ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL EVIDENCE ACQUISITION TECHNIQUES FOR CRIME PROFILING BASED ON PROCESS EXECUTION CONTEXT ANALYSIS

Supervisor
(Ms. NANCY JAIN)
Associate Dean Silver Oak Law College
School of Law and Liberal Studies
Silver Oak University Ahmedabad

AUTHORED BY
BAVISHI DEVANGBHAI
MUKESHKUMAR
Enrolment No- (2519070400015)
School of Law and Liberal Studies
Silver Oak University Ahmedabad

CERTIFICATE

WHEREAS, under LL.M. Degree Course of Study and Examination, a student is required to write a Dissertation carrying 100 marks on the subject approved in partial fulfillment of the requirement for the degree of **MASTER OF LAWS** of the **Silver Oak Law College, School of Law and Liberal Studies, Silver Oak University.**

AND WHEREAS, **BAVISHI DEVANGBHAI MUKESHKUMAR** has been permitted to write a Dissertation on **DIGITAL EVIDENCE ACQUISITION TECHNIQUES FOR CRIME PROFILING BASED ON PROCESS EXECUTION CONTEXT ANALYSIS** for **LL.M.**

Examination of **2025-26** of the **Silver Oak Law College, School of Law and Liberal Studies, Silver Oak University.**

NOW THEREUPON, **BAVISHI DEVANGBHAI MUKESHKUMAR** has submitted the said dissertation which has been carried out by him under my guidance and supervision.

Date: **Supervisor**

(Ms. NANCY JAIN)
Associate Dean
Silver Oak Law College School of Law and Liberal Studies Silver Oak University Ahmedabad

ISSN: 2582-6433

DECLARATION (BY THE STUDENT)

I, **BAVISHI DEVANGBHAI MUKESHKUMAR,** hereby declare that the Dissertation work titled "**DIGITAL EVIDENCE ACQUISITION TECHNIQUES FOR CRIME PROFILING BASED ON PROCESS EXECUTION CONTEXT ANALYSIS"** is an original work done by my me under the supervision of **Ms. NANCY JAIN**, Silver Oak Law College, School of Law and Liberal Studies, Silver Oak University.

I further declare that to the best of my knowledge this LL.M. Dissertation does not contain any part which has been submitted for the award of any degree either in this University or in any other Institutions without proper citations. This dissertation work is done by me in adherence to the SOU-Anti-Plagiarism and Academic Integrity Policy 2020-21.

Date:

Name of the Student- BAVISHI DEVANGBHAI MUKESHKUMAR LL.M-CRIMINAL LAW

Enrollment Number: 2519070400015

ISSN: 2582-6433

ACKNOWLEDGEMENT

On Successful completion of my project report is marked by the gracious presence and blessing of "God" in my life though these blessings are beyond my thanks but still I pray to mark presence always ahead in my life. First and foremost, I express my sincere gratitude to my supervisor, Ms. NANCY JAIN, for their invaluable guidance, constant encouragement, and scholarly insights throughout the course of this research. Their mentorship has been instrumental in shaping the direction and depth of this study. I am also indebted and highly thankful to the Ms. Nancy Jain, Mr. Abhinav Kuchipudi, Rishabh Singh Panwar, Ms. Renu Beniwal, Ms. Mansi Pragya, and Ms. Mansi Sharma, faculty members, Silver Oak Law College, School of Law and Liberal Studies, Silver Oak University for their persistent encouragement and providing necessary facilities for carrying out the present investigation. It`s my personal conviction and no amount of space or word suffer to express my heartiest thanks to my friends and colleagues for unmatched help and encouragement during the investigation as well as study period. Finally, I acknowledge the contributions of all scholars, jurists, and researchers whose published works have informed and inspired this dissertation. Any errors or omissions in this work remain entirely my own. Many more people helped me directly or indirectly during course of studies, if I do not list them all, it is not due to lack of gratitude it is due to lack of space. To them all, I convey my best compliments and lots of thanks.

ISSN: 2582-6433

TABLE OF CONTENTS

ABSTRACT . . . . . .i iii
ACKNOWLEDGEMENT ix
LIST OF FIGURES xi
LIST OF TABLES . . . . . .
LIST OF TERMS AND ABBREVIATIONS xii

1 INTRODUCTION 1

1.1 Digital forensics 2
1.2 Memory forensics 2
1.3 Disk forensics 3
1.4 Network forensics 3
1.5 Cloud forensics 3
1.6 Mobile forensics 4
1.7 General data protection regulation 4
1.8 Goals of digital forensics 5
1.9 Crime profiling 6
1.10 Motivation for the work 8
1.10.1 Recent findings 9
1.11 Challenges in the field of digital forensics 10
1.12 Objectives 11
1.13 Research contributions 11
1.14 Organization of the thesis 12
1.15 Summary 12

