2007). This means that one policy may have multiple rules in it.

3.3.1.1. Advantages

Compare observed usage to profiled usage: Fraud management models that use user profiling as their mechanism for detection have the ability to use a longer-term detailed profile of each user to determine if observed behaviour is outside what is expected for that individual. This is to ensure maximum accuracy in the findings.

Reduced learning curve: A learning curve is a representation of the increase of learning that comes with experience. Neural networks are particularly effective at solving new kinds of problems whose solutions are difficult to define and, therefore, results in reduced time. Once the profiles are constructed, they are relatively straightforward to communicate to the users of the information.

Context adaptation: Fraud management models through user profiling present the ability to adapt to users' current context in real time so that the information used for detection is timely in nature and tied to the context of current user information.

Targeted: The last advantage of these models is that they focus on only one target, which is the group that has been previously designated as the one of primary importance. This makes it possible to focus on a single target rather than to fragment attention among several targets, as is the case with segmentation.

3.3.1.2. Limitations

High rate of false alarms: It is generally acknowledged that the main limitation of fraud detection through user profiling is that it generates a higher rate of false alarms. The challenge remains accurately characterising the mobility behaviour of users.

Incomplete data: Data can be incomplete, inconsistent, or even deliberately misleading. Data gathering can also be expensive; there are legal issues, especially involving privacy, that need to be considered. With that said, the set of identification attributes of a user are not always enough to properly distinguish a legitimate user from that of a fraudster.

Does not make use of scenarios: Another disadvantage of using profiles for fraud detection is that they often lead the investigator to concentrate on differences and thus ignore absolute levels of response (Stewart & Davies, 1997). From the response, an expert might conclude, for example, that a typical mobile banking application user only uses the application for airtime purchases and that the majority of transfers would occur over the Internet. As a comparison, the conclusion may be valid, but the temptation is to go even further here and conclude that this is not the case.

Forced combination: With group user profiling, there may be a forced combination of several different groups into one. This leaves no room for discovery for the anomalies or differences that may lie between the groups.

3.3.1.3. Summary

In conclusion, the main idea behind user profiling is that of gathering the past behaviour of a user in order to construct a profile of what might be the expected values of the user's behaviour (Hilas & Sahalos, 2005). Moreover, neural network technology is interested in fraud detection through learning of the interconnected units within data. The inherent nature of neural networks is being able to capture and represent complex relationships. Fraud management approaches of this type are best suited to three layers of the architecture stack, which are as follows:

- **Presentation and application layers:** Financial institutions, such as banks, want to minimise the risk of possible fraud occurring on users' accounts through detection. On the basis of extensive user profiling, customers are assigned a certain scoring value that aligns to their common activities; input to this value is conducted through the second layer of the mobile architecture.

- **Backend systems layer:** This type of approach is also best suited to the fourth layer of the architecture, which describes the backend systems where data is stored. In this layer, databases with transactions may be searched through the use of algorithms to find behaviours that deviate from the standard, indicating potentially suspicious transactions. Also, user profiling can automatically scale the difference between fraudulent and non-fraudulent activities as well as evolve over time to discover new user patterns and trend types in data.

3.3.2. A rule-based approach to fraud management

Most of today's fraud detection tools are either rule-based or at least comprise a rule-based detection component. A rule-based approach allows detecting the definite frauds with a low rate of false alarms. Moreover, the rule-based tool can easily provide reasons for an alarm being raised. Rule-based tools make use of the profiling strategy described in the previous section, and its features are similar to those of the supervised neural network discussed in the sections that will soon follow.

One of the key methods used in rule-based detection is data mining, which can be defined as the process of discovering valid and comprehensible knowledge from large data sources with the purpose of applying this knowledge to making decisions (Mata-Toledo, 2003). There are typically two kinds of techniques used in data mining. The first is called the supervised technique, which depends on specific classification models of data. The second type is called non-supervised learning; it groups data with similar trends and patterns together (Humaid & Barhoum, 2013). In the previous section, one of the limitations of user profiling was that there was no holistic approach to identity management. To cope with this, organisations use identity and data matching and various techniques such as data modelling and mining to verify client information during each new service request. Various pieces of literature (PhridviRaj & GuruRao, 2014) describe data mining as the process of discovering hidden patterns and information from existing data. This commonly consists of the following steps (PhridviRaj & GuruRao, 2014):

- Anomaly detection: The identification of unusual data records that might be interesting or data errors that require further investigation.
- Association rule learning: Association rule searches for relationships between variables through association rule learning.
- Clustering: Clustering is the task of discovering groups and structures in the data that are in some way or another 'similar', without using known structures in the data.

- Classification: The process of classification is used to generalise a known structure in order to apply to new data.
- Regression: Regression attempts to find a function which models the data with the least error.
- Summarisation: This step involves a more compact representation of the data set, including visualisation and report generation.

Research shows that association rules as a data mining technique are widely used to discover patterns from user behaviour data. For example, association rules are used to discover a user's interaction preferences with an interface agent (Schiaffino & Amandi, 2009). The Apriori algorithm (Agrawal & Srikant, 1994) is used to generate association rules from a set of user-agent interaction experiences, which describes a unique interaction between the user and the agent. Further, Humaid and Barhoum (2013) use a prediction model in which they compare a user's transactional information, for example, with the historical trading patterns. This is done in order to predict the probability of a current transaction, and either refuse access or authorise and launch investigations into suspicious transactions. Other forms of rule-based fraud detection techniques are found in Humaid and Barhoum (2013), where the use of rule-based detection in large databases with millions of records is studied. The research applies the rule induction technique, as a descriptive model, to allow one interested in the data to browse through the rules in order to gain insight into the domain of data.

The fraud management approaches already discussed suggest that rule-based systems are efficient at detecting known fraudulent activity and criminal schemes; however, they are nonetheless static. Predictive neural networks complement these models by providing an adaptive and early warning system for new and ever-changing criminal tactics and customer behaviour. Neural network-driven fraud detection is based totally on the human brain working principal (Patidar & Sharma, 2011). As the human brain learns through past experiences and uses its knowledge or experience in making decisions regarding daily life problems, so does fraud detection through neural network technology. Neural network-based fraud detection will learn about the particular patterns of the user, just as in user profiling, but it is also trained on previous frauds experienced by organisations. Based on the pattern and use of the application, the neural network will make use of an algorithm to determine whether a particular transaction is fraudulent or legitimate.

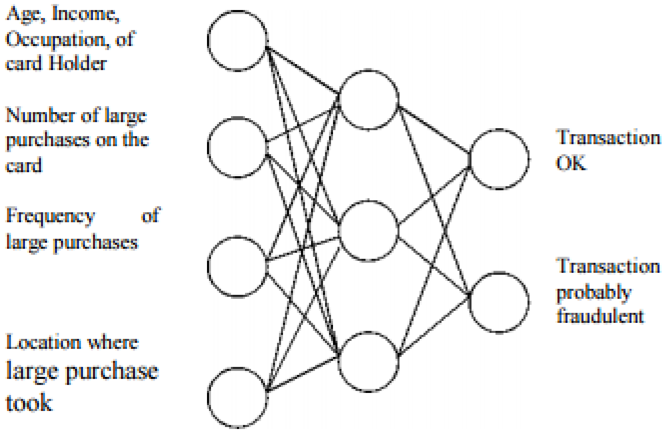

Age, Income, Occupation, of card Holder
Number of large purchases on the card
Frequency of large purchases
Location where large purchase took
Transaction OK
Transaction probably fraudulent

Figure 3.5: Typical structure of a neural network
Source: (Patidar & Sharma, 2011)

Figure 3.5 demonstrates the typical structure that is associated with neural networks. Each is composed of a collection of processing elements grouped in layers. These processing elements receive input, process the input and then deliver a single output.

Liu, et al. (2009) propose an integrated framework to detect fraud in financial systems. It makes full use of the subjective considerations of the people investigating the case and the objective data and information of the fraud incident. The integrated framework employs subjective and objective models to detect fraud in financial systems, and then integrates their results and gives a synthetic result. The framework can be used to analyse fraud scenarios, select the intrinsic features, and detect the abnormities and alarms. Similarly, the neural network of Patidar and Sharma (2011) is designed to produce output in real values between 0 and 1. If the neural network produces an output that is below 0.6 or 0.7, then the transaction is okay, and if the output is above 0.7, then the chance of a transaction being illegal increases. This is very different to Verrelst, et al. (2000) whose research introduces a supervised neural network tool that uses a classifier in the fraud detection engine. This classifier maximises the performance on previously unseen data, eliminates errors using an error minimisation procedure and is repeated for different architectures of the neural network in order to determine the optimal one. Once found, it can simply be used on top of the frontend, and it will produce an alarm value between 0 and 1 each time a suspicious transaction is presented through the fraud detection tool (Grabec, 1989).

Similarly, Renu and Suman (2014) introduce two Bayesian networks to describe the behaviour of a user. First, a Bayesian network is constructed to model behaviour under the assumption that the user is fraudulent and another is constructed to model behaviour under the assumption that the user is legitimate. Krenker, et al. (2009) propose a bi-directional neural network architecture-based approach capable of detecting fraud in real time. The model allows for the prediction of user behaviour and compares it in real time with monitored real-life behaviour. Other types of fraud management models through the use of neural network are decision trees and regression analysis. These are tree-shaped structures that represent sets of decisions (Chaudhary, et al., 2012). These decisions generate rules for the classification of a data set. These models are generally applicable in trend prediction, where decision trees can transform a model into if-then rules (Chang & Chang, 2009). Another form of neural network fraud detection is prototyping. This is a method of forming an optimal discrete representation of a naturally continuous random variable (Burge & Shawe-Tyalor, 2001).

3.3.2.1. Advantages

Flexibility of rules within rule-based detection: Each rule created can easily be applied into the knowledge base without the need to amend other existing rules. This benefit grants flexibility because it enables the incremental development of rule base.

Inductive logic in neural networks: As can be seen with user profiling, fraud detection becomes a very complex problem once the differentiation between fraudulent and normally atypical profile is very subtle. Detection through data mining is able to perceive alterations on a user’s profile and also confront this typical behaviour with the consumer’s history data. Neural networks continuously learn from the provided data and can continue to grow as more data becomes available. This type of technique is best suited for problems in pattern recognition, classification and interpretation of incomplete data, for example.

Rule-based approaches are robust: The neural network approach, in particular, is a soft computing technique that models the pervasive imprecision of the real world and has the ability to cope with incomplete data and are tolerant of faults if properly implemented for fraud detection (Lin & Hwang, 2000). Because neural networks consist of a large number of interconnected data that is all operating in parallel, the neural network can operate at a considerable speed and almost instantly detect fraudulent behaviour.

No prior knowledge of fraud: Generally in neural network detection, there is no need for an expert design of the rules. Unsupervised neural networks are used to look at how a user’s behaviour changes over time and need no prior knowledge of fraud unlike in case-based reasoning (Verrelst, et al., 2000). The data that is analysed for consistent patterns and/or systematic relationships between findings can also be validated by applying the detected patterns to new subsets of data.

Information sharing across entities: Collaborated data pooling makes it possible to achieve a single integrated view of customers. Data sharing is secure. Data is pooled from trusted sources and only shared with other participants sharing data. When businesses share information across an industry, participating businesses can detect fraud more quickly and improve efficiencies.

Ability to process large amounts of data: Using customer data collected over several years, organisations are able to develop models that predict whether, for example, an accident claim may be fraudulent and should be investigated more closely. In this case, data mining may also assist investigators by speeding up their data analysing process.

3.3.2.2. Limitations

Rule-based schemes are slow: Rule-based methods depend on an assumption that the system knows what to expect in time to defend the organisation. For example, fraudsters are adversarial and behave both unpredictably and fast. Over and above that, fraud modus operandi is not consistent, and fraudsters will always attempt new ways. On that account, rule-based detection that works exclusively on past knowledge will inevitably increase the number of cases flagged as false alarms.

Inability to discover new attacks: The main limitation of this approach is that the system fails to uncover new kinds of attacks; unless the system has been instructed to do so, a rule-based approach may sometimes become static, at least until an individual takes manual action to make changes. To keep up with the rate at which fraud patterns change, programs need to learn from the same transactional data that is being scored. A fraud prevention approach that collects real-time data and self-learns based on current information has a better chance of protecting the organisation against attacks.

Rule deterioration: Rule-based fraud detection applications and systems that implement conventional case-based reasoning techniques are limited, deteriorating over time as behaviour patterns impact the business change. As soon as an organisation can figure out a new tactic or criteria that will help catch future fraud attempts, there needs to be an individual to capture the rule.

Differentiation and personalisation: The current models have difficulty detecting a fraudster’s transaction behaviours during his non-criminal period, as these actions mimic those of regular legitimate users. Attempting to use generalised sets of rules or loose segmentation to fit unique individual customers may not end up satisfying the requirements.

Data quality: Data quality in data mining is about the accuracy of the data which can easily be affected by the structure and consistency of the data being analysed. The presence of duplicate user information, the timeliness of user activity updates, and human error can significantly impact the effectiveness of the more complex data mining techniques, which are sensitive to subtle differences that may exist in the data (Seifert, 2004).

3.3.2.3. Summary

As literature has shown, traditional rule-based approaches mostly use the if-then approach for fraud detection. In typical mobile application architecture, these rules would be applied to any layer that contains useful information and is worth analysing for detailed information. Moreover, the ultimate goal of rule-based detection is prediction, and it integrates areas such as databases and intelligent information systems to help automatically find correlations and groupings of data. Fraud management approaches of this type are therefore best suited to all the following layers of the mobile architecture stack: the application, and middleware and backend system layers.

3.3.3. Case-based reasoning

During the 1970s and 1980s, one of the most visible developments in artificial intelligence research was the emergence of rule-based expert systems. These programs were applied to various domains requiring extensive knowledge for rather critical tasks. Despite their success in various instances, their limitations were evident from the previous section. In the past decade, an alternative reasoning paradigm and computational problem-solving method attracted a great deal of attention. This reasoning paradigm is called case-based reasoning. Case-based reasoning (CBR) may be used a fraud detection technique to solve new fraud cases by remembering previous similar experiences. CBR draws attention because it seems to address directly the foregoing problems outlined (Watson & Marir, 1994). CBR differs from traditional rule-based systems in that knowledge is not represented in rules, but in examples.

Kolodner (1993) lists four assumptions about the world, which represent the basis of the CBR approach. First, he makes statements that the same actions executed under the same conditions will tend to have the same or similar outcomes. Secondly, experiences tend to repeat themselves. The third assumption is that small changes in the situation require small changes in the interpretation and in the solution. Finally, when things repeat themselves, the differences are usually small, and those differences are easy to compensate for (Pantic, 2008). The CBR approach, therefore, can be described best in terms of four processing strategies (Kolodner, 1993):

- Case retrieval: After the situation has been assessed, the best matching case is searched in the case base, and an approximate solution is retrieved.
- Case adaptation: The retrieved solution is adapted to fit the new problem better.
- Solution evaluation: The adapted solution can be evaluated either before the solution is applied to the problem or after the solution has been applied. Should the result not be satisfactory, the retrieved solution must be adapted again or more cases should be retrieved.
- Case-based updating: If the solution is verified as correct, the new case may be added to the case base.

Given a new fraud situation, the model retrieves relevant cases that might match the current situation and adopts the same solution (Kolodner, 1993). In a situation where the previous case is identical and its solution was successful, it can be returned as the current problem’s solution. Should there be differences in the case presented, then an adaptation phase kicks in. Aamodt and Plaza (1994) proposed a CBR cycle that consists of four sequential steps organised around the knowledge of the CBR system.

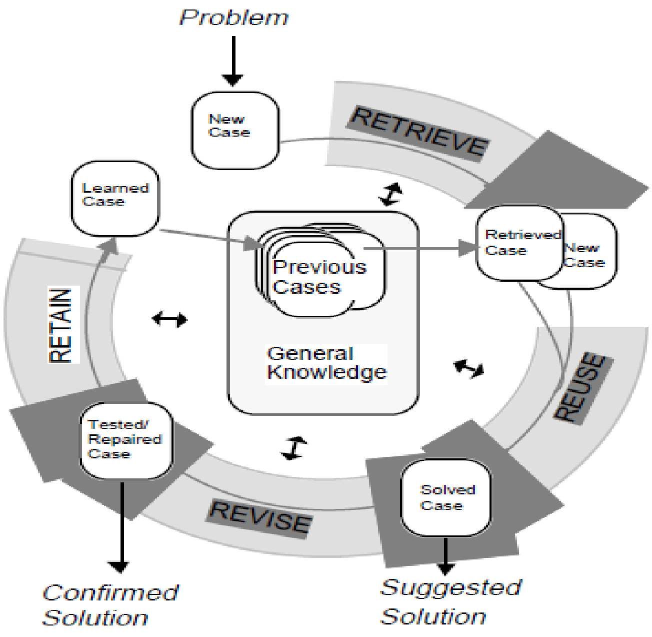


Figure 3.6: The CBR cycle
Source: (Aamodt & Plaza, 1994)

First, the retrieve phase, indicated in Figure 3.6, selects one or several similar cases from the case base that consists of previous cases. In the subsequent reuse phase, the solutions contained in those cases are adapted according to the query. In the revise phase, the solution is tested by being applied to a real-world environment and possibly corrected or improved by an expert. Finally, the retain phase takes the feedback from the revise phase and updates the knowledge in the case collection base.

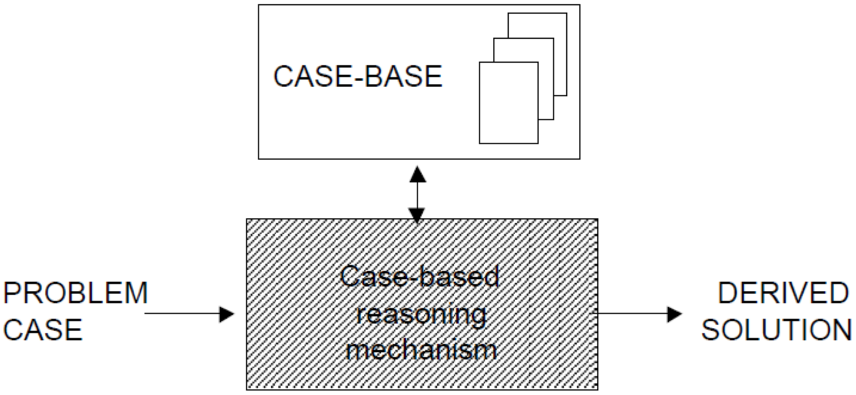


Figure 3.7: A CBR system

Source: Main, et al. (2001)

The structure of a CBR application can be thought of as a black box (general knowledge box) that incorporates reasoning mechanisms, as depicted in Figure 3.7. The problem or scenario feeds into the black box, where there are many pre-existing cases, and then a solution is derived based on the match (Main, et al., 2001). Richter (1995) proposed a unified view on the knowledge contained in a structural CBR application by introducing different knowledge containers, thereby providing some additional structure to the general knowledge box in Figure 3.7. The knowledge containers are the vocabulary, the case base, the similarity measure, and the adaptation knowledge:

- The vocabulary container is the basis of all knowledge and experience representation in CBR. This represents the information entities and structures (e.g. relations, attributes, and data types) that can be used to represent cases.
- The case base is the primary form of knowledge in CBR. This includes information such as hierarchical and generalised cases and are considered standard applications of artificial and database methods.

Curet, et al. (1996) discuss the application of case-based reasoning to assist accountants in identifying top management fraud. There is no coherent, structured knowledge about this type of fraud, only cases previously experienced by auditors. As a way to mitigate the gaps found in regular CBR systems, Wheeler and Aitken (2000) propose multiple algorithms for fraud detection in the credit approval process based on case-based reasoning. In their research, an adaptive diagnosis algorithm combining several neighbourhood-based cases was found to have the best performance. These results indicated that an adaptive CBR solution provided fraud filtering and case ordering functions for reducing the number of necessary fraud investigations. Similarly, Song and Song (2011) present a hybrid model of integrating CBR and hierarchy process in a fraud assessment model. The hierarchy process obtains expert knowledge from various other cases not contained in the data set in question. By using both these models, investigators may accomplish the task of fraud detection automatically and more efficiently.

On the contrary, Sun and Finnie (2004) recognise experience-based reasoning (EBR), a form of CBR, as a logical foundation for fraud and deception. EBR is based on a reasoning framework based on logical arguments, and in this research, eight different inference rules are proposed to cover all possibilities of fraud. This method immediately suggests that any fraud case is either not accounted for or included as part of the base, and as a result, one less relevant case falls off.

3.3.3.1. Advantages

Methodology and basis: Case-based reasoning builds on the idea that human expertise is not composed of formal structures such as rules, but of experience. In addition, case-based reasoning amounts to reasoning by comparing a new problem with a set of stored previous problems with their solution. The solution to the new problem is constructed by retrieving similar problems from memory and adapting their associated solutions to apply to the new problem.

Avoid repetitive mistakes: In applications that store fraudulent case information and user activity profiles, this model can use information about instances in the past to predict fraudulent behaviour in the future (Main, et al., 2001). When a problem is successfully solved, the experience is retained in order to solve similar problems in the future. When an attempt to solve a problem fails, the reason for the failure is identified and remembered in order to avoid the same mistake in the future.

Continuous learning from experience: Case-based reasoning favours learning from experience by retaining a concrete problem-solving experience. Frequent CBR systems are used for fraud detection, which allow the increased encountering of more fraudulent situations; this also directly creates more solutions. As more cases are added, the CBR system will be able to reason in a wider variety of scenarios and, therefore, be able to refine the solution.

Unexpected input: A case-based system can handle unexpected cases that did not previously exist in the system. Typically, the method would assess their similarity to stored cases and reuse relevant cases. The self-updatability of the system enhances the handling of unexpected cases (Prentzas & Hatzilygeroudis, 2007).

3.3.3.2. Limitations

Hard to find similarities: A major problem in case-based reasoning has to do with the retrieval of cases that are sufficiently similar to a new problem at hand. For the purpose of retrieval, a case-based reasoning system uses a similarity measure. Based on the specific measure employed, the system associates a numerical value with each case, indicating the similarity between this case and the problem under consideration. The basic idea is that cases with the highest similarity are retrieved from memory. The solutions of the retrieved cases are then combined to create a solution for the new problem. The difficulty with this approach is that it is hard to find a similarity measure that actually gives high values to cases that are similar to the new problem.

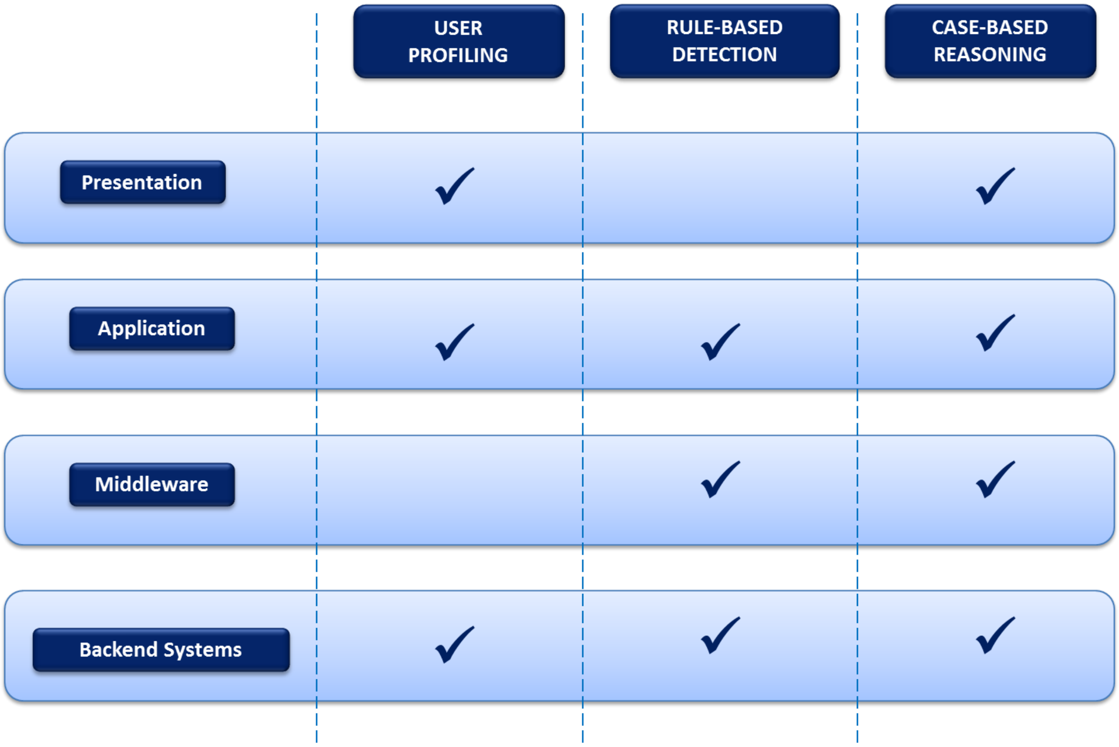
Time-intensive: One of the very clear limitations of rule-based techniques is that they take quite a long time to find and process actions of similar, previously identified cases. In an optimal fraud management model, a quick response time is vital. The process of case-based reasoning is about solving problems based on the solutions of similar past problems. The very nature of CBR is information retrieval and reuse, which suggests that the information will reside in a database of core application.

3.3.3.3. Summary

To sum up, the main idea behind case-based reasoning is about solving new problems by adaption solutions that were used to solve old problems. Fraud management approaches of this type are best suited to all layers of the architecture stack described in Chapter 2. Experience is required for complex problem-solving and is shared to obtain the experiences of different cases. This experience can be applied to the presentation, application, middleware and backend system layers. With the help of techniques such as data mining technology for feature selection and case retrieval, the quality of CBR systems can be improved.

3.4. SUMMARY OF FRAUD MANAGEMENT APPROACHES IN A MOBILE APPLICATION ARCHITECTURE

Mobile applications have similar threats, vulnerabilities and risks as those posed by typical web and client/server applications. That said, having had explored the various fraud management approaches, it is of utmost importance to distinguish which approach would satisfy the mitigation of risk in the various layers of the mobile application.



	USER PROFILING	RULE-BASED DETECTION	CASE-BASED REASONING
Presentation	✓		✓
Application	✓	✓	✓
Middleware		✓	✓
Backend Systems	✓	✓	✓

Figure 3.8: Summary of fraud management approaches in mobile application architecture

Figure 3.8 summarises the fraud management methods studied in this chapter and illustrates the applicability of these approaches to each layer of mobile app architecture. In general, most of the investigated approaches can be implemented at most layers of the architecture. Although some implementation may be out of the organisation's control, especially at the middleware layer, it would make perfect sense to use a combination of approaches at the backend system layer so as to ensure security enforcement. From the figure, it is clear that case-based reasoning can be applied throughout all four layers for effective fraud risk mitigation.

3.5. CONCLUSION

Through the growth and use of mobile devices for applications, fraud has become more prevalent in recent years. Building a precise and simple mobile application fraud management solution is one of the key tasks for organisations. Proper management of mobile application fraud requires a model that is intelligent enough to adapt to the criminal strategies and ever-changing attacks that are so prevalent. Effective and efficient fraud management for mobile applications is a core capability required towards detecting, preventing and managing fraud in an effort to minimise losses and reputational damage due to unlawful acts.

In this chapter, several studies for fraud detection were evaluated, such as user profiling and case-based reasoning. Case-based reasoning models, as an example, generally give good or reasonable solutions, but are not the best solution. Intelligent user profiling implies the application of intelligent techniques, from data mining or information retrieval, for example, to building user profiles. The data these techniques use to automatically build user profiles is obtained mainly from the observation of a user’s actions. Furthermore, research has demonstrated that neural networks are also a promising technique in modelling and identifying different kinds of frauds. Although there are several fraud detection technologies that exist based on data mining, intelligent user profiling and neural networks, all these are, however, not capable enough to detect the fraud at the time when a fraudulent transaction is in progress due to reduced chances of a transaction being fraudulent.

The purpose of this chapter was to explore existing literature on various fraud management models, approaches and frameworks. The techniques were discussed together with their strengths, weaknesses, and advantages along with disadvantages. Research of such kind will enable one to build a hybrid approach for fraudulent mobile application activity identification, which is discussed in Chapter 5. The next chapter follows a similar approach to Chapter 3 by reviewing the various digital forensic approaches available in literature today.

4. REVIEW OF DIGITAL FORENSIC APPROACHES

4.1. INTRODUCTION

Digital forensics (DF) is an emerging area within the broader domain of computer security whose main focus is the discovery and preservation of digital evidence. The evidence may be used to prove criminal wrongdoing and ultimately the prosecution of criminal activity. This tradecraft has grown from a relatively vague one to an important part of many investigations. As opposed to FM, discussed in Chapter 4, which speaks to the prevention of fraudulent activity, DF's main focus is on the actions to be taken post an incident.

The types of data contained within mobile devices and the way they are being used are constantly evolving. With the popularity of smartphones, it is no longer sufficient to document only the phonebook, call history, text messages and media storage areas. Mobile devices have now become fully functioning minicomputers and potentially contain much more relevant data. The data from an ever-growing number of installed applications also contain a wealth of relevant information, for example, storage devices, networks, telecommunications traffic and other similar locations that a mobile application would make use of. Traditional digital forensic skills are becoming more and more necessary for mobile device examinations. Efficiency and accuracy are central issues facing the field of digital forensics, and the integrity of the methodology used to acquire, preserve and analyse digital evidence is a key factor.

The previous chapter reviewed some FM approaches. This chapter aims to unpack current literature and research focused on DF process models, approaches and frameworks, more so in the field of mobile applications. The review seeks to extract and study advantages and limitations of the models explored. The chapter is structured as follows: Section 4.2 gives an overview of the general mobile forensic process and further explains the need for such a model. In Section 4.3, a thorough literature review of the various DF models and frameworks in existing research are discussed with a brief overview of their benefits and limitations. The last section then sums up the findings in the form of a matrix table and their applicability to the mobile application architecture.

4.2. OVERVIEW OF FORENSICS

4.2.1. Definition of digital forensics

Forensics can be defined as the “process of using scientific knowledge in the collection, analysis and presentation of evidence to the courts” (Nolan, O'Sullivan, Branson and Waits, 2005:3). Computer forensics or digital forensics is then a subset of forensics that deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in a manner that is admissible in a court of law (Nolan, et al., 2005). Forensics primarily deals with the recovery and analysis of evidence.

Chapter 2 noted mobile devices as an evolving form of computing, where these devices are used in managing electronic documents. Because over time they accumulate a sizeable amount of information that can be used in crimes or other fraudulent incidents, proper techniques are required to recover evidence from these devices. Mobile forensics is then a subset of digital forensics related to the recovery of digital evidence from mobile devices. Jansen and Ayers (2007) define mobile forensics as the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods, or as defined by Thing, et al. (2010), it is the process of preservation, identification, extraction and documentation of digital evidence stored as data. Mobile device forensics is best known for its application to law enforcement investigations, but it is also useful for military intelligence, corporate investigations, private investigations, criminal and civil defence, and electronic discovery.

Mobile phones are the most personal electronic devices a user accesses. They are used for performing simple communication tasks, such as calling and texting, while still providing support for internet browsing, e-mail, taking photos and videos, creating and storing documents, identifying locations with Global Positioning System (GPS) services, and managing business tasks. More often than not, mobile phone forensics is applied to digital data retrieval of deleted communications. The next section discusses the need for mobile forensics.

4.2.2. The need for mobile forensics

As already discussed, the evolution of mobile devices and the applications thereof has fast outsold personal computers. Today, these devices are being used to store and transfer personal and even corporate information. Word processors, spreadsheets, presentations and database applications have already been ported to mobile devices as part of their core functionality. Additionally, technologies such as freely available e-mail wireless connections provide users with instant e-mail notifications and download capabilities. This, in turn, transforms a mobile device into an e-mail storage and transfer tool (Al-Zarouni, 2006).

Mobile devices are also used for online transactions. Banking technologies such as e-wallet, online shopping, and flight reservations added the convenience of online transactions via mobile phones. This advancement gives rise to fraudulent activity and use.

As previously mentioned, the main objective of digital forensics is to extract suspicious or unusual events and their causal relationships. In a case where forensic information would need to be extracted, the typical information to be analysed would include (Al-Zarouni, 2006):

- the recovery of hidden data, deleted data, or partially overwritten data on devices;
- the examination and analysis of communications, files and programs;
- geographic location analysis; and
- the reconstruction of user activity, communications, and movements on the device.

The basic notion of forensics is that evidence is a set of traces that are usually in a sequence (bits and pieces of information), and also that it is latent in nature and technical (need tools to explain it). Unlike the world of personal computers with its limited number of operating systems, there are countless manufacturers of mobile devices that may have their own formats and technologies. For the purpose of this study, the research will focus on the DF models and methodologies used, as opposed to the actual tools and technology.

4.3. A REVIEW OF MOBILE DEVICE DIGITAL FORENSIC APPROACHES

Over the past several years, digital forensic examiners have seen a remarkable increase in requests to examine data from mobile phones and other mobile devices. The examination and extraction of data from these devices present numerous unique challenges for forensic examiners. With smartphones and tablets representing an increasing proportion of mobile devices submitted for examination, the number of unique challenges continue to grow. As organisations rely more heavily on technology-based methods of communication, such as mobile phones, many corporations and legal professionals are increasingly looking to computer forensics for the recovery of electronic information. Computer forensics can be utilised as a means to combat fraud, investigate theft or monitor user activity. The methodology of digital forensics aims to recreate a sequence of events arising from, for example, the unauthorised intrusion by an external party into, or unusual activities by an authorised user of, digital systems (Brewer, et al., 2006). In digital forensics, forensic data may be analysed. Forensic data is data that is used to discover what it is that occurred and possibly who the responsible party is. This data can be classified into two categories: (1) the content of the entity, for example, a word document, an e-mail file, and (2) the meta-data associated with it such as document timestamps.

The digital forensics process is broken into three main categories: seizure, acquisition, and examination/analysis. Such methodologies consist of the following steps:

- the preparation of a forensic copy of the acquired digital media while preserving the acquired media’s integrity;
- an examination of the forensic copy to recover information;
- an analysis of the recovered information; and

- the reporting of pertinent information uncovered.

Some suggested and proposed digital investigation models have been selected for review and discussion in the following section. Some of these methodologies and frameworks and their applicability to the mobile application architecture described in Chapter 2 will be explored. The section also aims to highlight the potential benefits that could be relied upon for the suggestion of a unified fraud management and digital forensic framework that will be discussed in Chapter 5.

4.3.1. Physical digital forensic process models and approaches

The digital forensic process models that fall into this category distinguish themselves by connecting the digital investigative process with the more established investigative processes associated with physical crime scenes by conceptualising a digital device itself as a crime scene. One of the first research efforts into digital forensics (Pollit, 1995) compares computer forensics process to the admission of documents in a court of law. The basis formed on this model is that digitally based evidence must be both scientifically sound and legally acceptable. It comprises four distinct phases: acquisition, identification, evaluation, and admission.

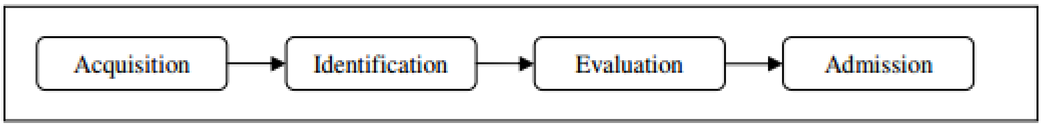


Figure 4.1: Computer forensic investigative process
Source: Yusoff, et al. (2011)

- Acquisition: In the acquisition phase, evidence is acquired in an acceptable manner, with proper approval. In a paper-based world, how a document is acquired is subject to a set of rules. For digital media, there needs to be consideration of what the data means and represents, if represented as binary, for example, as well as where it comes from.

- Identification: The identification phase follows next, where digital components from the acquired evidence are identified and converted into a readable format. In a paper-based scenario, a document would be read and its content understood. A digital media file requires conversion in the form of a program, which will transform the data into a form that is humanly readable.

- Evaluation: The evaluation phase determines whether the components identified in the identification phase are relevant to the case being investigated. Should this be the case, then the evidence is considered to be legitimate. In a paper-based world, this step would allow the analyst to determine if the information contained in the document is relevant; this is the same as with digital media.

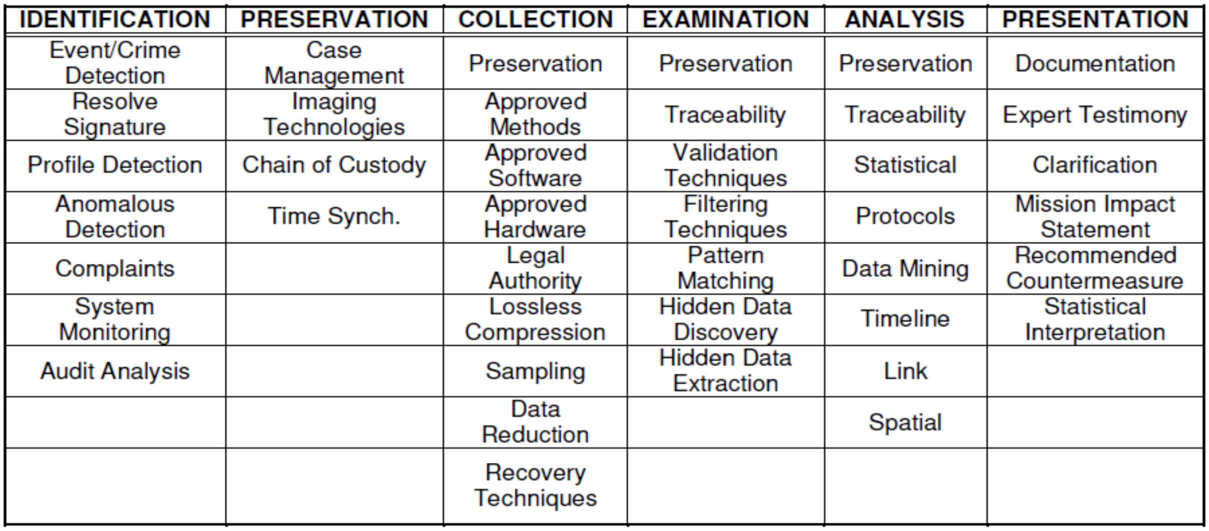
- Admission: The last phase involves the presentation of the acquired and extracted evidence in the form of findings.

In years past, the US Department of Justice published a process model. This model (US Department of Justice, 2001) consists of four phases:

- Collection: This involves evidence search, evidence recognition, evidence collection and documentation.
- Examination: This is designed to facilitate the visibility of evidence while explaining its origin and significance. It involves revealing hidden and obscured information and the relevant documentation.
- Analysis: This looks at the product of the examination for its significance and probative value to the case.
- Reporting: This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation.

The Digital Forensic Research Conference (DFRWS) is a non-profit organisation dedicated to the sharing of knowledge and ideas about digital forensics research. The DFRWS framework (DFRWS, 2001) is a consensus developed between 2001 and

2003 by an ad hoc group of researchers and practitioners in digital forensic science. At the first digital forensic workshop (DFRWS, 2001), the members agreed to this model with fellow researchers by agreeing that the core process of the DF cycle was identification, preservation, collection, examination, analysis and presentation (Stephenson, 2003a).



IDENTIFICATION	PRESERVATION	COLLECTION	EXAMINATION	ANALYSIS	PRESENTATION
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation
Resolve Signature	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Audit Analysis		Sampling	Hidden Data Extraction	Link	
		Data Reduction		Spatial	
		Recovery Techniques			

Figure 4.2: The DFRWS digital investigation framework
Source: (Stephenson, 2003b)

Identification: The identification class describes a method by which the investigator is notified of a possible incident and consists of seven elements (Stephenson, 2003a). These elements are event detection, resolve signature, profile detection, anomalous detection, complaints, system monitoring, and audit analysis. These elements are concerned with the identification of cases through detection.

Preservation: This component deals with those elements that relate to the management of items of evidence. The DFRWS describes this class as the requirement for proper evidence handling that is basic to the digital investigative process as it relates to legal actions.

Collection: The collection component is concerned with the specific methods and products used by the investigator and forensic examiner to acquire evidence in a digital environment.

Examination: The examination phase is concerned with evidence discovery and extraction as well as the examination of that data and the identification and extraction of possible evidence from it.

Analysis: The analysis phase refers to those elements that are involved in the analysis of evidence collected, identified and extracted from a gross data collection. The validity of techniques used in the analysis of potential evidence impact directly the validity of the conclusions drawn from the evidence and the credibility of the evidence chain constructed therefrom.

Presentation: In this phase, a forensic investigator develops a set of conclusions regarding evidence presented from the other five previous stages. As with all elements of the framework, a clear understanding of the applicable process is required, thus ensuring adherence to standard tools, technologies and techniques. Reporting of the facts is in an organised, clear and objective manner.

In his research, Stephenson (2003) discusses an approach to post-incident root cause analysis of digital incidents. The ability to model the investigation and its outcome lends materially to the confidence that the investigation truly represents the actual events. The approach is best suited to large, complex investigations; it offers the ability to identify investigative process flaws that could compromise the investigation procedurally or could lead to developing flawed evidence or missing important evidence.

The investigation process proposed by Carrier and Spafford (2003) was done with the intention of combining the various available investigative processes into one integrated model. The authors introduce the concept of a digital crime scene, which refers to the virtual environment created by software and hardware where digital evidence of a crime or incident exists. Carrier and Spafford (2003) define a process model for digital investigations using theories and techniques from the physical investigation world. In their proposal, the authors treat the computer as a secondary crime scene. Their ‘Integrated Digital Investigation Process’ defines 17 phases organised into five groups shown in Figure 4.3.

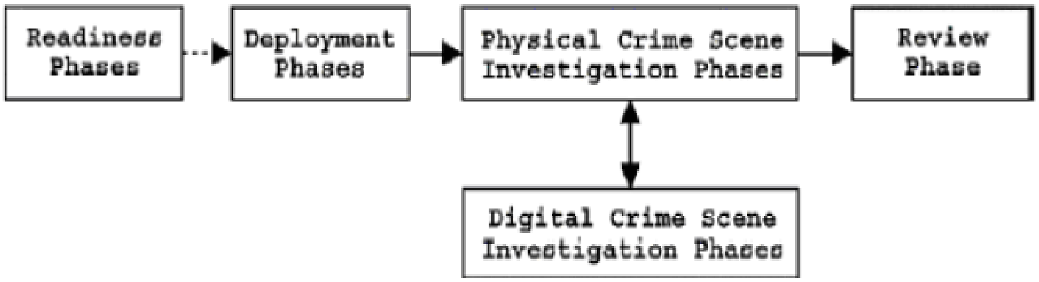

Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

Figure 4.3: Integrated digital investigation process
Source: (Carrier & Spafford, 2003)

The **readiness phase** ensures that the operations and infrastructure are able to fully support an investigation. In this readiness phase, the equipment must be ever-ready, and the personnel must be capable of using it effectively. Further, this phase is an ongoing phase throughout the lifecycle of an organisation and consists of two sub-phases: operation readiness and infrastructure readiness.

The **deployment phase** provides a mechanism for an incident to be detected and confirmed, and consists of two sub-phases: detection and notification, and confirmation and authorisation.

The **physical crime scene investigation phase’s** goal is to collect and analyse the physical evidence and reconstruct the actions that took place during the incident. It consists of six sub-phases: preservation, survey, documentation, search and collection, reconstruction, and presentation (Carrier & Spafford, 2003).

The **review phase** entails a review of the whole investigation and identifies areas of improvement.

In examining security and fraud incidents, it is necessary to be able to reconstruct one or more events that occurred during the time of the fraud. The result is an event-based framework that can be used to develop hypotheses and answer questions about an incident or crime. Carrier and Spafford (2004) added several new elements to the digital forensic framework: events and event reconstruction. Hypotheses are developed by collecting objects that may have played a role in an event that was related to the incident. Once the objects are collected as evidence, the investigator can develop hypotheses about previous events at the crime scene (Carrier & Spafford, 2004). Prosise and Mandia (2003) proposed an incident response methodology that is simple and accurate. An initial response phase to ascertain the incident and formulation of a response strategy phase is added. The investigation phase includes collection and analysis phases as in their earlier models.

4.3.1.1. Advantages

The aforementioned models and approaches are useful from the physical perspective, as all digital evidence ultimately exists in physical space. Furthermore, by explicitly drawing a parallel between the handling of digital and physical crime scenes, these models encourage the transfer of mature crime scene investigation techniques from the physical forensic science to the digital forensic science (Casey & Schatz, 2011).

As one of the very first approaches developed in forensics, Pollit (1995) brings about a very basic but concise methodology to forensic investigations. The phases in his framework are distinct and provide a straightforward methodology for dealing with digital evidence to allow for results to be scientifically reliable and legally acceptable. In addition to this, the model of the US Department of Justice (2001) attempts to describe the computer forensics process free from specific technologies. The model identifies the core aspects of the forensic process and then builds steps to support it; no technology or methodology is prescribed. This allows traditional physical forensic knowledge to be applied to electronic evidence. Moreover, the model does not make a distinction between forensics applied to computers or other electronic devices but instead attempts to build a generalised process that will be applicable to most electronic devices. The approach of Carrier and Spafford (2004) particularly highlights the reconstruction of the events that led to the incident and puts emphasis on reviewing the whole method, hence ultimately building a mechanism for quicker forensic examinations. The advantage of this is also that it gives accurate results from the investigation process. This model is also appropriate for the collection of evidence in a live environment, as it is integrated with both the law enforcement process and the abstract model discussed in section 4.3.2.

The DFRWS framework provides a consistent method of identifying the research and development areas for digital investigation. The main advantage of DFRWS is that it is the first large-scale organisation that is led by academia rather than by law enforcement. It therefore defines and focuses the direction of the scientific community towards the challenge of digital forensics (Jafari & Satti, 2015). Because of the introduction of classes that categorise the activities of an investigation into groups, this methodology can be applied to a range of digital devices or even unrealised digital devices of the future. This would enhance the science of forensics by providing a basis for analysing new digital and electronic technology while at the same time providing a common framework for law enforcement to feasibly work within a court of law.

4.3.1.2. Disadvantages

The differences between searching physical and digital crime scenes are significant and may create challenges for digital investigators. The potential for error in data representation is unique to digital crime scenes as opposed to physical crime scenes and thus requires extra precautions in reporting the evidence found through the use of these tools. In addition, one of the very noticeable limitations of these approaches is the sequential ordering of the phases. This implies that the process models do not make way for iteration. The assumption that a particular phase is carried out without error for the first time does not hold true.

In addition to this, because of the comparison to physical evidence process, the collection of the physical hard disk is assumed to be the collection of electronic evidence. At that point in the investigation, it is unknown to the investigator if the physical hard disk contains relevant electronic evidence or not. On that account, irrelevant and unnecessary data may be collected. In the case of Carrier and Spafford (2004), the model depicts the deployment phase as being independent of the physical and digital investigation phase. In practice, however, it seems impossible to confirm a digital or computer crime unless and until some preliminary physical and digital investigation is carried out.

Finally, the DFRWS model is rigid and linear; however, it is suitable for cases where necessary investigative activities are well understood (Bradford & Ray, 2007). In addition to that, the definition of these classes is not standardised; for example, analytical procedures and protocols are not regulated, nor do practitioners use standard terminology due to the generality of the framework. Moreover, the introduction separate classes to the model make it more cumbersome to use.

4.3.2. Staircase digital forensic process models

The set of digital forensic process models that follow depict the approach as a sequence of ascending stairs and provide a practical and methodical approach to conducting effective digital investigations. The steps in these approaches may proceed simultaneously, and it may be necessary to take certain steps more than once at different stages of an investigation or as new information emerges (Casey & Schatz, 2011). Baryamureeba and Tushabe (2007) suggest a modification to the process model of Carrier and Spafford (2003) by describing two additional phases: traceback and dynamite. The Enhanced Digital Investigation model (EIDIP) separates the investigations at the primary and secondary crime scenes while depicting the phases as iterative instead of linear. The goal is to reconstruct the two crime scenes concurrently in order to avoid inconsistencies. This is to enable the investigator to make traces all the way back to the actual device/computer used by the criminal to perform the crime.

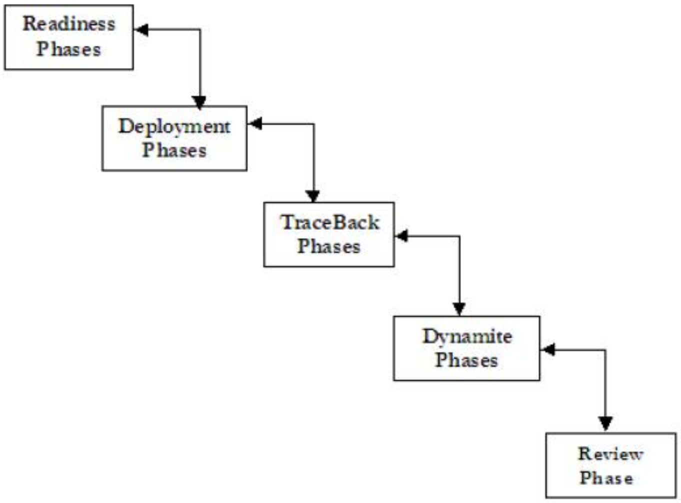


Figure 4.4: EIDIP model
Source: (Baryamureeba & Tushabe, 2007)

The EIDIP model is the integration of the forensic process model as well as the abstract process model and consists of the following additional phases (Baryamureeba & Tushabe, 2007):

Traceback phase: Within this phase, the perpetrator’s physical crime scene of operation is tracked down, leading to identification of the devices that were used to perform the act.

Dynamite phase: The dynamite phase also investigates the primary crime scene.
Both these additional phases collect and analyse the items that were found at the primary crime scene to obtain further evidence that the crime originated from and help identify the potential culprits.

Casey and Palmer (2004) proposed an investigative process model to encourage a complete rigorous investigation to ensure proper evidence handling and reduce the chance of mistakes. Digital investigators and forensic examiners scale these steps in a systematic approach from bottom up in an effort to present a complete and comprehensive case. Apart from the common phases found in general digital forensic processes, the assessment phase validates the fraud incident in order to allow for a decision to be made in whether to continue with the investigation or not. This framework also includes the following key steps: recognition, preservation, classification, and reconstruction. The last two steps (classification and reconstruction) are the ones in which the evidence is analysed. The model is first presented in terms of standalone computer systems and then applied to the various other layers.

Reith, et al. (2002) then proposed an enhancement to the existing DFRWS model in the form of the Abstract Digital Forensic model. The basis of this Abstract Digital Forensic model is using the ideas from traditional (physical) forensic evidence collection strategy as practised by law enforcement, which consists of nine components.