2 LITERATURE REVIEW 13

2.1 Introduction 13
2.2 Digital forensic approaches 14
2.3 Information flow control and provenance 17
2.4 Cloud and distributed environment 19
2.5 Mobile security and general data protection regulation (GDPR) 21
2.6 Summary of existing approaches in literature 25

ISSN: 2582-6433

2.7 Key concepts and approaches from literature 27
2.8 Challenges faced by forensics investigators 29
2.9 Existing challenges 31
2.9.1 *The challenges in profiling cyber criminals 32*
2.9.2 *Current research challenges 33*
2.9.3 *Typical scenario 33*
2.10 Summary 36
3 EVIDENCE ACQUISITION TECHNIQUE USING PROCESS EX-ECUTION CONTEXT ANALYSIS 38
3.1 Introduction 38
3.2 Crime pattern matching based on process execution context 39
3.2.1 *Crime pattern matching using process execution contexts modules 41*
3.2.2 *The crime pattern matching algorithm 44*
3.2.3 *Kernel mode components 46*
3.2.4 *LSM module for forensics 47*
3.2.5 *User mode components 47*
3.3 Results and discussion 52
3.3.1 *Performance analysis tools 53*
3.3.2 *Overall performance analysis 54*
3.4 Summary 59
4 EVIDENCE ACQUISITION IN ADVANCED RESOURCE MANAGE-MENT SYSTEM FOR CLOUD 60
4.1 Introduction to distributed environment 60
4.1.1 *The host module 62*
4.1.2 *The host operating system 65*
4.1.3 *Hypervisor 65*
4.2 Design of ARMS 66
4.3 The classical stable matching algorithm 68
4.3.1 *Mathematical analysis of classical SM design 68*
4.3.2 *Design of egalitarian stable matching algorithm variant for ARMS 70*
4.3.3 *Mathematical modelling of egalitarian SM algorithm 71*
4.4 Results and discussion 73
4.5 Performance metrics 78

ISSN: 2582-6433

4.6 Summary 80
5 MOBILE SECURITY AND FORENSICS 82
5.1 Introduction 82
5.2 Mobile devices and evidence preservation 84
5.3 Mobile forensics process workflow 85
5.3.1 *Seizure, isolation and identification 86*
5.3.2 *Evidence acquisition and analysis 86*
5.3.3 *Data acquisition types 87*
5.3.4 *Examination and analysis 89*
5.3.5 *Reporting 90*
5.4 MDM based GDPR compliance for Android and iOS 90
5.4.1 *European union general data protection regulation - GDPR 91*
5.4.2 *MDM concepts 92*
5.5 Methodology 92
5.5.1 *Prerequisites 92*
5.5.2 *Architecture 92*
5.5.3 *MDM server application 93*
5.5.4 *Android and iOS built-in MDM support 94*
5.5.5 *Mobile vault app 95*
5.6 Results and discussion 96
5.6.1 *Category - data management 97*
5.6.2 *Category - data protection and monitoring 101*
5.6.3 *Category - device control 103*
5.7 Summary 103
6 CONCLUSION AND FUTURE WORK 105
6.1 Conclusion 105
6.2 Future work 107
REFERENCES 108
LIST OF PUBLICATIONS 121

ISSN: 2582-6433

LIST OF TABLES

2.1 Summary of the review of existing approaches in digital forensics . . . 26
3.1 Comparison of impact on performance of file system operations 55
3.2 Performance impact on common process execution 56
3.3 Performance impact on system calls in a server type system 57
4.1 Number of policy groups vs. time taken 78
4.2 Number of physical nodes vs. time taken 79

LIST OF FIGURES

1.1 Cyber attack scenarios and tactics 2
1.2 Taxonomy of digital forensics 6
1.3 Stages in criminal profiling 7
1.4 Number of cybercrime cases reported 8
1.5 Rise of crime rate in southern india 9
1.6 Types of cyber crimes 10
3.1 A sample pattern definition 44
3.2 Crime pattern matching algorithm 45
3.3 Crime pattern matching using process execution contexts 46
3.4 Crime pattern matching mechanism 48
3.5 Pictorial representation of process list in a desktop system - 1 50
3.6 Pictorial representation of process list in a desktop system - 2 51
3.7 A sample pattern matching report 52
3.8 Pattern matching - sample rule and event 53
3.9 Performance logging and tracing tools in Linux 53
3.10 Performance impact of PEC on file system operations 55
3.11 Performance impact of PEC on common system calls on a desktop system 56
3.12 Performance impact of PEC on system calls in server type system 58
4.1 Advanced resource management system (ARMS) architecture 62
4.2 ARMS functional modules 63
4.3 ARMS system design block diagram 66
4.4 Resource allocation using egalitarian SM algorithm 73
4.5 Sample event logs from ARMS system 74
4.6 ARMS GUI main window 75