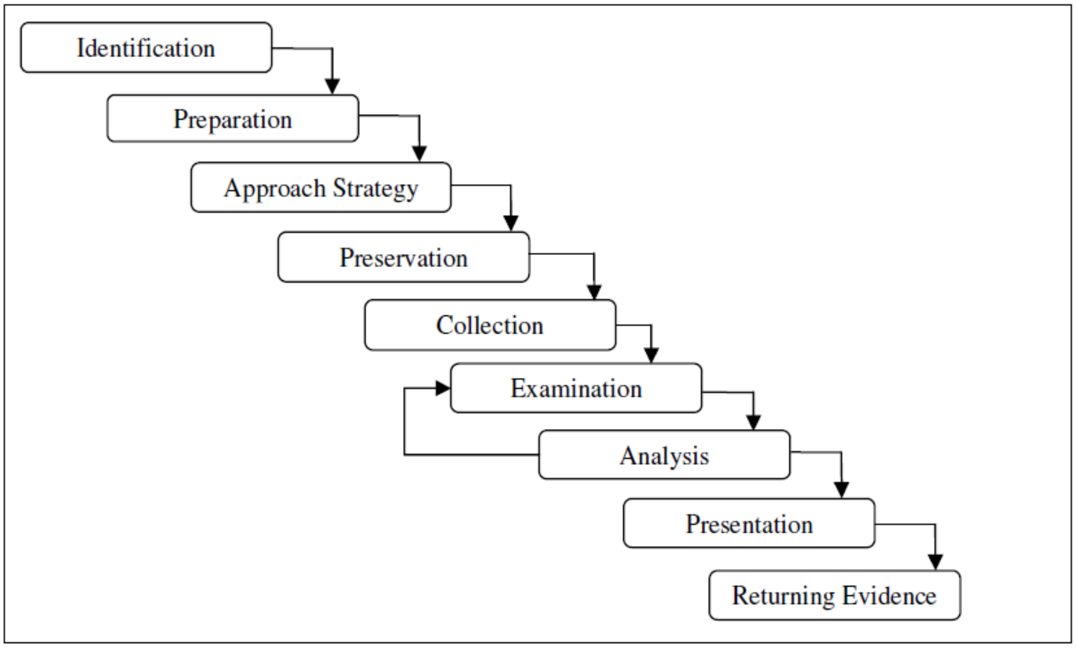


Figure 4.5: The Abstract Digital Forensic model
Source: (Reith, et al., 2002)

Three significant phases are introduced in this model, as shown in Figure 5.3. These phases include preparation, approach strategy and returning evidence. The phases are briefly discussed below (Reith, et al., 2002).

Preparation: The preparation phase includes identifying tools and techniques to be used during the forensic investigation in order to gain buy-in and support.

Approach strategy: The approach strategy phase was introduced with the objective of maximising the acquisition of untainted evidence and at the same time minimise any negative impact on the victim and their surroundings.

Returning evidence: At this phase, the investigation process is complete. The objective of this final phase is to ensure that evidence is safely returned to the rightful owner or properly disposed.

The extended model of Ciardhuáin (2004) goes beyond the steps required to preserve and examine digital evidence. The main goal of this model is to completely describe the flow of information during an investigation – from the moment digital investigators are alerted until the investigation reaches its conclusion, as seen in Figure 4.6.

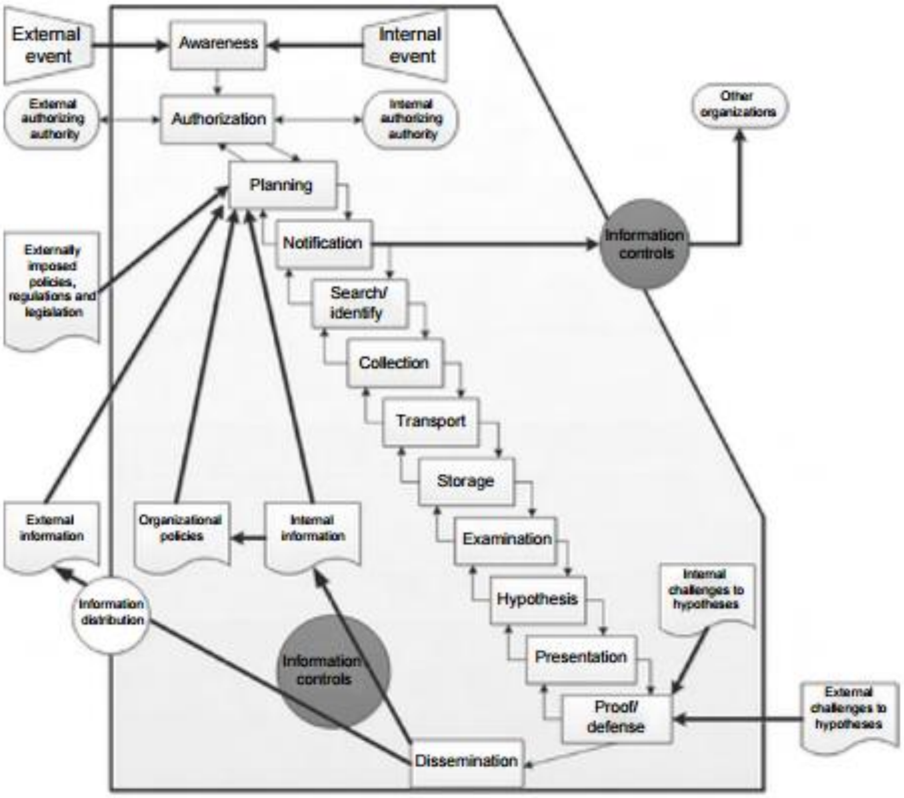


Figure 4.6: Extended model of cybercrime investigations
Source: Ciardhuáin (2004)

Ciardhuáin (2004) asserts that the existing models are general models of cybercrime investigation and only concentrate on the processing of evidence in cybercrime investigation. His proposed ‘extended model of cybercrime investigations’ explicitly represents the information flows in an investigation and captures the full scope of an investigation, rather than only the processing of evidence. Even though the model is generic, it concentrated on the management aspect. The steps or phases are also called ‘activities’ and are as follows:

Awareness: The first step consists of the creation of awareness or notification that an investigation is required. This is generally created by an event such as an intrusion detection system.

Authorisation: The authorisation activity gives permission for an investigation to be carried out.

Planning: Following the authorisation, the planning activity commences and is supported by information, both internal and external to the organisation.

Notification: The notification activity involves informing the subject or other concerned parties of the planned investigation; however, if the investigation is being done in secret, then no notification is sent.

The **search for and identify of evidence** activity is about locating the evidence to be used and identifying what is further required in that collected evidence.

The **collection** activity takes possession of the evidence in a form that can be preserved and analysed.

Transportation: Following the collection of evidence, the evidence must be transported to a suitable location for later examination.

Storage: The collected evidence is securely stored in order to maintain the integrity of the data.

The **examination** activity now involves the detailed assessment of the evidence through the use of various techniques in order to interpret the data.

Hypothesis: Following the examination, the investigator is then expected to construct a hypothesis of what it is that occurred during the crime.

Presentation: The hypothesis results are then presented in a manner that is easy to understand.

The **proof/defence** activity ensures that the hypothesis presented contains proof of the events and that what is documented and presented is valid.

The final activity of the process model involves the **dissemination** of information from the investigation to the authorised and interested parties.

4.3.2.1. Advantages

In the research, Casey & Palmer (2004) point out that the staircase digital forensic process model is an evidence processing cycle because the reconstruction can point to additional evidence that causes the cycle to begin again. Because the framework presented is inherently a process model, the output of each phase serves as input to succeeding phases. Casey and Palmer’s model is also quite general and is successfully applied to both standalone systems and networked environments.

The investigation phases of the EIDIP include both physical and digital crime scene investigations and a presentation of findings at that point. The introduction of the dynamite phase ensures that investigations are conducted at the primary crime scene, with the purpose of identifying the potential culprits. This also allows for reconstruction, where pieces of information are collected and put together so as to construct possible events that could have happened.

First, the introduction of the preparation and approach strategy phase helps to partially mitigate the limitation found in the framework of DRFWS (2001) on non-standardisation. The steps in the approach of Reith, et al. (2002) are abstract, defined to produce a model that is not dependent on a particular technology or electronic crime. This allows a consistent methodology for dealing with past, present, or future digital devices in a well-understood and widely accepted manner. Furthermore, the collection phase is properly placed in order to avoid collecting irrelevant evidence.

The model proposed by Ciardhuáin (2004) is considered to be one of the most complete approaches. This approach provides a consistent as well as structural framework for digital forensic investigations through the introduction of various distinct phases. This allows for standardisation and consistency of terminology and the identification of areas in which further developments are required. The flow of information in the investigation process is explicit; moreover, the process allows for deep exploratory research around an incident.

4.3.2.2. Disadvantages

Because of Casey's model being too general, this is a disadvantage, as the integrity of the investigation process and governance may be compromised. Though Integrated Digital Investigation Model IDIP has 17 and EIDIP model has 19 steps, there are repetitions of steps in these process models that will make them extensive and time-consuming with respect to the investigation (Jafari & Satti, 2015). The aforementioned process model also does not give much attention to the analysis phase. This phase is improperly defined and ambiguous and confuses analysis with interpretation despite these being two distinct processes. In addition to this, the EIDIP model introduces the reconstruction after all investigations have taken place instead of having to build the case concurrently in order to avoid inconsistencies and inaccuracy of the findings.

Very much like the framework of DFRWS (2001), the Abstract Digital Forensic model does not allow for much iteration apart from the examination and analysis phases. A majority of the phases are sequentially ordered and are a function of time, and there may be situations where within-investigation iteration is needed.

On the other hand, the generality of the staircase digital forensic process models process model may present some challenges. Some activities may be considered irrelevant and can be assumed by another activity. For example, the storage activity can be made part of transportation. Additionally, the terms used to describe each activity are not clearly defined, making it difficult to compare with other models. Another weakness of this model is that it excludes certain steps that are present in other models such as the return or destruction of evidence at the end of an investigation, for example, such as that highlighted by Reith, et al. (2002).

4.3.3. Phased digital forensic process models and approaches

Beebe and Clark (2005) contended that most investigative process models were too high level and proposed a multi-tiered digital forensic model with several sub-tasks for each of the phases in the process. The research introduces the concept of objectives-based tasks wherein the investigative goals are used to select the analysis tasks.

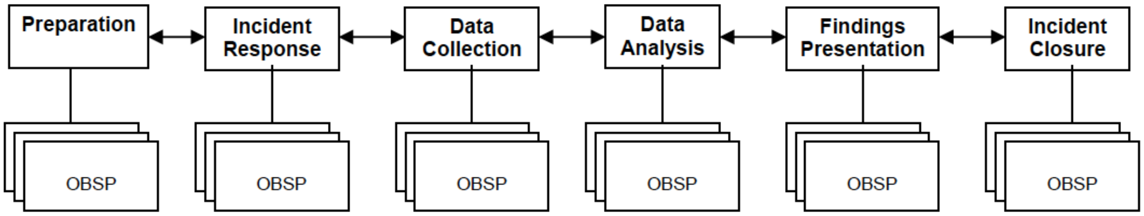


Figure 4.7: Two-tier digital forensic process framework
Source: (Beebe & Clark, 2005)

The second-tier sub-phases should be inclusive of all possible types of crime and digital evidence and consist of tasks that are subordinate to specific objectives of interest. While the objectives-based sub-phases (OBSP) will remain largely consistent from situation to situation, the specific tasks that populate the sub-phases will vary depending on the objectives sought in any given situation. Additionally, some tasks and sub-tasks may apply to more than one objective. As a result, the tasks can be matrixed to the set of digital forensic objectives as deemed appropriate. This enables the digital forensic examiner to quickly determine which objectives and specific tasks are applicable to the incident and approach strategy at hand.

Other similar models include the one by Agrawal, et al. (2011), who developed a systematic digital forensic model with the aim of helping forensic practitioners and organisations to set up appropriate policies and procedures in a systematic manner. The proposed model explores the different processes involved in the investigation of cybercrime and cyber fraud in the form of an 11-stage model. The model focuses on investigation cases of computer frauds and cybercrimes, and thus, the application of this model is limited to computer frauds and cybercrimes. In addition to that, Ademu, et al. (2011) introduced a structured and consistent approach for digital forensics by identifying activities that improve the process. The entire digital forensic investigation process can be conceptualised as occurring iteratively in four different phases. The first tier, which is the preparation phase, occurs over the course of an investigation, from assessment to final presentation phase. The first tier will have four rules for a digital forensic investigation that involves preparation, identification, authorisation and communication. The second tier will have rules such as collection, preservation and documentation; the third tier will have rules consisting of examination, exploratory testing, and analysis; and the fourth tier, which is the presentation phase, has rules such as result, review and report.

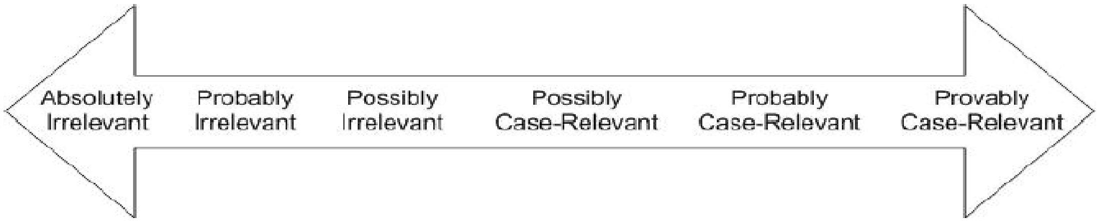


Figure 4.8: Degrees of case relevance
Source: (Gong & Chan Kai Yun, 2005)

On the other hand, Gong and Chan Kai Yun (2005) debate that existing investigation paradigms are laborious and require significant expertise. Their research identifies the need for computer intelligence technology for the current computer forensic framework, which will offer more assistance in the investigation procedures and better knowledge reuse within and across multiple cases and sharing. The first concept that was introduced by the authors is the notion of Seek Knowledge, which is the investigative clues which drive the analysis of data. The second notion is that of Case Relevance, which describes the distinctions between different cases, as opposed to simply a relevant or irrelevant case. Figure 4.8 uses ‘possible’ and ‘probable’ to describe the increasing levels of case relevance or irrelevance. The degree of case relevance provides the possibility to establish an effective framework for analysing cost versus completeness.

4.3.3.1. Advantages

A structured and consistent framework is vital to the development of digital forensic investigation and the identification of areas in which research and development are needed. These multi-tiered models identify the need for interaction in order to fully maximise the investigation through better definition of goals. Also, the definition of the fundamental goals within each step of the investigation allows for greater consistency and standardisation (Casey & Schatz, 2011). Another advantage of such process models is exploratory testing. Investigators can fully explore the characteristics of a specific element and, in turn, learn new techniques while performing an investigation.

In the case of Gong and Chan Kai Yun (2005), the degree of case relevance offers a great opportunity to rank the potential information according to the importance to the criminal investigation. This makes allowance for the investigators to handle the most important parts within the limited time.

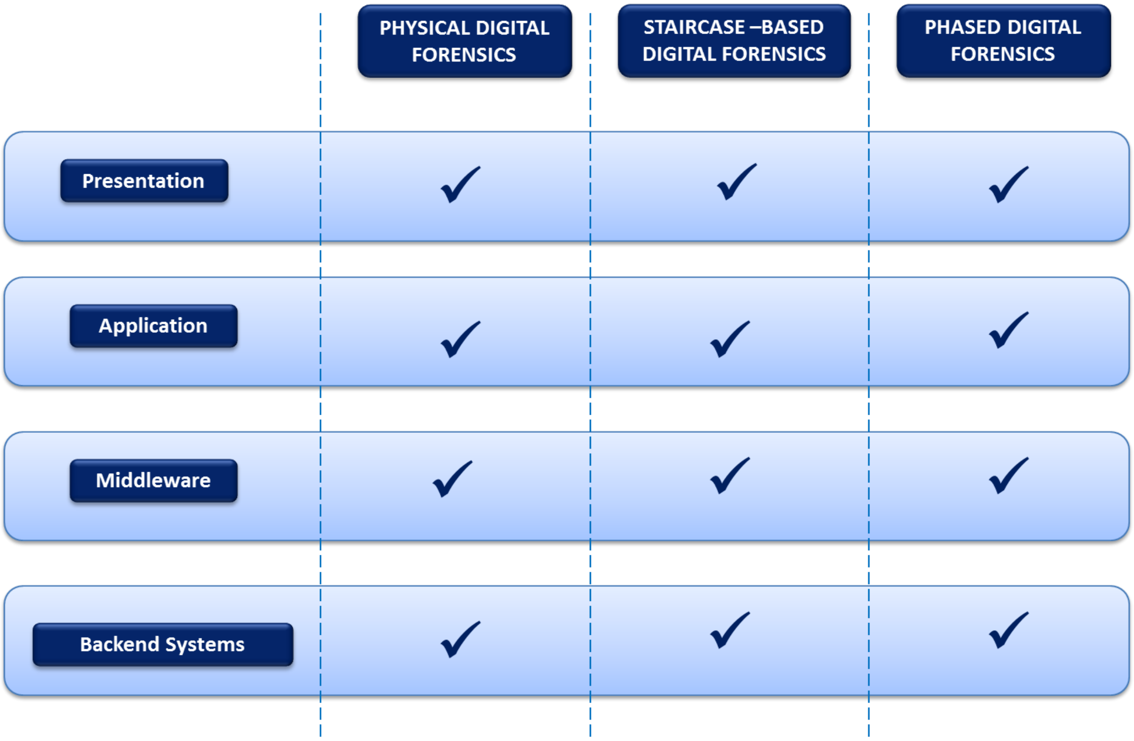
4.3.3.2. Disadvantages

Some methodologies are orientated towards a specific scenario of responding to a critical system that is suspected of being compromised. The granularity of the phases shows the focus on verifying an attack against a live system and restoring the system to its original state.

The framework of Beebe and Clark (2005) attempts to combine steps that are generally separated in other process models. For example, the redefinition of preservation as an overarching principle rather than the process of acquiring data introduces more confusion rather than clarity (Casey & Schatz, 2011). Also, the data analysis step should be separated from examination, as these two activities have different objectives. Although these models are generally a good reflection of the forensic process, some phases are to an extent duplications of another.

4.4. SUMMARY OF DIGITAL FORENSIC APPROACHES IN A MOBILE APPLICATION ARCHITECTURE

The facts revealed by reviewing previous models have shown some redundancies in performing the steps of various phases. Similar to Chapter 3, the various process models to the layers of the mobile application architecture need to be mapped to illustrate where the process model would be best suited to effectively mitigate fraud risk.



	PHYSICAL DIGITAL FORENSICS	STAIRCASE –BASED DIGITAL FORENSICS	PHASED DIGITAL FORENSICS
Presentation	✓	✓	✓
Application	✓	✓	✓
Middleware	✓	✓	✓
Backend Systems	✓	✓	✓

Figure 4.9: Summary of digital forensic models in mobile application architecture

The very nature of forensics entails that a large amount of data would need to be used in order to accurately and effectively investigate each case. For this reason, all discussed models are best suited when used in all layers of the mobile application architecture discussed in Chapter 3. At each layer of the architecture, various types of evidence is collected for examination and analysis. Figure 4.9 provides a summary of digital forensic models in mobile application architecture.

4.5. CONCLUSION

Digital evidence by its very nature is invisible to the eye and is therefore developed using tools that can be easily read and understood by humans. In many of the existing models, the logical investigation process mimics that of paper-based evidence. Several digital forensic frameworks have been proposed, yet no conclusions have been reached about which frameworks are more appropriate. This is to an extent because each framework may work well for different types of investigations. Despite the similarities identified in Section 4.3, the terminology is not well defined and is often inconsistent between process models. For example, the distinction between ‘examination’ and ‘analysis’ is unclear in many of these process models. In general, the differences between these process models may be explained by the way they break down the investigative process; some models use broad categories, whereas others divide the process into more discrete steps.

Developments in forensic research and process over the past decade have been very successful; nevertheless, for all its growing importance, digital forensics practice is often ad hoc and generally lacking in widely accepted theoretical models and principles. The above analysis of existing models proves that a digital forensic process model relies upon reaching a consensus about how to describe digital forensics and digital evidence.

In this chapter, various digital forensic approaches used in the academic environment were discussed. Each approach was discussed briefly with its corresponding terminology and a short analysis of the advantages and shortcomings discussed. The aim of the chapter was to identify some standard method for conducting a digital forensic investigation. Based on the presented computer forensic investigation processes, one is able to extract the basic common investigation phases that are shared among all models.

What can be concluded from this chapter is that the objective of an investigation of a digital incident is often not to trace the incident to its external source but rather to determine the underlying root cause that permitted the incident to be successful in the first place. There are potential benefits from creating a better and more efficient digital forensic approach that will apply appropriate countermeasures to prevent an incident’s reoccurrence. A framework for digital forensics needs to be flexible enough so that it can support future technologies and different types of incidents through its simplicity nature. A unified fraud management and digital forensic framework that takes all previous models into consideration is proposed in the next chapter of this study.

5. A FRAUD MANAGEMENT AND DIGITAL FORENSIC FRAMEWORK FOR MOBILE APPLICATIONS

5.1. INTRODUCTION

Research has shown an increase in the number of published literature on how organisations can improve in detecting, managing, preventing and investigating fraud. Given that these models and approaches exist already, what is the motivation for presenting another one? The existing fraud management and digital forensic approaches are effective, but unfortunately, their effectiveness is in isolation. For example, most fraud management approaches focus mainly on detection and do not put emphasis on other aspects such as deterrence or disruption. Similarly, existing digital forensic approaches focus mainly on the processing of digital evidence, but they are not equipped with techniques, not only of describing the investigative process but also of reconstructing the so-called crime scene in support of the evidence at hand.

The preceding chapter reviewed digital forensic approaches. In this chapter, a conceptual fraud management and digital forensic framework that can support the mobile application architecture landscape described in Chapter 3 is introduced. In doing so, this provides an answer to the fourth research question which related to how unified fraud management and digital forensic framework can be developed for mobile applications. The unified FMDF framework in this study provides a common reference environment for discussions and for the development of tools and technology in the future. In providing this, the intention is to leverage enterprise architecture systems' security capabilities. Since there is a strong correlation between frauds and forensic, it is useful to put in place a combined framework such that fraud management and digital forensics become an end-to-end process for securing organisation's information systems.

The remaining part of this chapter is structured as follows: Section 5.2 discusses the motivation and objectives of the proposed framework as well as discusses the characteristics and phases that make up the framework. A view of how the framework applies to the mobile application architecture discussed in Chapter 2 is then provided. The chapter then discusses the benefits of the unified FMDF framework.

5.2. A UNIFIED FRAUD MANAGEMENT AND DIGITAL FORENSIC FRAMEWORK

5.2.1. Motivation

Patterns of fraud continuously evolve, making it difficult for financial institutions to isolate and proactively prevent such behaviour. As financial institutions grow through and make online-based services available to their clients, it becomes even more difficult to manage the fraud risks that arise as a result of that span in business. It is therefore imperative to guard financial institutions against fraud that would, as a result, threaten the institution's reputation and lead it to bankruptcy. The following challenges are currently experienced by financial institutions:

- The fraud detection and prevention as well as digital forensic teams exist for many financial institutions; however, they do so in isolation.
- Various financial institutions may focus on limited aspects of fraud management as a whole as opposed to the entire lifecycle.
- The digital forensic process is a reactive exercise that is only triggered long after the fraud has already been committed, making it difficult to (a) respond to fraud in time and (b) reconstruct digital evidence; and
- There is limited learning in previous fraud incidents which does not allow for the improvement of robust prevention engines.

To mitigate these challenges, there needs to be a framework that can help correlate and analyse data from a wide variety of sources and interactions in real time; a solution can immediately initiate a process-based workflow to engage the fraud investigation component when a suspicious transaction is detected. Convergence towards a unified framework through the combination of processes and technologies creates an opportunity for financial institutions to benefit from improved mobile application fraud control, reduced complexity and a more cost-effective risk environment.

5.2.2. Objectives

The objective of the FMDF framework is to bring together the essential components of a fraud detection and prevention strategy through the intelligent use of existing approaches. In addition, the framework presents a comprehensive digital investigation process framework that focuses on the concrete principles of the investigation.

The framework aims to enhance organisations' ability to detect fraud through combined use and demonstrate how feedback from digital forensics can assist in enhancing the fraud management as a whole. The framework is aimed at also providing a level of efficiency through the expansion of fraud detection databases with the modus operandi of perpetrators.

5.2.3. Characteristics

No single layer of fraud prevention is enough to keep determined fraudsters out of critical systems or applications. While absolute proof of mobile application fraud may be difficult to obtain, there are many measures that can be used to track user accounts or profiles so that potential fraudulent activities can be flagged (fraud management) and investigated further (digital forensics). Any approach should consist of coordinated measures put in place to prevent, detect and respond to any instances of fraud (State audit institution, 2011). Although each organisation will establish its own specific procedures, effective fraud management has to start with a common understanding of the stages of the fraud management lifecycle. In cases where prevention is not possible, the FMDF framework will deter or detect the fraudulent activity and action accordingly. The proposed approach entails the following characteristics that form the basis of its function:

- **prevention techniques** that stop incidents of fraud from occurring;
- **deterrence mechanisms** that deter potential fraudsters from even attempting any fraudulent activity;

- **disruptive characteristics** that make it as difficult as possible for the fraudster to succeed;
- **the identification of new fraudulent attacks** to help mitigate weaknesses in the environment;
- **the reconstruction of events** arising from the unauthorised intrusion;
- **quicker problem-solving** and better information flows feeding into an investigation;
- **full coverage, scope and assistance** in the investigation procedures; and
- **better knowledge reuse** within and across multiple cases and sharing.

5.2.4. Phases

The FMDF framework leverages the benefits of previously proposed frameworks and models in an attempt to simplify their complexities and at the same time provide a mechanism for including the detail that is needed in the case of mobile application fraud. The framework also takes into account the current challenges experienced by financial institutions and aims to cater for these in the various phases. The framework consists of phases and sub-components which are distinct and represent objectives sought throughout the process. The unified FMDF framework consists of eight phases which are able to run concurrently as outlined in Figure 5.1.

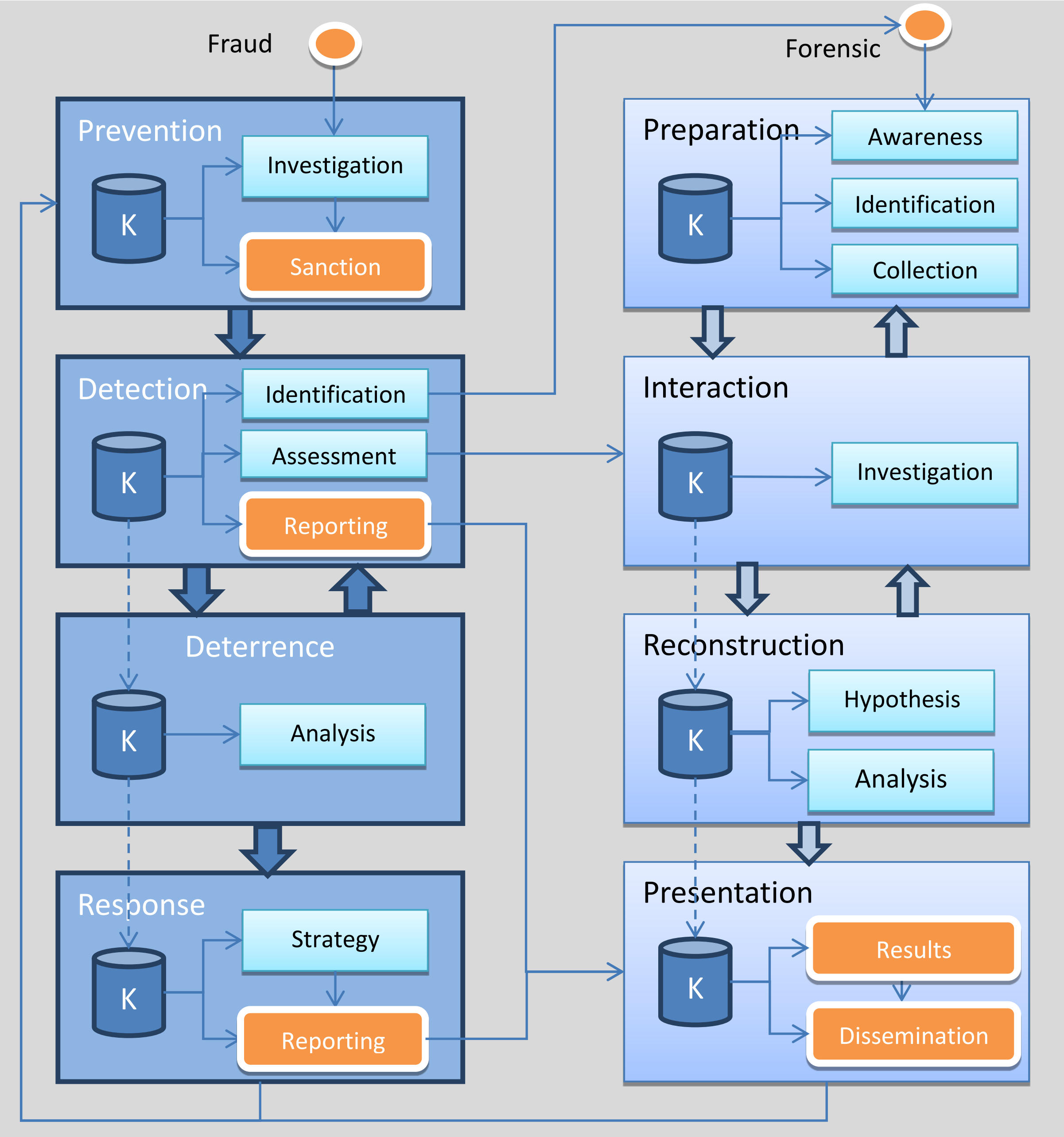


Figure 5.1: The unified Fraud Management and Digital Forensic framework

In the framework in Figure 5.1, some phases that inherently pertain to fraud management would feed to DF when necessary, making the end-to-end security process highly efficient organisation-wide. Phases consist of components that form part of an iterative cycle where fraud management and digital forensic capabilities are continually reviewed and developed. The maturity of the approach increases as the cycle continues.

5.2.4.1. The knowledge base

The introduction of a knowledge base (KB) serves as a central database used to store structured and unstructured information used by the framework. The KB represents facts about user activity and demographics, fraud patterns and other case information that can reason about those facts and use rules and other forms of logic to deduce new facts or highlight inconsistencies. This KB exists in all phases of the framework and serves different purposes.

Depending on the database schema used in the system, a central KB may be used or split for each component within the framework. The KB holds all the necessary knowledge required for facilitating fraud prevention, detection, deterrence and reporting, as well as those required for facilitating forensic investigations. For prevention, for example, the KB consists of all malicious patterns of interactions that may be regarded as fraudulent. This helps prevent fraud as early as possible when a user triggers a process. The content of the KB at the detection phase holds any data pattern that may be regarded as a genuine fraudulent query which will then be fed to other subsequent KB in the framework for further processing (deterrence, forensic and reporting). The KB feeding the forensic part of the framework pertains to those processes that are regarded as genuine fraud and warrant further forensic investigation and subsequent prosecution. The KB therefore plays a pivotal role in ensuring that the evidence is reconstructed for the successful presentation of evidence before a court of law, for example.

5.2.4.2. Prevention

Fraud prevention is about having arrangements in place that reduce the risk of fraud occurrence. It simply means detecting fraud before the damage claim has been paid for (Chartered Institute of Management Accountants, 2008). In this phase, the opportunity is reduced and the temptation of fraud from potential offenders is removed. Previously encountered malicious activities are part of the KB; the investigation component performs a check against the KB to ensure that the process triggered by the user is not of a malicious nature. If all goes well, the detection part is invoked. If not, the user is prevented from proceeding with the query and a ‘sanction’ is taken accordingly. These prevention techniques make use of defined rules of previous fraud cases as well as user profiling procedures and controls to stop fraud from occurring. This phase consists of two components which are described below.

Investigation: The investigation component of this phase queries an existing database with the aim of matching current user activity with that of the potential fraudulent activity. The goal here is to efficiently resolve true fraud from false alerts (Furlan & Bajec, 2008). When a suspicious activity is suspected, a brief investigation will be carried out to determine whether the activity is, in fact, fraudulent or not.

Sanction: When the investigation concludes, sanctioning becomes an important aspect of raising awareness against fraud. The goal of this activity is to support processes aimed at sanctioning fraudsters and reimburse any loss that might have occurred.

5.2.4.3. Detection

The distinct difference between fraud prevention and fraud detection is the current knowledge of data. The core component in the framework is detection; it feeds the overall fraud management and digital forensic process within the entire system. Fraud detection is aimed at detecting known types of fraud and irregularities, as well as anomalies that cannot be directly connected to fraud. Detection methods in the FMDF framework consist of user profiling that identifies anomalies in user behaviour, general rule engines that detect common fraudulent patterns, blacklisting processing to raise immediate alarms, and profiling of a known fraudster through pattern recognition. The component will check the user-triggered query against the KB to ascertain whether the query is fraudulent or not, based on well-known algorithms described above. If the query is deemed fraudulent, the forensic process is triggered; simultaneously, an assessment of such a fraud is performed as well as appropriate reporting. The user-initiated query is recorded for reconstruction purposes at the forensic stage, and the fraud pattern is also recorded in the KB for the deterrent phase. The fraud pattern even feeds into the KB down the hierarchy and subsequently in the prevention KB in order to ensure that such a fraudulent request is not accepted for future use of the system. The following three components make up the detection phase:

Identification: As fraud prevention techniques may not stop all potential perpetrators, it is important for organisations to then ensure that processes that will highlight occurrences of fraud in a timely manner are in place. This is done in the identification step.

Assessment: At this stage of the process, a fraud assessment is performed to identify potential schemes and events that need to be mitigated. This step attempts to identify where fraud occurred. Included in this process is the explicit consideration of all types of fraud schemes, scenarios and opportunities to commit fraud.

Reporting: The introduction of reporting provides for the communication of suspected fraudulent activities. This type of reporting not only focuses on the detection of the current fraudulent acts but also exception reporting and trend analysis to allow for the improvement of internal systems and controls.

The below SQL code provides a description of how the detection will occur in the KB database using data mining should an anomaly be detected:

5.2.4.4. Deterrence

Fraud deterrence is characterised by actions and activities intended to stop or prevent fraud before it is attempted, that is, to turn aside and discourage even the attempt of fraud (Chartered Institute of Management Accountants, 2008). It should not be confused with fraud prevention, which involves identifying and stopping existing fraud. The fraud deterrence phase is similar to detection; however, with this phase, further analysis is performed to check whether the fraud was really genuine or not so as to record it into the KB to ensure prevention in further iterations. In essence, the fraud deterrence phase attempts to reduce the opportunities for committing fraud and limits the ability for potential fraudsters to penetrate and consists of only one component.

Analysis: This component reveals potential fraud opportunities in the process through the analysis of conditions and procedures that affect fraud enablers. Analysis is conducted in order to try and predict what could happen in the future for further improvement of the overall security system.

5.2.4.5. Response

The objective of fraud response is to stop losses from occurring or continuing to occur as well as to hinder a fraudster from continuing or completing the fraudulent activity. The following are further actions taken by the organisation against the fraudster:

A response strategy: This is a formal means of setting down clearly the arrangements in place for dealing with detected or suspected fraud cases. Clearly defined plans help to reduce the damage and minimise the impact or losses that an attack might have had.

Reporting: The reporting phase provides for the communication of fraud cases and the subsequent response chosen. Again, this will add to the current body of knowledge; should there be a case of similar nature, the FMDF framework can react accordingly.

5.2.4.6. Preparation

The preparation phase of the FMDF framework is about the tools and techniques used to carry out investigations. It is part of the forensic process and is triggered when a fraud has been detected, through the identification component in the detection phase. The collection of evidence will then start as well as the real-time investigation. The components in this phase consist of:

Awareness: This involves the creation of awareness that investigation is needed and is typically created by internal events such as intrusion detection alerts.

Identification: Identification involves recognising the incident. It does this through searching an existing database in order to classify the incident type.

Collection: This component involves the collection of evidence in a form that can be preserved and analysed (e.g. date, time of the incident, user information and activity).

5.2.4.7. Interaction

Interaction forms the basis of the investigation process and may take several iterations before moving onto the next phase. Examination is an important aspect of interaction.

Examination: The examination of evidence involves an in-depth systematic search of evidence relating to the incident. Depending on the outcomes of the search/identification and collection activities, there may be very large volumes of data to be examined and thus many iterations and interactions with various steps of the entire process.

5.2.4.8. Reconstruction

Reconstruction is about proving the conclusive descriptions of fraudulent activities. In this stage, a detailed account of the events and actions that occurred at the time of the crime is provided. Reconstruction stems from the detection component; the activity log of the users that emanated from the KB are relied upon to reconstruct the facts that will form part of forensic evidence. The purpose of reconstruction is thus to strengthen forensic evidence so as to secure a possible conviction in the course of law, for example. Hypothesis and analysis are key areas that are considered as far as reconstruction is concerned.

Hypothesis: Based on the examination of the evidence, the investigators construct a hypothesis of what occurred. Constant interaction and backtracking from this activity to the examination activity are to be expected, as a greater understanding of the events which led to the investigation in the first place is developed.

Analysis: This step conducts a post-incident analysis of the events and consists of digital information originally collected in the first phase of the approach, as well as newly generated information. This evidence is analysed to reconstruct information about past events as a result of the incident.

5.2.4.9. Presentation

The final phase of the approach involves the consolidation and presentation of the investigation and results thereof. A successful prosecution means that a tangible fraud committed, and the pattern should be fed into the KB in order to prevent such a fraud from being committed again in the future. Such a pattern might have been recorded in the KB already, long before the prosecution of the fraud; therefore, any subsequent fraudulent query provided by the user immediately after the fraud has been detected will form part of the prevention KB and will therefore not be allowed by the system. However, should the prosecution outcome be unsuccessful, the KB can be amended, depending on the security strategy of the organisation. Since the outcome of the forensic investigation proves that there was no wrongdoing (insuffiecent evidence), the organisation may decide to amend the prevention KB to allow further similar queries or adjust the KB accordingly so that in the advent that a similar query occurs, further security challenges will be prompted to the user. This phase comprises two components, namely, results and dissemination.

Results: Information about the incident is documented as much as possible. This covers a summary of how the incident detection occurred (preparation phase), when the incident occurred, and what the scenario was that led to the incident (interaction and reconstruction phase).

Dissemination: The final activity in the approach is the dissemination of information from the investigation. These results are fed back into the presentation phase to add to the already existing case-based database. This iterative approach adds to the existing body of knowledge and will influence future investigations.

The entire presentation phase that has now successfully consolidated and presented the results will be fed into the prevention phase and start the process again in an iterative manner.

5.3. TECHNICAL EXAMPLE

There are several ways fraudulent transactions can occur through the use of mobile applications. The mobile device may have been lost or stolen, but the owner is yet to report its loss. There might also have been an intrusion into the client's application and thus putting them at a compromising position. As an online merchant, there needs to be a method to check the authenticity of transactions in order to safeguard and organisations business.

In this scenario an organisations online site will authorise an order if the mobile application location address matches the actual user details in the Knowledge Base. Unluckily, the mobile device has been compromised by Mr. ABC from another country through the Internet. Later, he logged onto a banking site and made a using the compromised information. The fraudsters order was then approved by the merchant because all the details matched the client's record in the Knowledge Base database.

In the below code, we use the mobile application location to compare the registered user location details in an effort to lookup country of origin from the visitor's IP address.

The below pseudocode provides a description of how the Knowledge Base is created and how new data is imported into the KB database.

1. *create the knowledge base database*
2. *create the user location table within the knowledge base database*
3. *insert a column within the user location table*
4. *import data from the mobile application into the table*

The below code provides a description of how the user location can be used to trigger fraudulent activity.

5. *initialise unique known mobile code*
6. *retrieve visitor IP address and translate it to IP address number*
7. *lookup valid range of IP address*
8. *assign mobile application location code for reference*
9. *if mobile application code is equal to mobile code then IP address originates from mobile code which equates to low fraud risk*
10. *else if IP address different from mobile code the result is high fraud risk*

5.4. THE FMDF FRAMEWORK IN MOBILE APPLICATIONS

The premise for the suggestion of a unified FMDF framework for mobile applications was based on the fact that most organisations approach fraud management and digital forensics in silos, which is counterproductive. The suggested framework in this study overcomes such a challenge by suggesting an integrated approach to deal with both fraud and forensics at organisational level. From the outset, organisations should be equipped with preventive measures against fraud. Fraud prevention entails ensuring that previously encountered attempts to fraudulent activities are recorded and kept in a knowledge base system-wide in order to learn from past mistakes. As such, the prevention component in the framework plays a pivotal role in ensuring that any suspicious interaction with the system is detected as early as possible and check against what is already known in the knowledge base so as to take relevant action if necessary. When prevention is successful, the overall environment may be regarded as safe from malicious activities. Of course, the system does not stop there; down the hierarchy is the most important detection component representing the core component in the framework of this study. The role of the detection component is to detect any fraudulent activity triggered by a potential criminal and take relevant measures to prevent such activity from occurring in the future. As such, using appropriate algorithms already addressed in detail in this research, the detection component will first identify a fraudulent occurrence, make the relevant assessment and report accordingly. At the same time, since most fraudulent activities ought to be investigated, the detection component has the responsibility to immediately trigger the forensic process at this early stage for security consistency. This will facilitate the overall forensic process pertaining to the detected fraud.

5.5. BENEFITS OF THE FMDF FRAMEWORK

The suggested framework in this study identifies all the relevant information flows, from the moment the fraud is detected till the very last step of dissemination. It is thus an end-to-end process that combines both fraud management and digital forensic principles. Such an approach allows for more efficiency and structure, which minimises room for errors. In the framework, components of fraud management feed into digital forensics and vice versa. This justifies our argument that fraud management and digital forensics should not necessarily be undertaken in isolation, as it is the case in organisations nowadays. Instead, the minimisation of security threats and risk thereof should emphasise on the need of having DF and FM coupled so as to ensure and end-to-end model for managing fraud, securing appropriate prosecution of fraud, and taking remedial preventive measures digitally. The FMDF framework also identifies the need for constant interaction and iteration among phases and between components. At various stages of the process, there is consistent communication, feedback and repetition with all resources that form part of the overall investigation process.

Because the framework presented is inherently a process model, the output of each phase serves as input to succeeding phases; nonetheless, it does not follow a typical waterfall model where activities have to follow one another in sequences. Instead, the approach allows for backtracking and the initiation of other steps. To successfully prevent fraud, the methods in use must be able to provide results in a speedy way. Speed is achieved through the use of various detection methods, such as rule engines and behaviour profiling of both the fraudster and the user. Furthermore, data mining boosts performance through the use of a faster data access characteristic.

For the reason that there is a consistent flow of information throughout, it makes it easier and quicker to detect and efficiently respond to known fraud types. These detection methods described in the FMDF framework are incremental and constantly adapt to new types of fraud and the associated behaviour. Fraudsters will continuously learn of new prevention techniques, and as a result, some knowledge becomes obsolete. It is therefore significant that this approach uses methods that are able to adapt in such a way that they reflect changes in fraudsters’ behaviour. Reporting plays a prominent role in combining and presenting information from various sources. The various reporting phases encompassed in the proposed solution will aid in the increased efficiency of the fraud management and investigation processes.

5.6. CONCLUSION

The unified FMDF framework seeks to use strong elements of fraud management and digital forensics and improve alignment between the fields of fraud management and digital forensics. In fact, it incorporates the existing approaches and process models respectively by recommending that they be used optimally in conjunction.

The first section of the chapter provided an introduction to the framework, followed by a detailed analysis, including motivation, objectives and characteristics of the unified FMDF framework. Various benefits of the framework were also discussed to demonstrate the current limitations and setbacks that the framework overcomes.

The next chapter will explain the data collection process and the research instrument used to validate the proposed framework with industry experts. The chapter also presents results that emanated from the analysis of the data collected.

6. DATA COLLECTION AND ANALYSIS

6.1. INTRODUCTION

The previous chapter provided a discussion that dealt with a fraud management and digital forensic framework for mobile applications. This chapter describes and explains the data collection process and the research instrument used in this study. The chapter also discusses results that emanated from the analysis of the data collected and analysed following the research problem statement highlighted in Chapter 1. From the literature review, various models, frameworks and approaches of fraud management and digital forensics were studied. From the analysis of these models, an integrated framework for fraud management and digital forensics was proposed. However, the proposed framework remains conceptual because it was suggested based on findings from the literature and, as such, ought to be validated in a real-life context. Two fundamental goals drove the collection of the data and the subsequent data analysis. Those goals were first to develop a basic knowledge about the current fraud management and forensic approaches, with focus on their benefits and challenges. Secondly, the goal was to propose a unified framework for fraud management and digital forensics so that investigated limitations can be overcome within the proposed framework of this study in the context of mobile applications.

Therefore, the objective of this chapter is first to describe the instruments used for data gathering and, secondly, to validate and improve the proposed unified FMDF framework. To achieve this, primary research was conducted with the aim of validating the identified factors in the proposed approach for the effectiveness and use of a unified framework for mobile applications in the context of the South African banking industry.

This chapter will bring in a presentation of the findings and analysis derived from an online survey. A total of 40 responses were received from the targeted 79 potential respondents, which constitutes a 50.6% response rate for the survey. Out of 40 respondents, 90% have completed all of the questions that were required to be answered, and 10% of the respondents have either exited the survey half way or have not attempted to answer some of the questions. The responses gathered from the online survey have been analysed using the embedded tool from SurveyMonkey.

This chapter will provide an overview of the data collection methods used as well as the research instrument. This is followed by an explanation of the sample design, followed by findings and analysis of the survey, where tables and diagrams have been used to facilitate a simplistic reader-friendly writing.

6.2. DATA COLLECTION

According to Mouton (2001), collecting or gathering data is done through a variety of methods. Among these, observation, interviewing, testing and analysing texts are the main methods. For this study, the data collection techniques that follow were used.

6.2.1. Data generation

Data was generated through the use of a self-administered electronic structured questionnaire as discussed in Chapter 1. The questionnaire consisted of questions focused on fraud management and digital forensics, and contained both closed- and open-ended questions to accommodate both statistical and thematic analysis of the results. Appendix B provides a complete list of questions within the questionnaire that are aligned to each research objective.

6.2.2. Data description

The responses gathered from the online survey were analysed using the embedded tool from SurveyMonkey. The reference to the data and corresponding numeric values used in statistical analysis can be found in the survey results attached in the appendix (Appendix C).

6.2.3. Response rate

Seventy-nine survey questionnaires were initially sent to individuals identified as having either experience in fraud management or digital forensics. Six survey questionnaires were marked as undeliverable; therefore, 71 questionnaires were considered acceptable for this research. As a result, 40 usable questionnaires were returned; 36 of these were completed accurately, while four respondents either exited the survey half way or have not attempted to answer some of the questions. The detail of the responses will be analysed next.

6.2.4. Quantitative data collection

Quantitative data collection instruments establish a relationship between measured variables. When these methods are used, the researcher is usually detached from the study, and the final output is context-free (Oates, 2006). The advantage of using this type of approach is that it will prevent bias in gathering and presenting the research data to be explained later in this chapter. It will avoid subjectivity by means of collecting and exploring information that describes the experience being studied. In the context of this study, a range of quantitative questions were posed to participating respondents. The results from collected data will then be analysed quantitatively in order to draw relevant conclusions.

6.2.5. Qualitative data collection

A second form of data collection used in this study is that of a qualitative method, which makes gathered data more reliable and objective. The respondents are given an opportunity via free text to describe and give input into the questionnaire responses without constraint. Contrary to the quantitative method, a qualitative approach generates verbal information rather than numerical values (Polgar & Thomas, 2008). Instead of using statistical analysis, the qualitative approach utilises content analysis to explain and comprehend the research findings. The questions posed to the respondents were closed questions, which, however, allowed the respondents free text to indicate their opinion.

6.3. THE RESEARCH INSTRUMENT

6.3.1. Questionnaire content

The chosen research instrument to test the framework proposed in this chapter was a self-administered electronic structured questionnaire (Appendix B), which consists of questions focused on fraud management and digital forensics. The questionnaire contains both closed- and open-ended questions to accommodate both statistical and thematic analysis of the results. The questionnaire was divided into the following sections:

- Section 1: General information and professional experience

  The first section of the questionnaire collected general information about the respondents' professional background and experience. Respondents are asked to give a view of which area of fraud management or digital forensics they are familiar with.

- Section 2: Understanding of mobile application landscape

  This section focused on the respondents' understanding of the mobile application landscape as well as the current threats from a user point of view.

- Section 3: Approach to fraud management for mobile applications

  The third section of the questionnaire was aimed at understanding respondents' approaches to fraud management. This includes detection, prevention and response.

- Section 4: Approach to digital forensics for mobile applications

Similar to section 3 of the questionnaire, this section of the questionnaire aimed to get an understanding of the approach to digital forensics and the current use of the approaches. Furthermore, the aim was to understand the challenges that exist within the current approaches that could be improved.

- Section 5: Critical success factors of the unified approach

  This section aimed at validating the framework as presented in Chapter 5. Questions were formulated in such a way that the analysis of respondents' responses would validate or invalidate the unified process suggested by the framework and also ascertain the importance of the various components used. Qualitatively, some open-ended questions were suggested to capture suggestions from respondents, which were aimed at improving the unified framework.

6.3.2. Questionnaire structure

Most parts of the questionnaire consisted of closed-ended questions that asked the respondent to choose among a possible set of answers – the response that most closely represents their viewpoint. This allowed for the respondent to be restricted to a finite and, therefore, more manageable set of responses. The questions also allowed for free responses that were not followed by any choices. Should the respondent not have made any choices in the possible set of answers, they were able to supply a response by entering short text. This allowed for the addition of new information that was not previously known.

6.3.3. Choice of measuring scale

The Likert survey was the selected questionnaire type to assess the proposed framework, as this enabled the respondents to answer the survey easily. Additionally, this research instrument allowed the researcher to carry out the quantitative approach effectively with the use of statistics for data interpretation. In this survey type, four choices are provided for every question or statement. The choices represent the degree of agreement each respondent has on the given question. The format of the scale is a five-level Likert item and consists of the following options:

- Strongly disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

6.3.4. Validation of the questionnaire

The questionnaire designed for the study was subjected to a validation process for face and content validity. Face and content validity have been respectively defined as “the idea that a test should appear superficially to test what it is supposed to test; and the assurance that the questionnaire will indeed generate data about the concept being studied” (Oates, 2006:131).

Both face and content validity was sought through a review of the draft questionnaire by academic supervisors. Once complete, feedback was incorporated and a revised draft of the questionnaire produced. Furthermore, content validity was tested using a pilot study with three respondents. These respondents as well as their answers were not part of the actual study process and were only used for testing purposes. After the questions have been answered, the respondents were asked for any suggestions or any necessary corrections for improvement. The survey questionnaire was then revised based on the suggestions of the respondents to ensure that each question in the questionnaire is brief, relevant, unambiguous, specific and objective.

6.3.5. The research tool

SurveyMonkey was chosen as the tool to construct and disseminate the questionnaire. The tool was chosen for its ease of use and a full list of features in designing and analysing questionnaire responses. Being a web-based tool also allowed the respondents to complete the questionnaire online in their own time and space, without having to download any specific software.

6.4. SAMPLE DESIGN

6.4.1. Population

The population researched was that of the banking environment. On average, it consists of a team of 30 individuals that deal with fraud management or digital forensics as part of their responsibilities. Five banking institutions in South Africa were chosen as part of the study, which, therefore, makes the population an estimated 150 people.

6.4.2. Sampling frame

Oates (2006) defines a sampling frame as a list or a collection of the whole population of people that could be included in the survey. The sampling frame for this study was professionals in the banking industry.

The sampling criteria for this research were

- individuals residing within South Africa;
- individuals in the South African banking industry;
- professionals who have experience in fraud management; and
- professionals who have experience in digital forensics.

6.4.3. Sampling technique

There are two types of sampling techniques: probability and non-probability sampling. Probability sampling is chosen when the researcher believes that there is a high probability that the sample of respondents chosen is a representation of the overall population being studied (Oates, 2006). With non-probability sampling, on the other hand, the researcher does not know whether the sample of people is representative, as respondents might have unique characteristics. An overview of sampling techniques is depicted in Table 6.1.

Probabilistic	Non-probabilistic
Random	Purposive
Systematic	Snowball
Stratified	Self-selection
Cluster	Convenience

Table 6.1: Sampling techniques
Source: (Oates, 2006)

The sampling technique utilised in this study is non-probability, purposive sampling. Professionals in the banking industry were deliberately selected to participate in the survey, as they are more likely to produce valuable data that meets the purpose of this research.

6.4.4. Sample size

The sample population chosen is 130 on a 95% confidence level and accuracy range of 3%. The accuracy range is the margin of error that reveals how close to the true population value the research is. A confidence level of 95% means that one is 95% sure that the true population value falls within the range of values obtained from the sample (Oates, 2006). At a target population size of 150, the required sample size for a 95% confidence level and a 3% accuracy range is 130.

6.5. DATA ANALYSIS AND FINDINGS

The data gathered in this quantitative study was analysed manually. Based on the analysis and interpretation of results achieved, answers to the various research questions described in Chapter 1 are provided. The various sections of the questionnaire will now be analysed.

6.5.1. General information and professional experience

The first section of the questionnaire aimed at collecting general information about the respondents' professional background and experience. The profile of the respondents is considered in terms of years of experience as well as their involvement and understanding of fraud management or digital forensics.

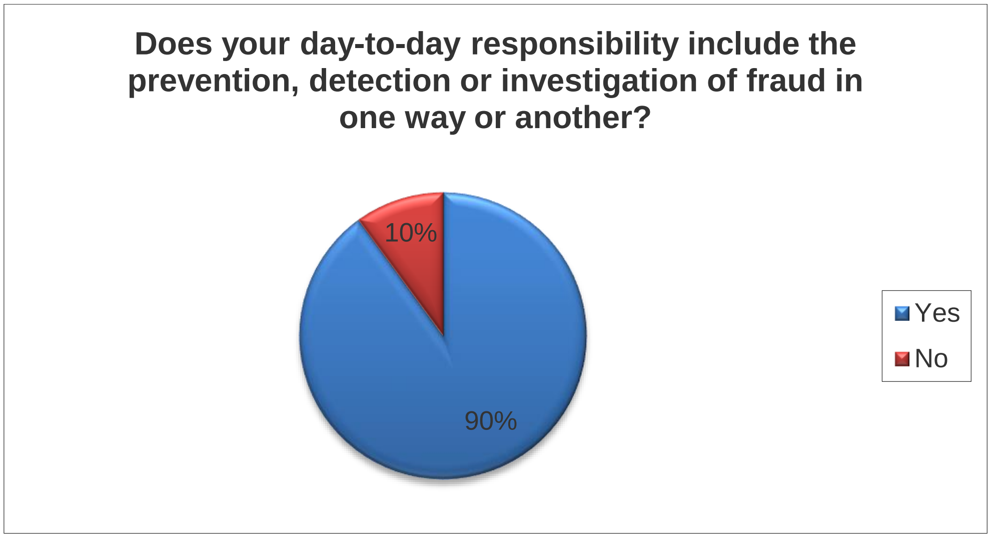


Figure 6.1: Current responsibilities of respondents

To verify that the targeted participants were correctly identified to participate in the survey, the first question was used to confirm whether their current or past responsibilities included the prevention, detection or investigation of fraud. Ninety per cent of the participants responded 'yes', while the remaining 10% said 'no', as illustrated in Figure 6.1. It should be noted that the selection criteria used to identify participants was based on their corporate role that falls within either the forensic department or the fraud management department of their organisation. The 10% of participants who responded negatively may be justified by their current functional role, which may not involve direct contact with digital forensics or fraud management; this is reasonable in that they may fulfil a more managerial than operational role in their organisation.

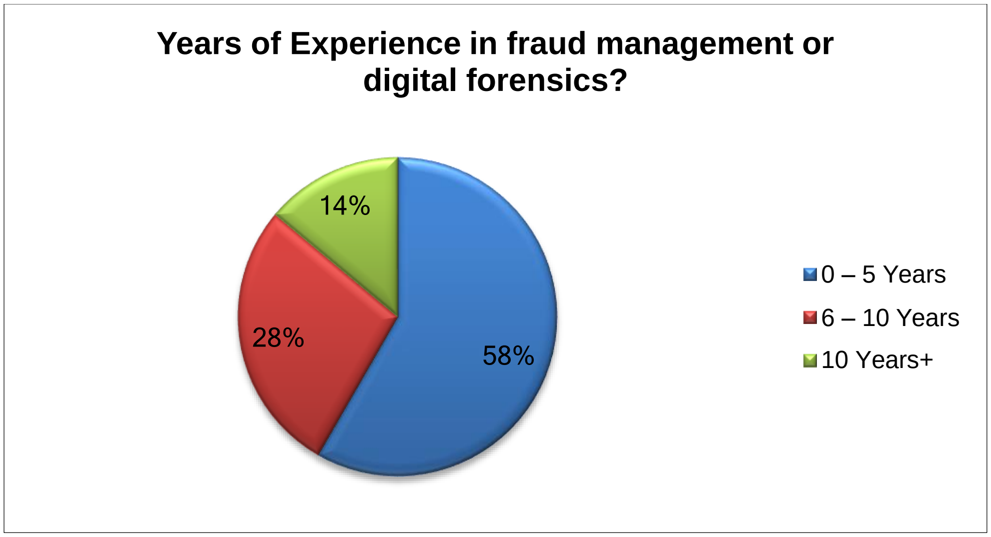


Figure 6.2: Respondents' years of experience

In an attempt to obtain a clearer picture of the respondent, the participants were also asked about the number of years of experience in either fraud management or digital forensics. According to Figure 6.2, a majority of the respondents (58%) had between 0-5 years' experience, while 28% of the respondents had 6-10 years' experience. The remainder of the respondents had over 10 years' experience.

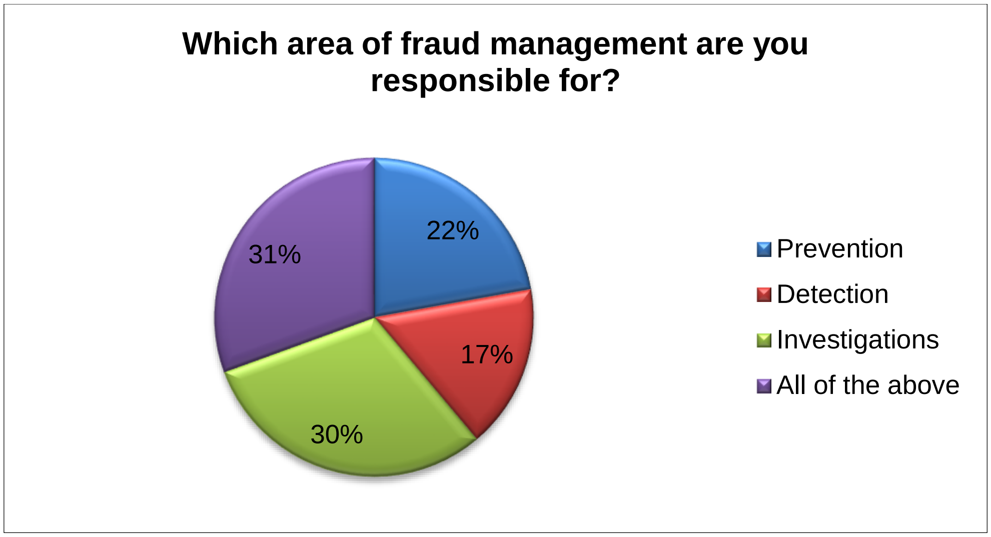


Figure 6.3: Overall fraud management responsibilities

Figure 6.3 illustrates the general split in fraud management and digital forensics that the respondents are responsible for. Thirty-one per cent of the respondents indicated having had previous experience in all three components of fraud management and digital forensics. The remainder of the responses is split between investigations, prevention and detection, which constitute 30%, 22% and 17% of the findings respectively.

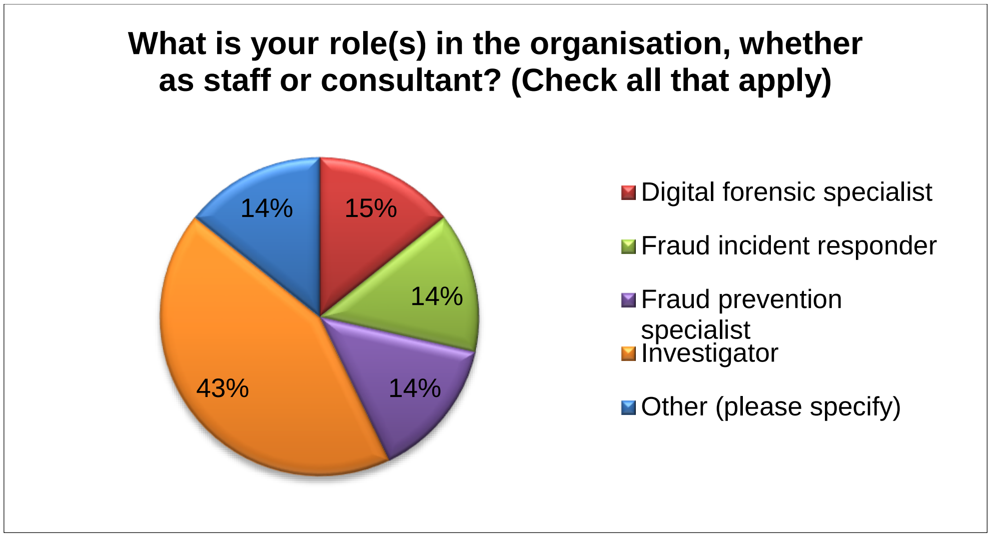


Figure 6.4: Role in the organisation

As a continuation of Figure 6.3, Figure 6.4 assesses the respondents' current or past roles within their organisation. Forty-three per cent of respondents indicated their roles being that of investigators. An almost equal average of 14% is split between digital forensic specialists, incident responders and fraud prevention specialists. Studies have shown that prevention is the most cost-effective way to prevent loss through fraud; however, the synopsis of Figures 6.3 and 6.4 suggests that organisations take a rather reactive approach when it comes to fraud management and digital forensics. Such outcome further strengthens the argument that organisations should be more proactive in such endeavour. The 14% of respondents who chose 'other' did not give an indication as to what other role they perform outside of what was listed, which actually corroborates with the analysis of the first question.

6.5.2. Understanding of mobile application landscape

Mobile applications have grown to support a much wider range of activities than desktop applications and are built to either extend an existing business system or will interface with an existing system. The second section of the questionnaire focused on the respondents' understanding of the mobile application landscape as well as the current threats from a user point of view. The findings below examine the respondents' understanding of the general architecture.

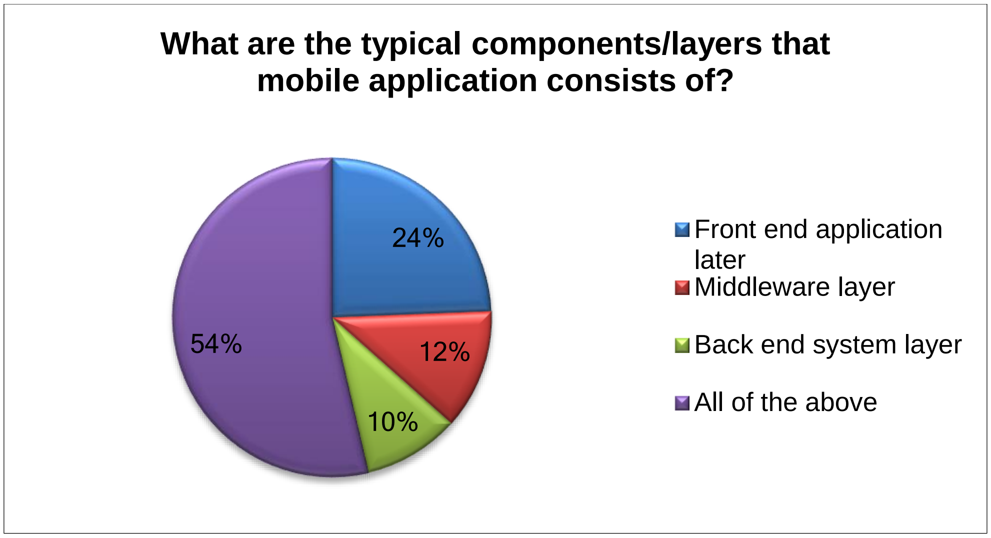


Figure 6.5: Understanding of mobile application architecture

A majority of the respondents (54%) generally understood the general components of a mobile architecture to include all three layers as portrayed in Figure 6.5. Twenty-four per cent of the respondents agreed that the frontend application layer was also a component of the architecture. However, it is important to note that this layer does not run on its own and that its objective is to support the main functionalities of the existing system. The middleware layer's purpose is to provide data transformation, apply business logic, and be a central point of communication for the devices. The backend layer is the hub, where all information is stored, and its main function is to carry out operations for a specific application.

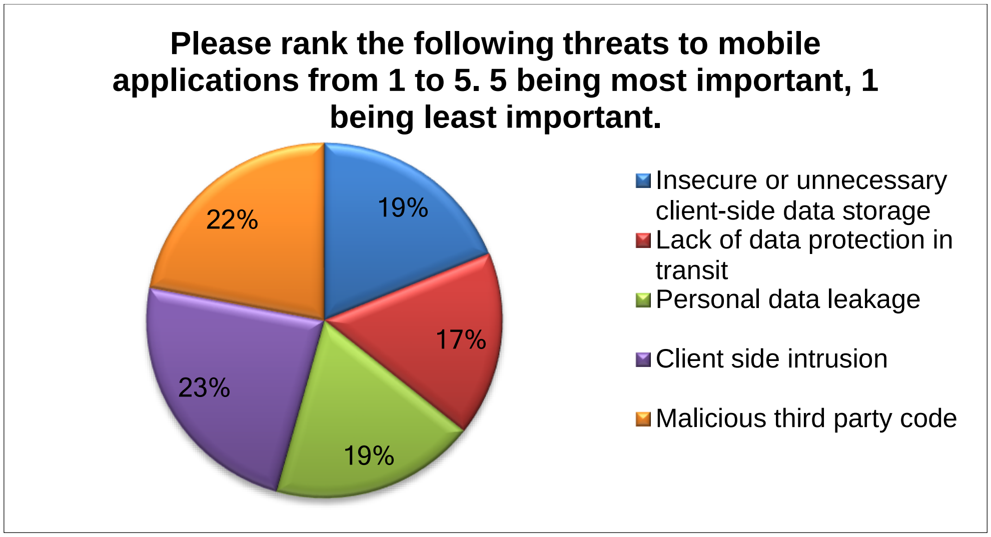


Figure 6.6: Threats to mobile applications

Chapter 3 gave a high-level overview of the current top 10 mobile applications threats, of which the top 5 were presented to the participants, and they were asked to rank them according to their experience. The results in Figure 6.6 did not vary too much and yielded an overall average split of 20% for each threat. Client-side intrusion, which forces a database to yield otherwise secure information, ranked highest (23%) on the threats to mobile applications, with malicious third-party code, which usually comes in the form of a Trojan horse that masquerades as legitimate software, ranking second highest (22%) on the list. An almost equal response was received for the remaining threats, which shows that organisations are generally concerned about the common threats to their mobile platforms. One can summarise this by concluding that the confidentiality, integrity and availability of data are integral for continued business operations.

6.5.3. Approach to fraud management

The third section of the questionnaire aimed to get an understanding of respondents' approach to fraud management. This includes the common stages of the fraud management lifecycle defined in Chapter 3 that consist of deterrence, detection, mitigation and investigation.

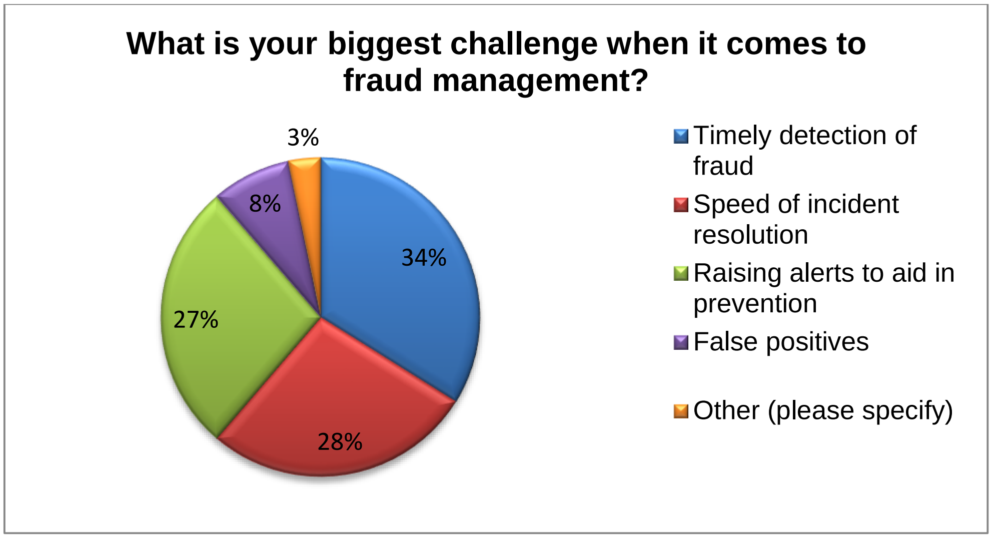


Figure 6.7: Challenges with fraud management

When asked what the biggest challenge was when it came to fraud management, 34% of the respondents indicated that the timely detection of fraud was the most challenging factor. The time it takes to resolve an incident as well as making an alert ranked second highest to the biggest threats, with 28% and 27% respectively, as indicated in Figure 6.7. It can be assumed from these results that either inductive fraud detection, which proactively searches for fraud without determining the type of fraud to look for, or deductive fraud detection, which determines the types of frauds that can occur then queries the data set to see if they exist, is of importance to organisations. A small percentage of respondents were concerned about false positives, which suggests that most respondents would rather receive alerts and investigate to determine the validity than not receiving any alerts at all.

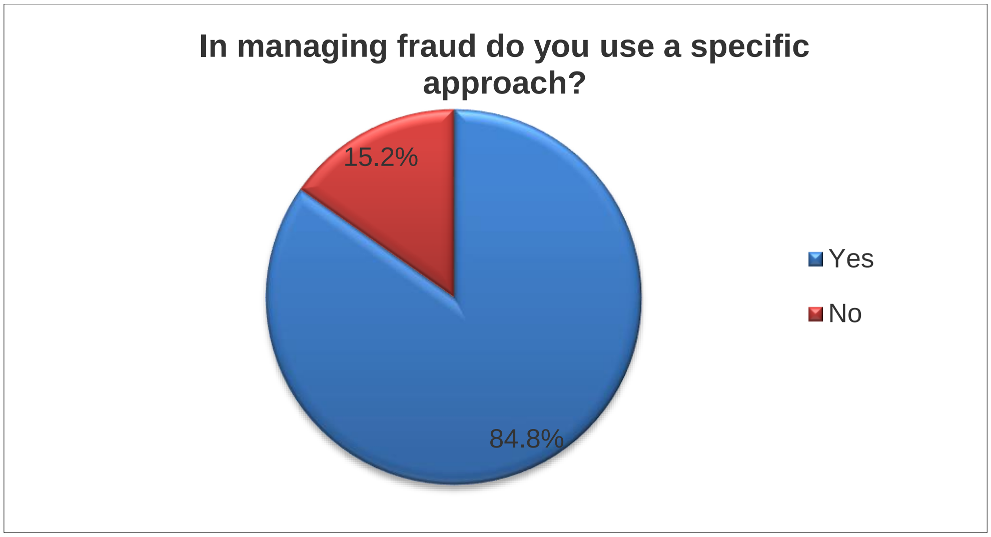


Figure 6.8: Use of fraud management approach

Figure 6.8 reveals the results of the respondents when asked whether a specific or defined approach was used to manage fraud. Eighty-five per cent of the respondents indicated that an approach was used, while 15% indicated that none was used.

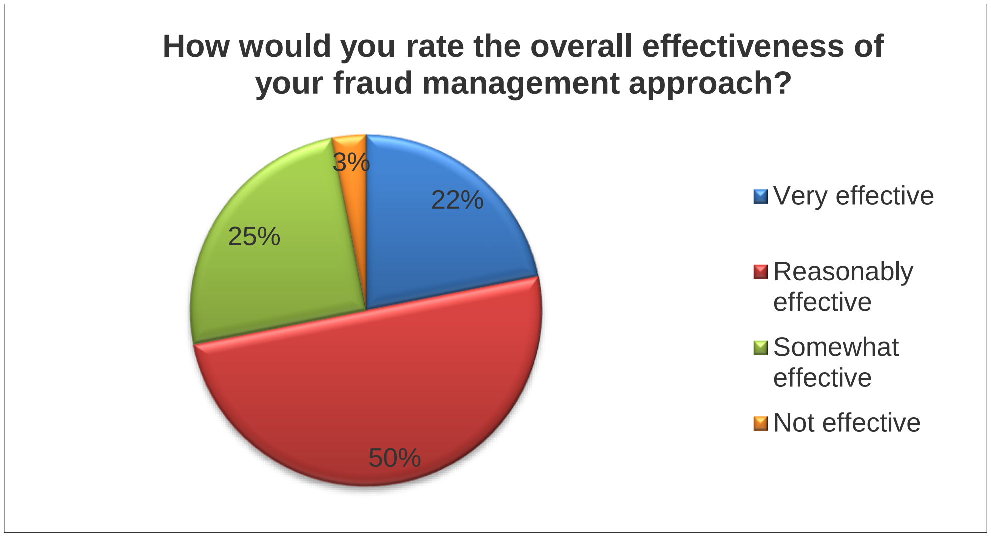


Figure 6.9: Effectiveness of the respondents’ fraud management approach

Respondents were also requested to rate their current approach towards managing fraud. Seventy-two per cent of the respondents were satisfied with the current approach, with 22% rating their framework as very effective. Figure 6.9 shows the spread of responses on overall effectiveness.

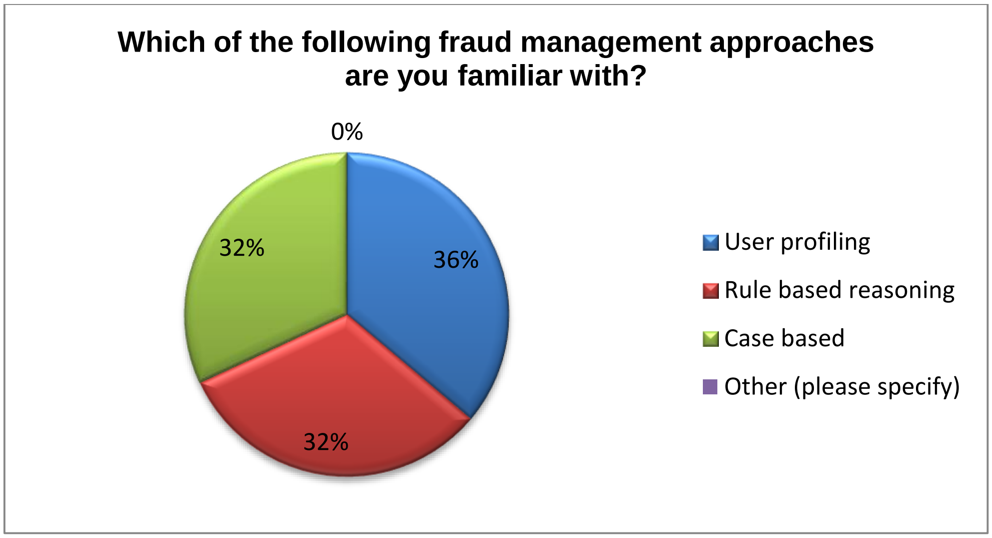


Figure 6.10: Approaches to fraud management

The next question was to assess the familiarity of respondents with regard to fraud management approaches. Results highlighted in Figure 6.10 reveal that all respondents were familiar with existing approaches, with the majority of them (36%) being more familiar with the user profiling approach.

6.5.4. Approach to digital forensics

Similar to the preceding subsection, this section of the chapter aims to get an understanding of the approach to digital forensics and the current use of the models.

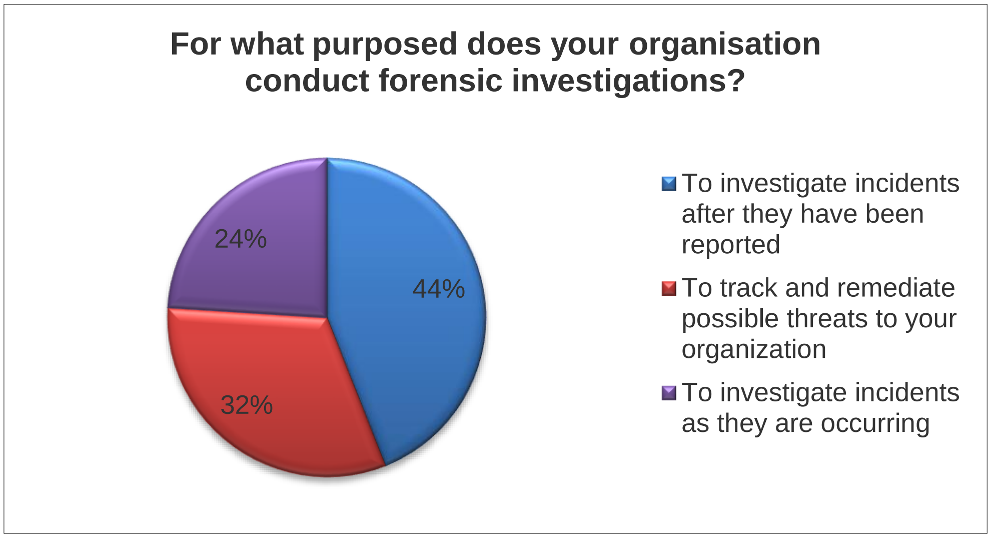


Figure 6.11: Use of forensic investigations

The question posed in Figure 6.11 was asked to gain a better understanding of the use of digital forensics within an organisation. Forty-four per cent of the respondents indicated that their biggest use of forensics was to investigate incidents after they had been reported, while 24% of the respondents revealed that forensics was also used to investigate and remediate incidents as they occur. In addition, 32% of the respondents use forensics for more than just incident resolution, but rather as a proactive measure to track and attempt to remediate possible threats to their organisations.

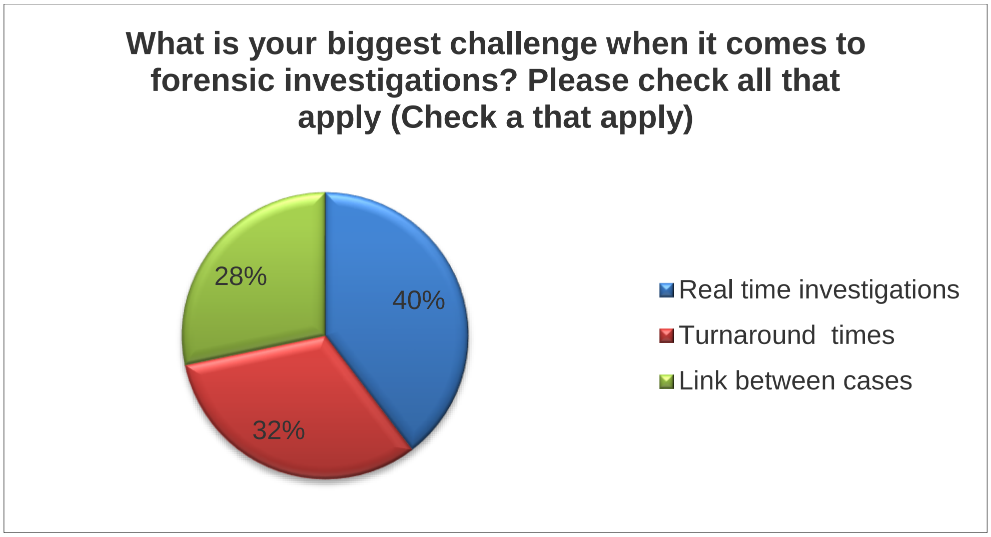


Figure 6.12: Challenges with forensic investigations

When asked what their biggest challenge was regarding investigations, three options were given. In Figure 6.12, 40% of the respondents agreed that the inability to do real-time investigations was a concern; this was followed by 32% of the respondents who argued that quick turnaround times were of concern. The remaining 28% maintained that finding a link between various cases was also a challenge.

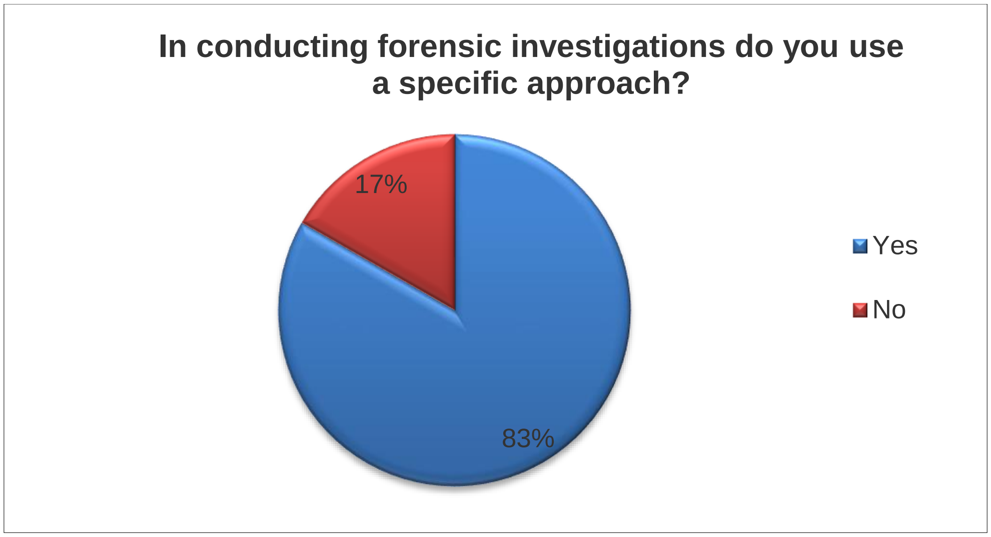


Figure 6.13: Use of forensic approaches

Figure 6.13 highlights the results of the respondents when asked whether a specific or defined approach was used when conducting a forensic investigation. Eighty-three per cent of the respondents indicated that an approach was used, while 17% indicated that none was used.

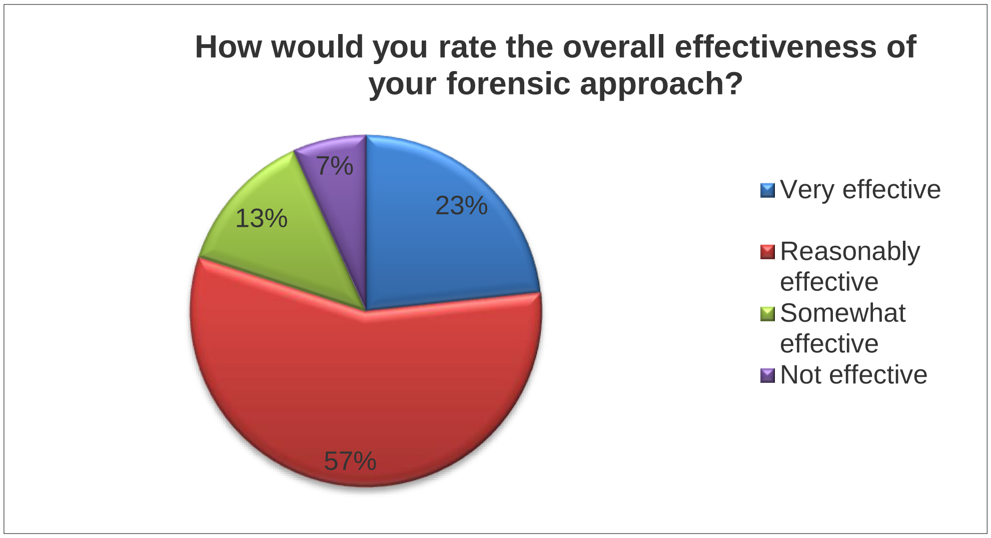


Figure 6.14: Effectiveness of forensic approach

Respondents were also requested to rate their current approach towards forensic investigations. A majority of the respondents (80%) were satisfied with the current approach, which was split between very effective (23%) and reasonably effective (57%). Figure 6.14 shows the spread of responses on overall effectiveness.

6.5.5. Critical success factors of a unified approach

The last section of the questionnaire was intended to test the use and applicability of the unified approach. The Likert scale was used to interpret that section of the questionnaire. These responses were based on the respondents' assessment of the statements presented that refer to the proposed unified approach. The scale is in a category of 1-5, signifying levels of agreement and disagreement with certain statements raised by the questionnaire. The range and interpretation of the five-point scale are shown in Table 6.2.

Scale	Interpretation
1	Strongly disagree
2	Disagree
3	Neither agree nor disagree
4	Agree
5	Strongly agree

Table 6.2: The Five-point Likert scale

The results of the survey are presented and discussed next.

6.5.5.1. Results

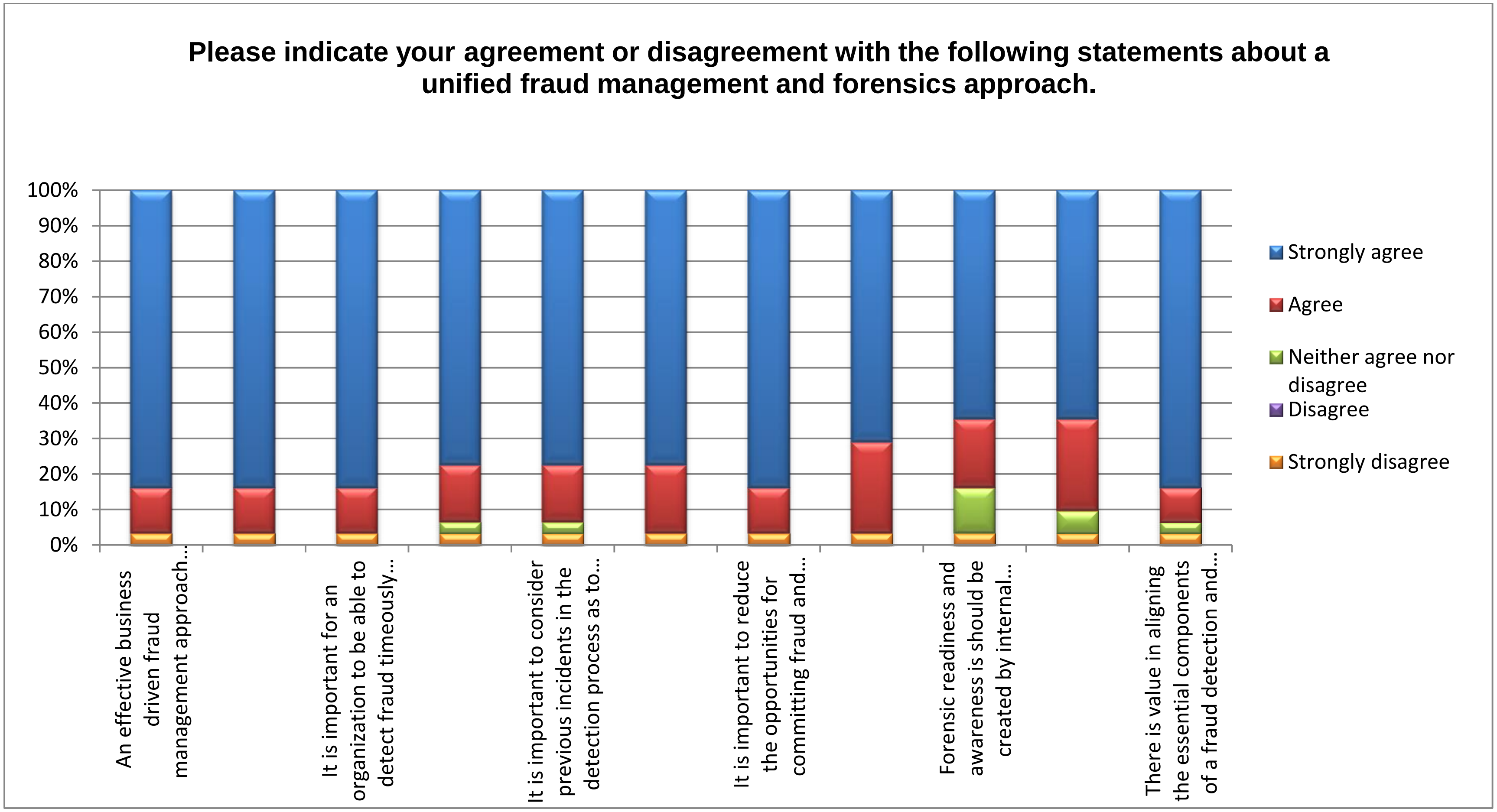


Figure 6.15: Analysis of a unified fraud management and digital forensic approach

Statement 1: An effective business-driven fraud management approach encompasses controls that have three objectives: prevent, detect and respond.

Although each organisation would establish its own specific procedures, effective fraud management has to start with a common understanding of the stages of the fraud management lifecycle. This first statement was aimed at assessing the respondents' understanding of the objectives and components of an overall fraud management approach. Ninety-seven per cent of the respondents (including 84% who strongly agree and 13% who agree) concurred that an effective business-driven fraud management approach is one that encompasses prevention, detection and response.

The prevention phase of a unified FMDF approach is about having arrangements in place that reduce the risk of fraud occurring by decreasing the opportunity and removing the temptation of fraud from potential offenders. At the same time, the detection capability's objectives are about detecting known types of fraud and irregularities, as well as anomalies that cannot be directly connected to fraud. Finally, the response controls in the unified FMDF approach will set down clearly the actions to be taken should fraud be detected or suspected.

Statement 2: Ideally, an organisation should be able to prevent fraud before it occurs.

It was noted earlier that fraud prevention reduces the opportunity of fraud from occurring by removing the temptation to potential offenders and other means. Ninety-seven per cent of the respondents agreed with Statement 2 (including 84% who strongly agree and 13% who agree). Ideally, when a suspicious activity has been brought to light, an organisation should be able to promptly investigate it and invoke response strategies for its mitigation. In the FMDF framework, for example, an existing database hosting a range of suspicious activity trends is queried in order to match the current activity with that of the potential fraudulent activity. Should a match be detected, the appropriate response is applied immediately.

Statement 3: It is important for an organisation to be able to detect fraud timeously and remediate it as quickly as possible.

One can never completely eliminate every type of incident that occurs as a result of fraudulent activities. The above statement assesses the respondents' agreement or non-agreement to the timeous resolution of known fraud incidents. The preparation phase of the FMDF approach involves first creating awareness of the incident, which is typically generated by internal controls such as alerts. In the case of the FMDF framework, the speed is achieved through the use of various detection methods, such as rule engines and behaviour profiling of both the fraudster and the user. Ninety-seven per cent of the respondents agreed with Statement 3 (including 84% who strongly agree and 13% who agree).

Statement 4: A formal detection and prevention approach is important in developing an effective fraud management approach.

The FMDF provides an abstract framework independent of any technology or organisational environment. The approach consists of coordinated measures put in place to prevent, detect and respond to any instances of fraud with specific procedures. Ninety-four per cent of the participants agreed that a formal detection and prevention approach to fraud management is necessary.

Statement 5: It is important to consider previous incidents in the detection process so as to learn from previous cases.

All relevant data for detecting fraud attempts may not be at hand at the time that an incident occurs. Detecting known types of fraud and irregularities/anomalies is a good place to start, according to 94% of the respondents who agreed with this statement. The FMDF approach makes use of detection methods such as general rule engines that detect common fraudulent patterns.

Statement 6: It is important to profile customer behaviour in order to assist in detecting anomalies related to fraudulent behaviour.

Similar to Statement 5, Statement 6 assesses the positives that behaviour profiling might have. This does not only include profiling the behaviour of a customer but also that of the fraudster in order to study the typical modus operandi. The information in a user profile may include various attributes of a user such as geographical location, academic and professional background, interests, preferences, as well as opinions. These users often have repetitive behaviours within software applications that can be observed and stored in their individual profiles. When given the remark about the importance of profiling user behaviour to assist in the detection of fraud, a 97% agreement response was obtained.

Statement 7: It is important to reduce the opportunities for committing fraud and limit the ability for potential fraudsters to penetrate.

Fraud deterrence is characterised by actions and activities intended to stop or prevent fraud before it is attempted, that is, to turn aside or discourage even the attempt at fraud (Wilhelm, 2004). The fraud deterrence capability of the FMDF approach attempts to reduce the opportunities for committing fraud and limit the ability of potential fraudsters from penetrating. Ninety-seven per cent of the respondents agreed that it was important to reduce opportunities for fraud and the environment in which they are able to penetrate.

Statement 8: A fraud response strategy is an essential means of setting down clearly the arrangements in place for dealing with detected or suspected fraud cases.

The goal of fraud response is to stop losses from occurring or continuing to occur as well as hinder a fraudster from continuing or completing the fraudulent activity. A response strategy consists of a set of rules that are implemented, should particular criteria be met. Ninety-seven per cent of the respondents agreed that a fraud response strategy is essential in setting down clearly the arrangements in place for dealing with detected or suspected fraud cases. As in the FMDF approach, having a clearly defined plan will help lessen the damage and minimise the impact or losses that an attack might have had.

Statement 9: Forensic readiness and awareness should be created by internal events such as the intrusion detection alerts to allow the investigation to happen almost immediately.

Earlier on in the study, when respondents were asked what their biggest challenge was with respect to forensic investigations, they indicated real-time investigations as well as the timely conclusion of investigations as their challenges. This is because the trigger for forensics to occur is currently through the reporting of an actual fraud case. The FMDF approach uses awareness, typically created by internal events such as intrusion detection alerts, to notify the need for an investigation process to begin. When presented with the above statement, 84% of the respondents showed agreement to the statement, while 13% remained neutral.

Statement 10: A post-incident analysis of the event can enhance the already existing body of knowledge about fraudulent cases.

A post-incident analysis consists of the reconstruction of an incident to assess the chain of events that took place. Ninety per cent of the respondents agreed that a post-incident analysis could enhance the body of knowledge of fraud cases. As seen in Chapter 5, the FMDF approach allows for this. Based on the examination of the evidence, investigators are able to construct a hypothesis of what actually occurred through constant interaction and backtracking. This is done in order to develop a greater understanding of the events which led to the investigation in the first place and, as a result, contribute to the existing database of known fraudulent behaviour.

Statement 11: There is value in aligning the essential components of a fraud detection and forensic investigation through the intelligent use of both approaches.

The objective of this last statement was to round up the thought process that the respondents would have gone through when completing the questionnaire. Based on their previous experience, their rating of current approaches as well as challenges noted, the respondent would be able to better assess the need for a unified approach. Ninety-four per cent of the respondents established that there is value in aligning the essential components and fraud management and forensic investigation processes and approaches. As noted in Chapter 5, the unified FMDF approach brings together the optimal fraud management and digital forensic approaches to present them as one. The approach brings together the essential components of these models through the intelligent use of both approaches. It demonstrates (1) how feedback from digital forensics can assist in enhancing the fraud management approach (2) how fraud detection is able to trigger the forensic process, therefore rending it more proactive.

6.6. CONCLUSION

This chapter provided a description of the data collection procedures implemented in the research method. The research apparatus used, the content of data, the structure and validation thereof were subsequently discussed. This chapter also gave a detailed account of the survey performed to understand the current approaches to fraud management and digital forensic investigations, as well as obtain an opinion about the proposed unified approach for mobile applications. Data was collected through the use of an online self-administered questionnaire that was divided into five sections. The first section was used to gather the respondents' demographic and professional experience, while the second section analysed their understanding about the mobile application architecture. The second and third sections then went on to study the respondents' experience and challenges relating to fraud management and digital forensics respectively. The objective of the last section (section 4) was to test the respondents' agreement or disagreement with the proposal of a unified approach to fraud management and digital forensics. Various graphs were used to illustrate the survey results and the interpretation and analysis of each question and response. The final chapter discusses findings and conclusions, and makes reflections and recommendations for further research.

7. CONCLUSION AND RECOMMENDATIONS

7.1. INTRODUCTION

This research was initiated with the aim, first, to understand the fraud landscape for mobile applications; secondly, to investigate the various approaches and models used for fraud management and digital forensics respectively. Finally, it was the aim of this research to investigate the value and use of fraud management and digital forensic components through a unified approach. The research's aims were achieved by reviewing pieces of literature as well as conducting surveys with subject matter experts.

Having conceptually proposed a unified FMDF framework in Chapter 5 and undertaken a survey aimed at its validation, the purpose of this concluding chapter is to summarise the research study and provide recommendations based on feedback received from expert evaluations through the survey conducted. This chapter will first start by depicting an improved and validated FMDF framework based on findings that emanated from the survey. A summary of the dissertation will then follow by ascertaining that identified objectives set out in the introductory chapter have been achieved. In Section 7.5, some indications will be provided about future research that can span from this study. The last section will summarise and conclude the study.

7.2. IMPROVED FRAUD MANAGEMENT AND DIGITAL FORENSIC FRAMEWORK

Based on the feedback received from the participants, an improved FMDF framework is suggested. The framework now portrays the unified nature that the study has been advocating, and fraud management and digital forensics are now seen as an integral exercise instead of being considered in isolation. Figure 7.1 illustrates the improved framework.

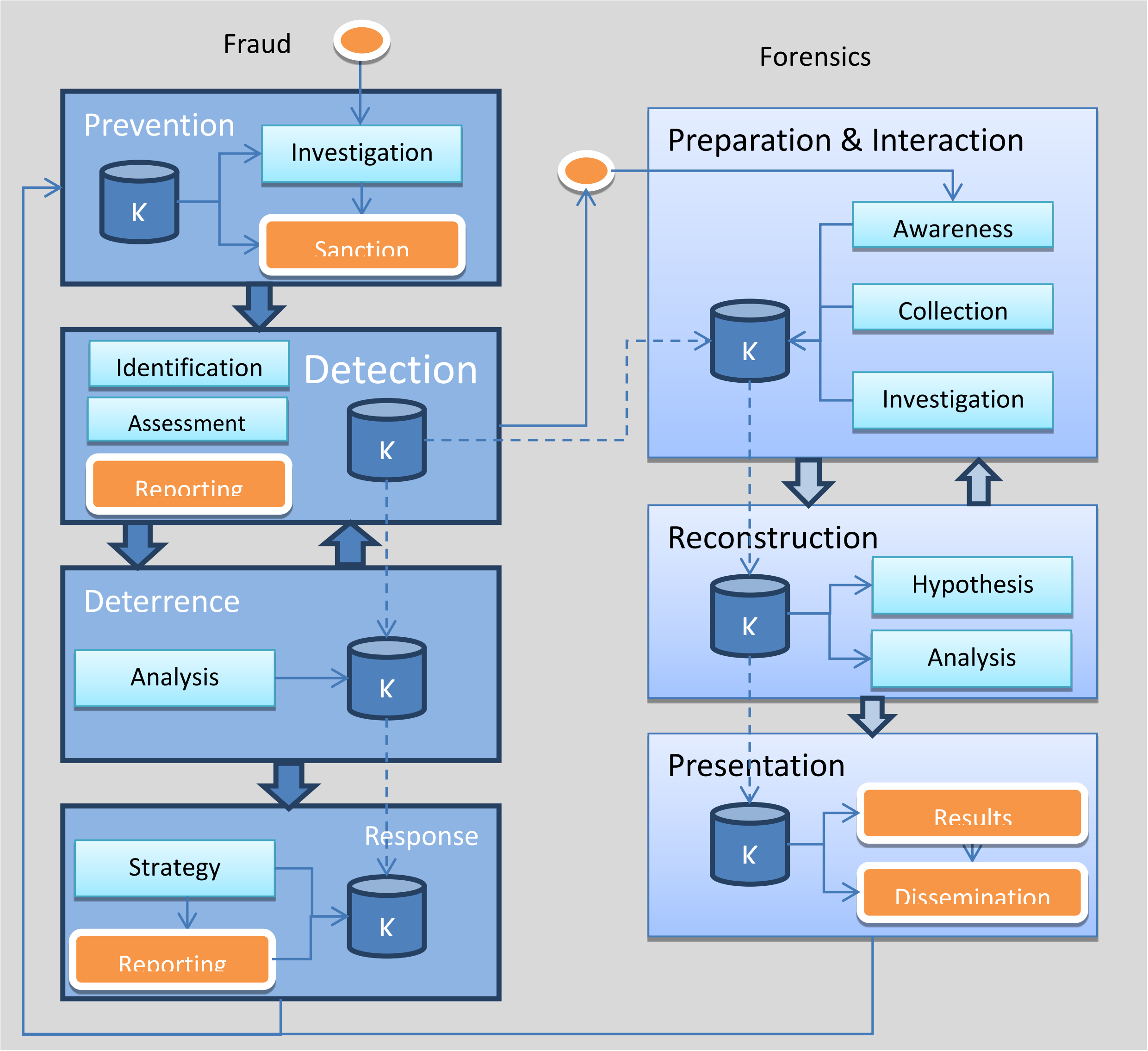


Figure 7.1: Improved unified FMDF framework

The improved unified FMDF framework allows for digital forensics to become integrated into the fraud management process and is triggered by detection. This means that once fraud is detected, forensics starts immediately, even if at a later stage investigations reveal that it might have been a false alert or not. The improved FMDF framework now caters for true integration through the combination of the preparation and interaction phases.

7.3. RESEARCH FINDINGS

The central focus of this study was the proposal of a unified FMDF framework for the handling and investigation of fraud for mobile applications. Although existing approaches, models and frameworks were identified and analysed in the literature, this study demonstrated the importance of a consolidated framework for handling fraud management and digital forensics on a proactive manner in organisations. In addition to the review of existing literature that lead to the conceptualisation of the framework, findings from the survey corroborated with the need for such a unified framework. The research questions presented in Chapter 1 and undertaken in Chapters 2, 3 and 4 guided the development of the proposed FMDF framework. The framework was fully described in Chapter 5 in terms of the stages, components and inputs and outputs relevant to each stage.

The research was conducted using a survey where participants completed online, self-administered questionnaires that pertained to the evaluation of the proposed framework. The participants identified as role players in the design of the framework were analysts, fraud managers, forensic investigators, prevention specialists and managers in the banking industry. The quantitative data collected through the survey was analysed and presented in Chapter 6 through the use of graphs.

An enhanced understanding of fraud management and digital forensics and its role in mobile applications was achieved. Participants responded favourably to the proposed unified FMDF framework and highlighted the benefit of achieving cohesion and integration when mitigating risks to fraud.

7.4. RESEARCH SUMMARY

This research was initiated with the aim of first understanding the fraud landscape for mobile applications. Secondly, the aim was to investigate the various approaches and models used for fraud management and digital forensics respectively. The final aim was to investigate the value and use of fraud management and digital forensic components through a unified approach. To achieve this, three sub-objectives stated in Chapter 1 provided guidelines for the study.

The sub-objectives were explored in various chapters of this research and are further examined here to establish the extent to which they were achieved. Each of the subsections that follow explores a particular objective. The findings are based on information that was obtained from the participants surveyed. Findings made by this study are stated under the respective sub-objective together with brief discussions.

7.4.1. Sub-objective 1: Investigate mobile applications, their architecture and threat landscape

The first sub-objective of the study was explored in Chapter 2 where the study characterised mobile applications and identified the various challenges faced by their usage from a fraud risk perspective. The study also went into details about the growing trends in mobile applications, including the diversity of application types, their impact on the enterprise and consumer. Furthermore, the architecture of a mobile application, as well as the threat landscape associated with each layer, was identified. Table 7.1 provides a summary of the threat modelling of mobile applications.

Threat	**Application layer**
Physical theft	Presentation
Phishing	Application
Open connectivity	Application; Middleware
Spyware	Application; Middleware; Backend systems
Networking exploits	Application; Middleware; Backend systems
Trojan horses	Application; Middleware; Backend systems
Interception	Middleware

Denial of service	Application; Middleware; Backend systems
SQL injection	Middleware; Backend systems

Table 7.1: Threat modelling of mobile application architecture

7.4.2. Sub-objective 2: Explore and analyse the advantages and limitations of existing fraud management approaches with regard to mobile applications

The second objective of the study was explored in Chapter 3. The chapter studied existing frameworks and approaches of fraud management for mobile applications. Although these methodologies approach the subject of fraud differently, their ultimate goal is to prevent and detect fraudulent activity and, as a result, reduce risk to an acceptable level as well as protect an organisation from reputational and financial damage. Table 7.2 summarises these approaches as well as the advantages and limitations thereof, as discussed in detail in Chapter 3.

Fraud Management Approach	Advantages	Limitations	Mobile Application Layer
User profiling	• Compare observed usage to profiled usage • Reduced learning curve • Adapt to users' current context in real time • Focus on a single target rather than fragmented attention	• Generates a high rate of false alarms • Data can be incomplete, inconsistent, or even deliberately misleading • Often leads the investigator to concentrate on differences and thus ignore absolute levels of response • No room for discovery for the anomalies or differences that may lie between the groups	• Presentation • Application • Backend system
Rule-based approach	• Flexibility of rules which can easily be applied to existing knowledge base • Inductive logic in neural networks • Rule-based approaches are robust • No prior knowledge of fraud • Information sharing across entities	• Rule-based schemes are slow • Rules deteriorate over time as the behaviour patterns impact the business change • Existing rules fail to uncover new kinds of attacks • Complex rule definition which requires only expert knowledge • Difficulty detecting a fraudster's transaction behaviours during his non-criminal period • Inability to process large amounts of data • Bad data quality	• Presentation • Application • Middleware • Backend systems
Case-based reasoning	• Ability to use information about instances in the past to predict fraudulent behaviour in future • Ability to reason in a wider variety of scenarios through learning of new cases • Can handle unexpected cases that do not previously exist in the body of knowledge	• Gives room to many false positives, as the most similar past case becomes the solution to a new problem • Takes a long time to find and process actions of similar previously identified cases • Long time to find and process action of similar previously identified cases	• Presentation • Application • Middleware • Backend systems

Table 7.2: Summary of fraud management approaches

7.4.3. Sub-objective 3: Explore and analyse the advantages and limitations of existing digital forensic approaches concerning mobile applications

The second objective of the study was to investigate existing digital forensic approaches and the benefits and limitations thereof. Chapter 4 was aimed at unpacking the current literature and research focused on digital forensics, more so in the field of mobile applications. The various approaches studied have a common theme aimed at recreating a sequence of events arising from, for example, the unauthorised intrusion by an external party into, or unusual activities by an authorised user of, digital systems. Table 7.3 gives a summary of these approaches as well as the advantages and limitations thereof, which were discussed in detail in Chapter 4.

Digital Forensic Approach	Advantages	Limitations	Mobile Application Layer
Physical digital forensic process models	- Basic and concise methodology - Computer forensics process is free from specific technologies - Generalised process that will be applicable to most electronic devices - Event reconstruction allows for quicker forensic examinations - Gives accurate results from the investigation process - Applied to a range of digital devices including unrealised digital devices of the future	- Potential for error in data representation - Phases are sequentially ordered and, therefore, do not make way for iteration - Not appropriate to perform digital investigation thoroughly - Irrelevant and unnecessary data may be collected - Deployment phase independent of the physical and digital investigation phase - Rigid and linear - The definition of these classes is not standardised	- Presentation - Application - Middleware - Backend systems
Staircase-based digital forensic process models	- Reconstruction can point to additional evidence - Investigations are conducted at the primary crime scene - Consistent and structured framework - Standardisation and consistency of terminology - Output of each phase serves as input to succeeding phases	- Repetition of steps in the process models - Ambiguous definition of analysis phase - Activities may be assumed by another activity - Excludes crucial steps that are present in other models - Too generic	- Presentation - Application - Middleware - Backend systems
Phased digital forensic process models	- Not dependent on a particular technology or electronic crime - Granularity of the phases shows the focus on verifying an attack - Consistent and structured multi-tiered framework - Allows for greater consistency and standardisation - Ranks potential information according to the importance to the criminal investigation	- Attempts to combine steps that are generally separated in other process models - Combination of data analysis and examination may result in confusion - Scenario-specific - Some phases are to an extent duplications of another	- Presentation - Application - Middleware - Backend systems

Table 7.3: Summary of digital forensic approaches

7.4.4. Sub-objective 4: Conceptualise a preliminary fraud management and digital forensic framework for mobile applications

Over the years, there has been an increased amount of published literature on how organisations can become better in detecting, managing and preventing fraud. The literature review of this study demonstrated that existing fraud management and digital forensic models and approaches worked well; however, they did so in isolation. As discussed in Chapter 3, for example, existing fraud management models may focus on detection and not put emphasis on other aspects such as deterrence and disruption. Similarly, existing digital forensic approaches were found to be focusing on the processing of digital evidence, but they are not general enough to describe the investigative process.

Given that these models and approaches exist already, the motivation for presenting another approach was based on the benefits that could be gained through leveraging off the strengths of the existing components of these approaches. Sub-objective 3 is therefore satisfied through the proposal of a unified FMDF approach which brings together best practices of the fraud management and digital forensic approaches to present them as one. The entire fraud management and forensic investigation process can be conceptualised as occurring iteratively with explicit interaction within various phases. Unlike a traditional linear lifecycle, the stages in the FMDF approach are not all necessarily sequential; instead, the FMDF approach facilitates simultaneous as well as sequential actions within the various stages of the activities.

7.5. FUTURE WORK

To generate a trusted, unified approach with reference to diversification, there is a need for more case studies to allow further assessment of the dimensions and expansion of the subject. Exploring the following as future research can facilitate the attainment of this goal:

- The study can be expanded beyond the South African environment. This could be useful for South African organisations that have a presence in other countries.

- The approach can also focus on industries other than the financial services industry, which was the primary focus of this study. Future research may want to apply this approach to other forms of mobile applications and test its applicability with subject matter experts in those fields.

- Fraud management and digital forensics by its very nature is not limited to just mobile applications. New research could investigate the use of the approach for next-generation communication platforms.

- Having suggested a framework in this study, a plausible and very important study should be that of modelling the framework and designing a dedicated system architecture that would be able to operationalise the framework in a real-life setting.

- Following the above architectural design, a prototype implementation could be developed so as to demonstrate its applicability at organisational level. Such a prototype can be rolled out at organisational level in an incremental fashion.

7.6. CONCLUSION

This section reflects on what transpired throughout this research study. Chapter 1 outlined the quantitative survey research methodology implemented in this research. A self-administered online questionnaire was the main quantitative data collection technique aided by various analyses of quantitative techniques. Chapter 2 identified the various threats associated with mobile applications from a fraud point of view and expressed the need for an approach to mitigate these. The study then explored and assessed existing fraud management and digital forensic models and approaches and explored their benefits as well as limitations. This formed the basis of Chapters 3 and 4 respectively. In Chapter 5, the researcher discussed optimal fraud management and digital forensic approaches respectively and proposed a unified approach that would provide a more suitable solution to mobile application fraud. The unified FMDF approach was discussed in detail in Chapter 5 and tested in Chapter 6 through a survey with subject matter experts. Data was collected, presented, analysed and interpreted in Chapter 6. The findings of the study were stated and discussed based on respective objectives in Chapter 7 as research overview.

The following conclusions were made from this study:

- Organisations that use mobile applications, such as banks, have critical assets that need to be secured.
- Generally, fraud management and digital forensics were seen as two separate entities that function exclusively and independent of each other.
- Professionals in the fraud management and digital forensic environments are committed to combating fraud but lacked the proper tools to achieve this.
- The banking environment should continuously review and improve their overall fraud management approaches.
- The proposal of the unified FMDF framework was considered to be helpful and valuable by professionals who participated in this research.

These conclusions formed the basis on which recommendations were made to improve the overall fraud management and digital forensic approach for mobile applications. This study has clearly highlighted how critical it is to make advancement towards a unified fraud management and digital forensic framework for mobile applications during this technologically advanced era.

8. LIST OF REFERENCES

LIST OF REFERENCES

Aamodt, A. & Plaza, E., 1994. Case-Based Reasoning: Foundational Issues, Metholodical Variations, and System Approaches. *AI Communications,* 7(1), pp. 39-59.

Ademu, I. O., Imafidon, D. C. O. & Preston, D. D. S., 2011. A New Approach of Digital Forensic Model for Digital Forensic Investigation. *International Journal of Advanced Computer Science and Applications, ,* 2(12), pp. 175-178.

Aghghaleh, S. F. I. M. T. & Mohamed, Z. M., 2014. Fraud Risk Factors of Fraud Triangle and the Likelihood of Fraud Occurrence: Evidence from Malaysia. *Information Management and Business Review,* 6(1), pp. 1-7.

Agrawal, A., Gupta, M., Gupta, S. & Gupta, C., 2011. A systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS),* 5(1), pp. 118 -131.

Agrawal, R. & Srikant, R., 1994. *Fast algorithms for mining association rules.* Santiago, VLDB.

Al-Zarouni, M., 2006. *Mobile Handset Forensic Evidence: a challenge for Law Enforcement,* s.l.: s.n.

American Institute of Certified Public Accountants (AICPA), 1997. *Consideration of Fraud in a Financial Statement Audit,* New York: AICPA.

Anderson, E. & Choobineh, J., 2008. Enterprise information security strategies. *Computers & Security,* 27(1-2), pp. 22-29.

Andrew, M., 2007. *Defining a process model for forensic analysis of digital devices and storage media.* s.l., IEEE.

Baryamureeba, V. & Tushabe, F., 2007. *The enhanced digital investigation process model,* Kampala: s.n.

Beebe, N. L. & Clark, J. G., 2005. *A Hierarchical, Objectives-Based Framework for the Digital Investigations Process.* Baltimore, Beebe & Clark, pp. 1-17.

Bettini, A. & Price, M., 2011. *Downloading from Mobile App Stores Is a Risky Business,* California: McAfee.

Bihina Bella, M., Eloff, J. & Olivier, M., 2009. A fraud management system architecture for next-generation networks. *Forensic Science International,* 185(1-3), pp. 51-58.

Bishop, T. J. et al., 2010. *Managing the Business Risk of Fraud: A practical guide,* s.l.: The Institute of Internal Auditors.

Boehmer, W., 2010. *Analyzing Human Behavior using Case-Based Reasoning with the help of Forensic Questions.* Germany, IEEE.

Bradford, P. G. & Ray, D. A., 2007. *Models of Models: Digital Forensics and Domain-Specific Languages.* Alabama: s.n.

Brewer, N., Liu, N., de Vel, O. & Caelli, T., 2006. *Using Coupled Hidden Markov Models to Model Suspect Interactions in Digital Forensic Analysis.* Austrailia, IEEE.

Burge, P. & Shawe-Tyalor, J., 2001. An unsupervised neural network approach to profiling the behaviour of mobile phone users to use in fraud detection. *Journal of Parallel and Distributed Computing,* 61(1), pp. 915-925.

Carrier, B. & Spafford, E., 2003. Getting physical with digital investigation process. *International journal of digital evidence,* 2(2), pp. 1-20.

Carrier, B. & Spafford, E., 2004. *An Event-Based Digital Forensic Investigation Framework.* Baltimore, MD, pp. 1-12.

Casey, E. & Palmer, G., 2004. *The Investigative Process: Digital Evidence and computer crime.* Amsterdam: Elsiever academic press.

Casey, E. & Schatz, B., 2011. Digital Investigations: Conducting Digital Investigations. In: *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* s.l.:Academic Press, pp. 190-225.

Cavazza, F., 2011. *Forbes.* [Online]
Available at: http://www.forbes.com/sites/fredcavazza/2011/09/27/mobile-web-app-vs-native-app-its-complicated/
[Accessed 21 June 2014].

Chang, J.-S. & Chang, W.-H., 2009. *An Early Fraud Detection Mechanism for Online Auctions Based on Phased Modelling,* TamKang: IEEE.

Chartered Institute of Management Accountants, 2008. *Fraud risk management: A guide to good practice,* United Kingdom: Chartered Institute of Management Accountants.

Chaudhary, K., Yadav, J. & Mallick, B., 2012. A review of Fraud Detection Techniques: Credit Card. *International Journal of Computer Applications,* 45(1), pp. 39-44.

Ciardhuáin, S., 2004. An extended model of cybercrime investigations. *International journal of digital evidence,* 3(1), pp. 1-22.

Compaq, 2001. [Online] Available at: http://h18000.www1.hp.com/info/SP6140/SP6140PF.PDF [Accessed 22 12 2014].

Cressey, D. R., 1953. *Other People's Money: A Study in the Social Psychology of Embezzlement.* Montclair: Free Press.

Creswell, J. W., 2002. *Research Design: Qualitiative, quantitative and mixed methods approaches.* 2nd ed. Lincoln: SAGE Publications.

Curet, O., Jackson, M. & Tarar, A., 1996. *Designing and evaluating a case-based learning and reasoning agent in unstructured decision making.* San Diego, IEEE, pp. 2487-2492.

Dai, F. G., Ai, F. S. & Lei, S., 2011. *Billing attack detection and prevention in mobile communication netowrk,* Nanjing: IEEE.

Degu, G. & Yigzaw, T., 2006. *Research Methodology.* Ethiopia: USAID.

DeWin, B. et al., 2009. Security Middleware for Mobile Applications. In: B. Garbiato, H. Miranda & L. Rodrigues, eds. *Middleware for Network Eccentric and Mobile applications.* Belgium: Springer, pp. 265-284.

Dey, A., 2001. Understanding and using context. *Pers Ubiquitous,* 5(1), pp. 4-7.

DFRWS, 2001. *A Roadmap for Digital Forensic Research,* New York: DFRWS.

DFRWS, 2001. *DFRWS (Digital Forensic Research Conference.* [Online] Available at: www.dfrws.org [Accessed 22 09 2014].

Drake, S. D., 2008. *Embracing Next-Generation Mobile Platforms to Solve Business Problems,* Framingham: IDC.

Edge, M. E., Sampaio, P. R. F. & Choudhary, M., 2007. *Towards a Proactive Fraud Management Framework for Financial Data Streams.* Manchester, IEEE.

Eschelbeck, Gerhard, 2014. *Security Threat Report 2014,* Oxford: Sophos.

Furlan, S. & Bajec, M., 2008. Holistic approach to fraud management in health insurance. *Journal of Information and Organisational Sciences,* 32(2), pp. 99-114.

Gadhiya, S. & Wandra K.H, V. V., 2009. *Role of Mobile Augmentation in Mobile Application Development,* Gujarat: s.n.

Galliers, R., 1991. Choosing appropriate information systems research approaches: a revised taxonomy. In: *Information Systems Research: Issues, Methods and Practical Guidelines..* Oxford: Blackwell , pp. 144-162.

Gao, L., Mock, T. J. & Srivastava, R. P., 2011. *An Evidential Reasoning Approach to Fraud Risk Assessment under Dempster-Shafer Theory: A General Framework.* Hawaii, IEEE, pp. 1-10.

Garnham, B., 2008. Data Generation. In: L. M. Given, ed. *The Sage Encyclopedia of Qualitative Research Methods .* Alberta: SAGE.

Gartner, 2013. *Gartner Says Smartphone Sales Accounted for 55 Percent of Overall Mobile Phone Sales in Third Quarter of 2013,* Barcelona: Gartner.

Gong, R. & Chan Kai Yun, T., 2005. Case-Relevance Information Investigation: Binding Computer Intelligence to the current Computer Forensic Framework. *International Journal of Digital Evidence,* 4(1), pp. 1-13.

Grabec, I., 1989. *Self-organization of neurons described by the second maximum entropy principle.* London, IEEE .

Granlund, D., Johansson, D., Andersson, K. & Brännström, R., 2013. *A Case Study of Application Development for Mobile and Location-Based Services,* Austria.: ACM.

Guo, D. F., Fen Sui, A. & Shi, L., 2011. *Billing Attack Detection and Prevention in Mobile Communication Network,* Nanjing: IEEE.

Hall, J., Barbeau, M. & Kranakis, E., 2005. Anomaly-based Intrusion Detection Using Mobility Profiles of Public Transportation Users. *IEEE,* pp. 17-23.

Hasan, O. et al., 2013. *A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case.* Santa Clara Marriott, IEEE 2nd International Congress on Big Data.

Hewlett-Packard Company, 2005. [Online]
Available at: http://h71028.www7.hp.com/enterprise/downloads/featurelist093.pdf
[Accessed 22 10 2014].

Hilas, C. S. & Sahalos, J. N., 2005. *User Profiling for Fraud Detection in Telecommunication Networks.* Thessaloniki, IEEE.

Humaid, E. H. & Barhoum, T., 2013. *Water Consumption Financial Fraud Detection: a model based on rule induction.* Gaza, IEEE.

IBM, 2012. *Native, web or hybrid mobile-app development,* New York City: IBM Software.

ISACA, 2010. *ISACA.* [Online]
Available at: www.isaca.org
[Accessed 01 02 2010].

Jafari, F. & Satti, R. S., 2015. Comparitive analysis of digital forensic models. *Journal of advances in computer networks,* 3(1), pp. 82 - 86.

Jansen, W. & Ayers, R., 2007. *Guide on Cell Phone Forensics,* s.l.: National Insitute of Standards and Technology (NIST).

Jonkers, 2010. The forensic use of mobile phone flasher boxes. *Digital Investigation,* 6(3-4), pp. 168-178.

Jung Kim, P. & Ju Noh, Y., 2003. *Mobile Agent System Architecture for supporting Mobile Market Application Service in Mobile Computing Environment.* Korea, IEEE Computer Society.

Kesäniemi, A., 2012. *Mobile Application threat analysis,* Nixu: The OWASP Foundation.

Khalaf, S., 2014. *Flurry Analytics.* [Online]
Available at: http://www.flurry.com/bid/109749/Apps-Solidify-Leadership-Six-Years-into-the-Mobile-Revolution
[Accessed 10 April 2014].

Kim, H.-K. & Gelog, Y. E., 2013. Convergence Mobile Application Architecture on Requirement View. *International Journal of Multimedia and Ubiquitous Engineering,* 8(3), pp. 151-166.

Kirkos, E., Spathis, C. & Manolopoulos, Y., 2007. Data Mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications,* 32(1), p. 995–1003.

Kirubakaran, b. & Karthikeyani, D. V., 2013. *Mobile Application Testing – Challenges and Solution Approach through automation.* Tamil Nadu, IEEE, pp. 79-84.

Kolodner, J., 1993. An Introduction to Case-Based Reasoning. *Artificial Intelligence Review,* 6(1), pp. 3-34.

Kothari, C., 2004. *Research Methodology: Methods and Techniques.* Jaipur: New Age International.

Kount, 2015. *Mobile Payments and Fraud: 2015 Report,* Idaho: Kount.com.

KPMG Forensic, 2006. *Fraud Risk Management; Developing a strategy for prevention, detection and response,* s.l.: KPMG.

Krauss, S. E., 2005. Research Paradigms and Meaning Making: A Primer. *The Qualitative Report,* 10(1), pp. 758-770.

Krenker, A. et al., 2009. Bidirectional artificial neural netowrks for mobile-phone fraud detection. *ETRI Journal,* 31(2), pp. 92-94.

Lin, J. W. & Hwang, M. I., 2000. Assessing the risk of management fraud: A neural fuzzy system approach. *Issues in Information Systems,* 1(1), pp. 270-276.

Litan, A., 2011. *The five layers of fraud prevention and using them to beat malware,* Stamford: Gartner.

Liu, Q., Li, T. & XU, W., 2009. *A SUBJECTIVE AND OBJECTIVE INTEGRATED METHOD FOR FRAUD DETECTION IN FINANCIAL SYSTEMS.* Baoding, IEEE.

Lou, Y.-I., Wang & Ming-Long, 2009. Fraud Risk Factor Of The Fraud Triangle Assessing The Likelihood Of Fraudulent Financial Reporting. *Journal of Business and Economics Research,* 7(2), pp. 61 - 78.

Lynn, P., Erens, B. & Sturgis, P., 2012. *A Strategy for Survey Methods Research in the UK,* United Kingdom: ESRC.

Main, J., Dillon, T. & Shiu, S., 2001. A Tutorial on Case-Based Reasoning. In: S. K. Pal, T. Dillon & D. Yeung, eds. *Soft Computing in Case Based Reasoning.* London: Springer-Verlag, pp. 1-28.

Mata-Toledo, R. A., 2003. *Data mining process,* Harrisonburg: McGraw-Hill Education.

Meier, J. et al., 2008. *Mobile Application Architecture Guide,* s.l.: Microsoft Corporation.

Miles, M. B. & Huberman, M. A., 1994. *Qualitative Data Analysis: An Expanded Sourcebook.* 2nd ed. Beverley Hills: Sage.

Miller, D. & Creswell, J., 2000. Determining validity in qualitative inquiry. *Theory into practice,* 39(3), pp. 124-130.

Mouton, J., 2001. *How to suceed in your master's and doctoral studies.* 5th ed. Pretoria: Van Schaik.

Natchetoi, Y., Kaufman, Viktor & Shapiro, A., 2008. *Service-Oriented Architecture for Mobile Applications,* Montreal: ACM.

Njenga, K. & Ndlovu, S., 2012. On privacy calculus and underlying consumer concerns influencing mobile banking subscriptions. *Information Security for South Africa (ISSA),* pp. 1-9.

Noblett, M., Pollitt, M. & Presley, L., 2000. Recovering and Examining Computer Forensic Evidence. *Forensic Science Communications,* 2(4).

Nolan, R., O'Sullivan, C., Branson, J. & Waits, C., 2005. *First Responders Guide to Computer Forensics.* 1 ed. Pittsburgh: CERT Training and Education.

Oates, B. J., 2006. *Researchgin Information systesm and computing.* London: Sage Publications.

O'Brien, R., 1998. *An Overview of the methodological approach of action research,* Toronto: University of Toronto.

Onwuegbuzie, A. & Combs, J. P., 2011. Data Analysis in Mixed Research: A Primer. *International Journal of Education,* 3(1), pp. 1-25.

Pantic, M., 2008. *Introduction to Machine Learning & Case Based Reasoning.* s.l.:s.n.

Park, F. S., Gangakhedkar, C. & Traynor, P., 2009. *Leveraging Cellular Infrastructure to Improve Fraud Prevention.* Atlanta, IEEE.

Paspallis, N. & Papadopoulos, G., 2013. A pluggable middleware architecture for developing context-aware mobile applications. *Pers Ubiquit Comput,* 8 October, Volume 18, pp. 1099-1116.

Patidar, R. & Sharma, L., 2011. Credit card fraud detection using neural network. *International Journal of Soft Computing and Engineering,* 1(NCAI2011), pp. 2331-2307.

PhridviRaj, M. & GuruRao, C., 2014. *Data Mining – Past, Present and Future – A Typical Survey on Data Streams.* Romania, Procedia Technology, pp. 255-263.

Polgar, S. & Thomas, S., 2008. *Introduction to research in the health sciences.* 5th ed. Edinburgh: Churchhill Livingstone Elservier.

Pollit, M., 1995. *Computer Forensics: an Approach to Evidence in Cyberspace.* Baltimore, MD, pp. 487 - 491.

Prasad Kantamneni, R. & Narayanan, S., 2001. *Personalization of information retrieval through user profiling.* Dayton, IEEE, pp. 3475 - 3478.

Prentzas, J. & Hatzilygeroudis, I., 2007. Categorizing approaches combining rule-based and case-based reasoning. *Expert Systems,* 24(2), pp. 97-122.

Prosise, C. & Mandia, K., 2003. *Incident response and computer forensics.* New York: Osborne McGraw0Hill.

Radia, N., Zhang, Y., Tatipamula, M. & Madisetti, V. K., 2012. *Next-Generation Applications on Cellular Networks: Trends, Challenges, and Solutions.* s.l., IEEE, pp. 841-854.

Rajasekar, S., Philominathan, P. & Chinnathami, V., 2013. *Research methodology,* India: s.n.

Reith, M., Carr, C. & Gunsch, G., 2002. An Examination of Digital Forensic Models. *International journal of digital evidence,* 1(3), pp. 1-12.

Renu & Suman, 2014. Analysis on Credit Card Fraud Detection Methods. *International Journal of Computer Trends and Technology,* 8(1), pp. 45-51.

Richter, M. M., 1995. *The Knowledge Contrined in Similarity Measures.* Portugal, Springer.

Ruggiero, P. & Foote, J., 2011. *Cyber Threats to Mobile Phones,* s.l.: US-Cert.

Sage, 2011. Survey Research. In: *Research Design and Data Collection.* s.l.:SAGE, pp. 159-185.

Sangwhan, C., Kurz, J. B. & Weichang, D., 2009. *Toward a unified framework for mobile applications.* New Brunswick, IEEE.

Schiaffino, S. & Amandi, A., 2009. Intelligent User Profiling. *M. Bramer (Ed.): Artificial Intelligence,* pp. 193-216.

Seifert, J., 2004. *Data Mining, an overview,* s.l.: Congressional Research Service.

Song, d. & Song, x., 2011. *An audit decision aid system for management fraud risk assessment using AHP-CBR.* Wuhan, IEEE, pp. 1-4.

State audit institution, 2011. *Fraud control frameworks,* Abu Dhabi: State audit institution.

Stephenson, P., 2003a. *The DFRWS Framework Classes.* s.l.:CRC Press.

Stephenson, P., 2003b. *A Comprehensive Approach to Digital Incident Investigation,* s.l.: Elsevier Advanced Technology.

Stephenson, P., 2003c. Modeling of Post-Incident Root Cause Analysis. *International Journal of Digital Evidence,* 2(2), pp. 1-16.

Stewart, S. & Davies, J., 1997. *User profiling techniques: a critical review.* Swinton, British Computer Society.

Sun, Z. & Finnie, G., 2004. *Experience Based Reasoning for Recognising Fraud and Deception.* Wollongong, IEEE.

Tashakkori, A. & Teddlie, C., 2003. *Handbook of Mixed Methods in Social & Behaviou Research.* Thousand Oaks: SAGE Publications.

Tashakkori, A. & Teddlie, C., 2009. *Foundations of mixed methods research.* Thousand Oks: SAGE Publications.

Teng, C.-C. & Helps, R., 2010. *Mobile Application Development: Essential New Directions for IT.* s.l., IEEE, pp. 471-475.

The Open Group, 1995. *Information Layer.* [Online] Available at: https://www.opengroup.org/soa/source-book/soa_refarch/information.htm [Accessed 9 June 2015].

Thing, V. L., Ng, K.-Y. & Chang, E.-C., 2010. Live memory forensics on mobile phones. *Digital Investigation,* 7(1), pp. 74 - 82.

Turner, J. L., Mock, T. J., Srivastava & P, R., 2003. *An Analysis of the Fraud Triangle.* [Online]
Available at:
http://www2.aaahq.org/audit/midyear/03midyear/papers/Research%20Roundtable%203-Turner-Mock-Srivastava.pdf
[Accessed 22 June 2015].

Unhelkar, B. & Murugesan, S., 2010. *The Enterprise Mobile applications development framework,* Sydney: IEEE computer society.

US Department of Justice, 2001. *Electronic Crime Scene Investigation: A guide to first responders,* Washington DC: National Institute of Justice.

Vacca, J. R., 2002. *Computer Forensics: Computer Crime Scene Investigation, Volume 1.* Illustrated ed. Ohio: Charles River Media.

Vaughan, R., 2008. *Conceptual Framework.* s.l.:Bournemouth University.

Verhaeghe, P. et al., 2010. *Security and Privacy Threats of the Belgian Electronic Identity Card and Middleware,* Heverlee: s.n.

Verrelst, H. et al., 2000. *A rule based and neural network system for fraud detection in mobile communications,* London: Europa CORDIS.

Watson, I. & Marir, F., 1994. Case-based reasoning: A review. *The knowledge engineering review,* 9(4), pp. 327-354.

Wesley, K. W., 2004. The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management.. *Journal of Economic Crime Management,* 2(2), pp. 1-38.

Wheeler, R. & Aitken, S., 2000. Multiple algorithms for fraud detection. *Knowledge-based systems,* 13(2), pp. 93-99.

Wilhelm, W. K., 2004. The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management.. *Journal of Economic Crime Management,* 2(2), pp. 1-38.

Yang, D. Y., Lewis, D. E. & Newmarch, D. J., 2010. *Profile-based digital identity management - a better way to combat fraud.* Melbourne, IEEE, pp. 260 -267.

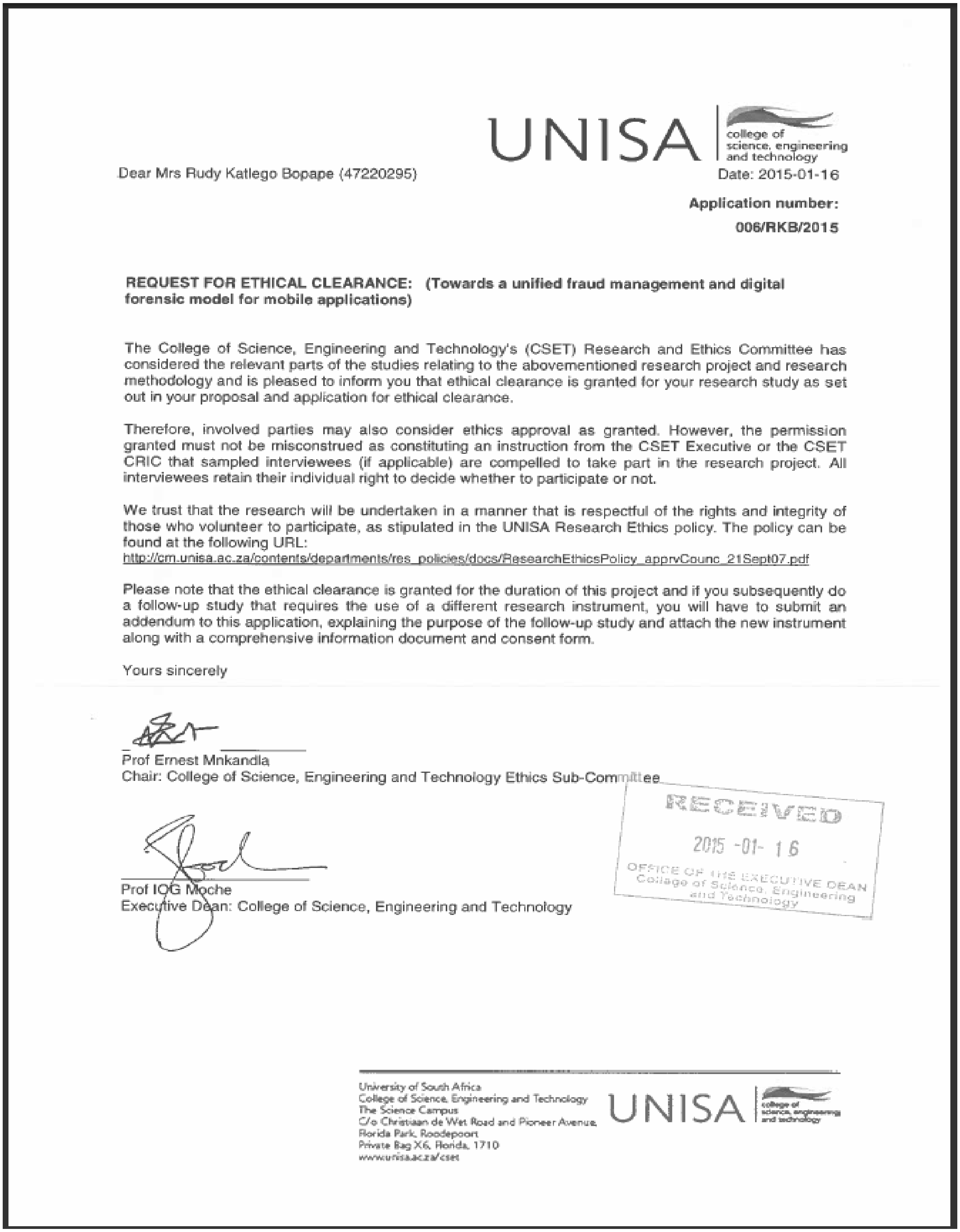
Yount, R., 2006. Survey Research. In: *Research Design and Statistical Analysis in Christian Ministry.* 4th ed. s.l.:NAPCE, pp. 1-16.

Yue, D., Wu, X., Wang, Y. & Li, Y., 2007. *A review of data mining-based financial fraud detection research.* Shanghai, IEEE.

Yusoff, Y., Ismail, R. & Hassan, Z., 2011. Common Phases of computer forensic investigaton models. *International Journal of Computer Science & Information Technology (IJCSIT),* 3(3), pp. 17-31.

APPENDICES

Appendix A: Ethical Clearance



UNISA | college of science, engineering and technology

Dear Mrs Rudy Katlego Bopape (47220295)

Date: 2015-01-16

Application number:
006/RKB/2015

REQUEST FOR ETHICAL CLEARANCE: (Towards a unified fraud management and digital forensic model for mobile applications)

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your research study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CRIC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:
http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

Please note that the ethical clearance is granted for the duration of this project and if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

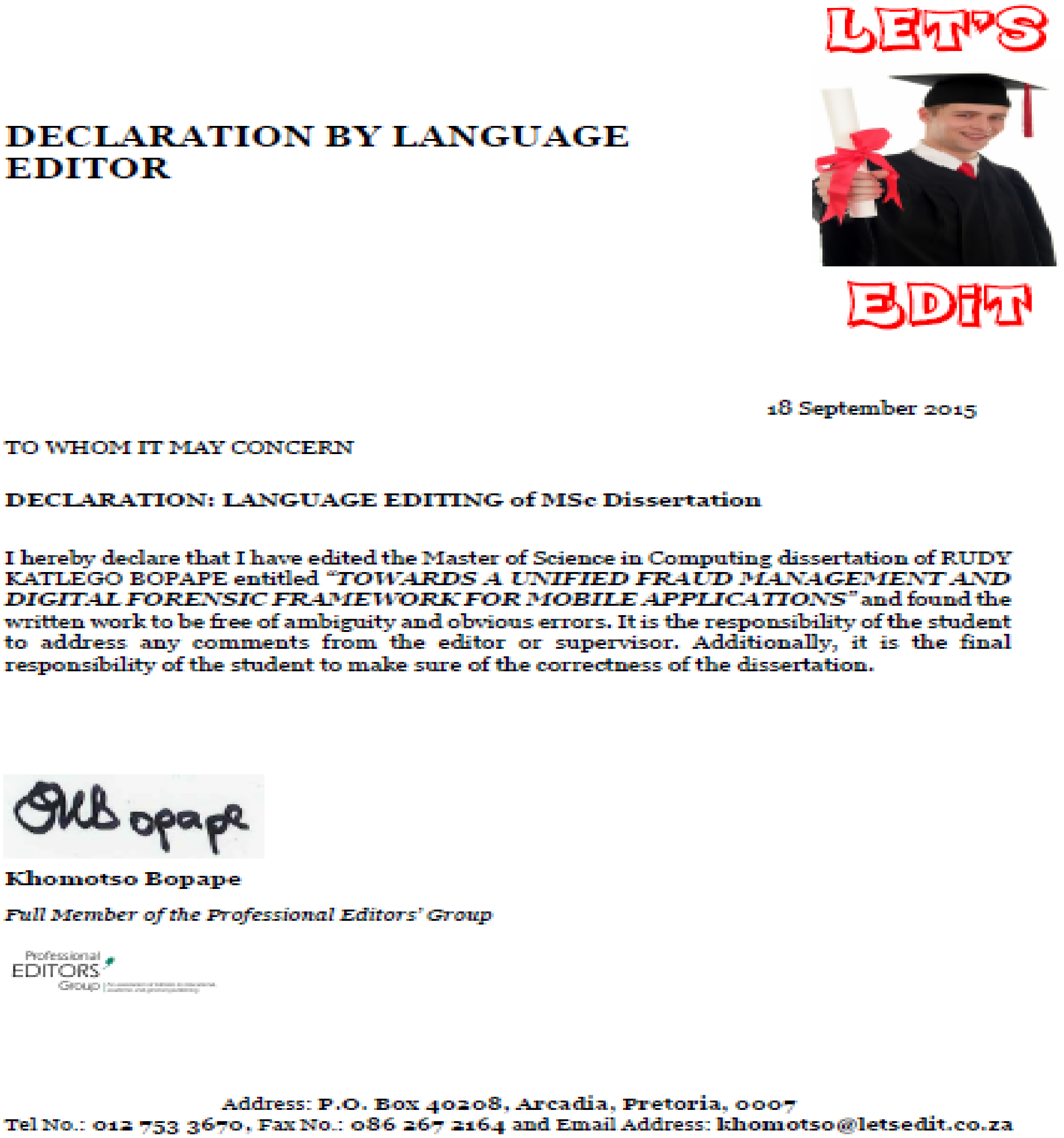
Prof Ernest Mnkandla
Chair: College of Science, Engineering and Technology Ethics Sub-Committee

Prof IOG Moche
Executive Dean: College of Science, Engineering and Technology

University of South Africa
College of Science, Engineering and Technology
The Science Campus
C/o Christiaan de Wet Road and Pioneer Avenue,
Florida Park, Roodepoort
Private Bag X6, Florida, 1710
www.unisa.ac.za/cset

UNISA | college of science, engineering and technology

Appendix B: Editor Certificate



LET'S EDIT

DECLARATION BY LANGUAGE EDITOR

18 September 2015

TO WHOM IT MAY CONCERN

DECLARATION: LANGUAGE EDITING of MSc Dissertation

I hereby declare that I have edited the Master of Science in Computing dissertation of RUDY KATLEGO BOPAPE entitled *"TOWARDS A UNIFIED FRAUD MANAGEMENT AND DIGITAL FORENSIC FRAMEWORK FOR MOBILE APPLICATIONS"* and found the written work to be free of ambiguity and obvious errors. It is the responsibility of the student to address any comments from the editor or supervisor. Additionally, it is the final responsibility of the student to make sure of the correctness of the dissertation.

opape

Khomotso Bopape

Full Member of the Professional Editors' Group

Professional EDITORS Group

Address: P.O. Box 40208, Arcadia, Pretoria, 0007
Tel No.: 012 753 3670, Fax No.: 086 267 2164 and Email Address: khomotso@letsedit.co.za

Appendix C: Questionnaire

Dissertation Title: Towards a unified fraud management and digital forensic framework for mobile applications
Primary Investigator: Rudy Bopape (MSc student)
Supervisor: Prof. Ernest Ketcha Ngassam

Dear research participant
You are invited to participate in a research study that forms part of my formal MSc degree. This information leaflet will help you to decide if you would like to participate. Before you agree to take part, you should fully understand what is involved.

In recent years, mobile technologies have become pervasive, seeping into every aspect of our personal and professional lives. Enterprises are now adopting these technologies for numerous applications to capitalise on the mobile revolution. This means that they are now able to increase their operational efficiency as well as responsiveness and competitiveness, and most importantly, meet new growing customer demands. For example, businesses are able to offer banking and travel services that are unique to the user's requirements. These applications, which were considered a mere trend a few years ago, are now dominating the mobile industry, which was inherently conceived for mere communication.

Although mobile technologies and applications present many new opportunities, they also present challenges. Fraudsters are able to use these devices to access enterprise applications and subsequently perform fraudulent transactions. When this occurs, it is important to examine and manage the cause and findings, as well as to prevent any future similar attacks through continued learning.

The intention of this questionnaire is to assess if the proposed unified fraud management and digital forensic model would assist in managing IT security risk more proactively and more effectively in a dynamic environment.

This Questionnaire is divided into the following segments:

Section 1: General information and professional experience
Section 2: Understanding of mobile application landscape
Section 3: Approach to fraud management for mobile applications
Section 4: Approach to digital forensics for mobile applications
Section 5: Critical success factors of the unified approach

Section 1: General information and professional experience

1. What typical activities do your organisation's clients use mobile applications for? Please tick all that apply.	
a) Banking	b) Communications
c) Documents repository	d) Other

2. If you chose "Other", please elaborate.

3. Does your day-to-day responsibility include the prevention, detection or investigation of fraud in one way or another?	
a) Yes	b) No

4. Which area of fraud management are you responsible for?	
a) Prevention	b) Detection
c) Investigations	d) All of the above

5. What is your role(s) in the organisation, whether as staff or consultant? Please check all that apply.

a) Digital forensic specialist	b) Fraud incident responder	c) Fraud prevention specialist
d) Investigator	e) Security analyst/manager	f) Other

6. Years of Experience within fraud management or digital forensics?		
a) 0-5 Years	b) 6-10 Years	c) 10 Years+

Section 2: Understanding of mobile application landscape

1. What are the typical components/layers that a mobile application consists of? Please check all that apply.	
a) Frontend application later	b) Middleware layer
c) Backend system layer	d) Other

2. If you chose “Other”, please elaborate.

3. Please rank the following threats to mobile applications from 1 to 5. Five (5) being most important, and one (1) being least important.	
a) Insecure or unnecessary client-side data storage	b) Lack of data protection in transit
c) Personal data leakage	d) Client-side intrusion
e) Malicious third-party code	

Section 3: Approach to fraud management

1. What is your biggest challenge when it comes to fraud management? Please check all that apply.

a) Timely detection of fraud	b) Speed of incident resolution
c) Raising alerts to aid in prevention	d) False positives
e) Other	

2. If you chose “Other”, please elaborate.

3. In managing mobile application fraud, do you use a specific approach?	
a) Yes	b) No

4. Which of the following fraud management approaches are you familiar with? Please check all that apply.	
a) User profiling	b) Rule-based reasoning
c) Case-based	d) Other

5. If you chose “Other”, please elaborate.

6. In which layer of the mobile architecture explained in section 2 of the questionnaire does your fraud management approach mainly satisfy? Please check all that apply.	
a) Frontend application layer	b) Middleware layer
c) Backend system layer	

7. How would you rate the overall effectiveness of your approach?	
a) Very effective	b) Reasonably effective
c) Somewhat effective	d) Not effective

Section 4: Approach to digital forensics

1. For what purpose does your organisation conduct forensic investigations? Please check all that apply.	
a) To investigate incidents after they have been reported	b) To track and remediate threats to your organisation
c) To investigate incidents as they are occurring	d) Other

2. What is your biggest challenge when it comes to forensics? Please check all that apply.	
a) Real-time investigations	b) Turnaround times
c) Incident response	d) Link between cases
e) Other	

3. If you chose “Other”, please elaborate.

4. In conducting forensic investigations, do you use a specific approach?	
a) Yes	b) No

5. Which of the following forensic approaches are you familiar with? Please check all that apply.	
a) Event reconstruction	b) Case-based
c) Other	

6. If you chose “Other”, please elaborate.

7. In which layer of the mobile architecture explained in section 2 of the questionnaire does your forensic approach mainly satisfy? Please check all that apply.	
a) Frontend application layer	b) Middleware layer
c) Backend layer	

8. How would you rate the overall effectiveness of your approach?	
a) Very effective	b) Reasonably effective
c) Somewhat effective	d) Not effective

Section 5: Critical success factors of a unified approach

1. An effective business-driven fraud management approach encompasses controls that have three objectives: prevent, detect and respond.				
a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

2. Ideally, an organisation should be able to prevent fraud before it occurs.				
a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

3. It is important for an organisation to be able to detect fraud timeously and remediate it as quickly as possible.

a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

4. A formal detection and prevention approach is important in developing an effective fraud management approach.

a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

5. It is important to consider previous incidents in the detection process so as to learn from previous cases.

a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

6. It is important to profile customer behaviour in order to assist in detecting anomalies related to fraudulent behaviour.

a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

7. It is important to reduce the opportunities for committing fraud and limit the ability for potential fraudsters to penetrate.

a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

8. A fraud response strategy is an essential means of setting down clearly the arrangements in place for dealing with detected or suspected fraud cases.

a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

9. Forensic readiness and awareness should be created by internal events such as the intrusion detection alerts to allow the investigation to happen almost immediately.				
a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

10. A post-incident analysis of the event can enhance the already existing body of knowledge about fraudulent cases.				
a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

11. There is value in aligning the essential components of a fraud detection and forensic investigation through the intelligent use of both approaches.				
a) Strongly agree	b) Agree	c) Neither agree nor disagree	d) Disagree	e) Strongly disagree

Appendix C: Survey Results

Question 1

Does your day-to-day responsibility include the prevention, detection or investigation of fraud in one way or another?		
Answer Options	**Response Per cent**	**Response Count**
Yes	90.0%	36
No	10.0%	4
answered question		**40**
skipped question		**0**

Question 2

Years of Experience within fraud management or digital forensics?		
Answer Options	**Response Per cent**	**Response Count**
0-5 Years	58.3%	21
6-10 Years	27.8%	10
10 Years+	13.9%	5
answered question		**36**
skipped question		**4**

Question 3

Which area of fraud management are you responsible for?		
Answer Options	**Response Per cent**	**Response Count**
Prevention	22.2%	8
Detection	16.7%	6
Investigations	30.6%	11
All of the above	30.6%	11
answered question		**36**
skipped question		**4**

Question 4

What is your role(s) in the organisation, whether as staff or consultant? (Check all that apply)		
Answer Options	**Response Per cent**	**Response Count**
Digital forensic specialist	19.4%	7
Fraud incident responder	19.4%	7
Fraud prevention specialist	19.4%	7
Investigator	58.3%	21
Other (please specify)	19.4%	7
answered question		**36**
skipped question		**4**

Question 5

What are the typical components/layers that a mobile application consists of? (Check all that apply)		
Answer Options	**Response Per cent**	**Response Count**
Frontend application later	29.4%	10
Middleware layer	14.7%	5
Backend system layer	11.8%	4
All of the above	64.7%	22
Other (please specify)		0
answered question		36
skipped question		4

Question 6

Please rank the following threats to mobile applications from 1 to 5. Five (5) being most important, and one (1) being least important.							
Answer Options	**1**	**2**	**3**	**4**	**5**	**Rating Average**	**Response Count**
Insecure or unnecessary client-side data storage	10	5	7	5	7	2.82	34
Lack of data protection in transit	10	12	2	7	4	2.51	35
Personal data leakage	9	5	11	2	7	2.79	34
Client-side intrusion	1	6	6	16	5	3.53	34

Please rank the following threats to mobile applications from 1 to 5. Five (5) being most important, and one (1) being least important.							
Answer Options	**1**	**2**	**3**	**4**	**5**	**Rating Average**	**Response Count**
Malicious third-party code	5	6	8	4	11	3.29	34
answered question							**35**
skipped question							**5**

Question 7

What is your biggest challenge when it comes to fraud management? (Check all that apply)		
Answer Options	**Response Per cent**	**Response Count**
Timely detection of fraud	65.6%	21
Speed of incident resolution	53.1%	17
Raising alerts to aid in prevention	53.1%	17
False positives	15.6%	5
Other (please specify)	6.3%	2
answered question		**32**
skipped question		**8**

Question 8

In managing fraud, do you use a specific approach?		
Answer Options	**Response Per cent**	**Response Count**
Yes	84.8%	28
No	15.2%	5
answered question		**33**
skipped question		**7**

Question 9

How would you rate the overall effectiveness of your fraud management approach?		
Answer Options	**Response Per cent**	**Response Count**
Very effective	21.9%	7
Reasonably effective	50.0%	16
Somewhat effective	25.0%	8
Not effective	3.1%	1
answered question		**32**
skipped question		**8**

Question 10

Which of the following fraud management approaches are you familiar with? (Check all that apply)		
Answer Options	**Response Per cent**	**Response Count**
User profiling	54.8%	17
Rule-based reasoning	48.4%	15
Case-based	48.4%	15
Other (please specify)	0.0%	0
answered question		**31**
skipped question		**9**

Question 11

For what purpose does your organisation conduct forensic investigations? (Check all that apply)		
Answer Options	**Response Per cent**	**Response Count**
To investigate incidents after they have been reported	73.3%	22
To track and remediate possible threats to your organisation	53.3%	16
To investigate incidents as they are occurring	40.0%	12
Other (please specify)		0
answered question		30

skipped question	10

Question 12

What is your biggest challenge when it comes to forensic investigations? Please check all that apply (Check all that apply)		
Answer Options	**Response Per cent**	**Response Count**
Real-time investigations	70.0%	21
Turnaround times	56.7%	17
Link between cases	50.0%	15
Other (please specify)		0
answered question		30
skipped question		10

Question 13

In conducting forensic investigations, do you use a specific approach?		
Answer Options	**Response Per cent**	**Response Count**
Yes	83.3%	25
No	16.7%	5
answered question		**30**
skipped question		**10**

Question 14

How would you rate the overall effectiveness of your forensic approach?		
Answer Options	**Response Per cent**	**Response Count**
Very effective	23.3%	7
Reasonably effective	56.7%	17
Somewhat effective	13.3%	4
Not effective	6.7%	2
answered question		**30**
skipped question		**10**

Question 15

Please indicate your agreement or disagreement with the following statements about a unified fraud management and forensic approach.						
Answer Options	**Strongly agree**	**Agree**	**Neither agree nor disagree**	**Disagree**	**Strongly disagree**	**Response Count**
An effective business-driven fraud management approach encompasses controls that have three objectives: prevent, detect and respond.	26	4	0	0	1	31
Ideally, an organisation should be able to prevent fraud before it occurs.	26	4	0	0	1	31
It is important for an organisation to be able to detect fraud timeously and remediate it as quickly as possible.	26	4	0	0	1	31
A formal detection and prevention approach is important in developing an effective fraud management approach.	24	5	1	0	1	31
It is important to consider previous incidents in the detection process so as to learn from previous cases.	24	5	1	0	1	31

Please indicate your agreement or disagreement with the following statements about a unified fraud management and forensic approach.						
Answer Options	**Strongly agree**	**Agree**	**Neither agree nor disagree**	**Disagree**	**Strongly disagree**	**Response Count**
It is important to profile customer behaviour in order to assist in detecting anomalies related to fraudulent behaviour.	24	6	0	0	1	31
It is important to reduce the opportunities for committing fraud and limit the ability for potential fraudsters to penetrate.	26	4	0	0	1	31
A fraud response strategy is an essential means of setting down clearly the arrangements in place for dealing with detected or suspected fraud cases.	22	8	0	0	1	31
Forensic readiness and awareness should be created by internal events such as the intrusion detection alerts to allow the investigation to happen almost immediately.	20	6	4	0	1	31
A post-incident analysis of the event can enhance the already existing body of knowledge about fraudulent cases.	20	8	2	0	1	31

Please indicate your agreement or disagreement with the following statements about a unified fraud management and forensic approach.						
Answer Options	**Strongly agree**	**Agree**	**Neither agree nor disagree**	**Disagree**	**Strongly disagree**	**Response Count**
There is value in aligning the essential components of a fraud detection and forensic investigation through the intelligent use of both approaches.	26	3	1	0	1	31
answered question						**31**
skipped question						**9**