ISSN: 2582-6433

4.7 ARMS GUI for resource allocation 76
4.8 ARMS GUI for virtual machine monitoring 77
4.9 Number of policy groups vs. time taken 79
4.10 Number of physical nodes vs. time taken 80
5.1 Security ecosystem of mobile and web apps 83
5.2 Remotely locate and erase all data in iPhone 85
5.3 Mobile forensics workflow 85
5.4 ADB logs 88
5.5 Managing devices in Internet 93
5.6 Managing devices in local network 94
5.7 DPS - High level software architecture 95
5.8 MDM server web interface for device control 96
5.9 MDM server web interface for device management 96
5.10 MDM client installed on iPhone 97

ABSTRACT

The large amount of data to examine as well as byzantine data flow patterns in con-temporary software systems have made the digital forensics process, specifically, the availability and acquisition of evidence data more difficult. A security enhanced oper-ating system kernel can make the evidence acquistion more authentic and spatiotempo-ral compared to conventional methods of evidence acquisition which usually rely upon analysis of application and system logs.

In this research, we have proposed such a security solution (Crime Pattern Matching based on Process Execution Contexts - CPM-PEC) which includes a process monitor-ing mechanism that is implemented with OS kernel. The kernel mode process monitors latent security susceptible events to an application counterpart that examines the events to find matches with latent crime patterns –which are pre-defined sequences of secu-rity susceptible events. This combination of kernel mode and user mode components makes sure that every process in the system is monitored from its creation to termina-tion for various outcomes in its lifetime. For evaluation purposes, the proposed solution is implemented and integrated to Linux Security Module (LSM) framework. Legacy methods of digital forensics tend to be lesser effective in a cloud environment. A proac-tive approach in which we observe and analyse the cloud system in real time using a distributed monitoring framework seems to be more practical. For investigations relat-ing to civil crimes and criminal cases, the digital data collected from mobile devices has become one of the primary sources of evidence.

ISSN: 2582-6433

In this thesis, the development and enforcement of policy for protecting the data in the systems using digital evidence acquisition techniques based on Process Execution Context (PEC) analysis which uses the Crime Pattern Matching (CPM) algorithm and CPM daemon process are proposed and implemented. The performance overhead of CPM is observed to be less than 2% on the Operating System kernel when compared against other security solutions. Evidence acquisition in Advanced Resource Manage-ment System (ARMS) for Cloud which uses the distributed policy and rule engines are implemented which make use of the egalitarian stable matching algorithm. The future work shall focus on research into more efficient evidence acquisition systems that should be ultimately built in as part of system software, even partially or fully im-plemented in hardware. Usage of Artificial Intelligence techniques by making use of distributed pattern matching to enhance the digital forensic investigation process is also under consideration.

Keywords: *Digital Forensics, Operating Systems, Cyber Security, Process Monitoring, GDPR.*

CHAPTER 1
INTRODUCTION

Digital forensics is around for a while and is rapidly becoming a specialized and ac-cepted investigative technique with its own tools and legal precedents that validate the discipline. The arena of digital forensics is not to impute guilt or innocence, but rather to find facts in the form of digital evidence that can be demonstrated so that others can consider the evidence and then impute, as appropriate, guilt or innocence in a constant way.

This work depicts the effectuation of the architecture in the field of digital forensics which could be used with stand-alone system as well as for forensics in distributed en-vironment. It is oriented towards concepts of cyber forensics, security architectures in Operating Systems, digital forensics support integrated with Operating Systems, chal-lenges of digital forensics and proposed solution for such challenges in a typical dis-tributed computing environment. The aim of digital forensics is not to prevent the crime as and when it happens, but to identify the victim and criminal either proactively or af-ter the attack or incident occurs in the system or in the network; analyse it in depth and record it for further reference.

Computer forensics can be defined as “the application of computer investigation and analysis techniques in the interests of determining potential legal evidence”; while digital forensics can be defined as “the application of scientifically established methods in preserving, collecting, validating, identifying, analysing, interpreting and presenting digital evidence to the court of law after obtaining

ISSN: 2582-6433

the evidence from reconstruction of events if possible". Digital forensics can be categorized into different groups such as Cyber Forensics, Disk Forensics, Memory Forensics, Cloud Forensics, Network foren-sics etc. And the attackers are usually referred as cyber criminals not as digital criminals and the crime is referred as digital/cybercrime.

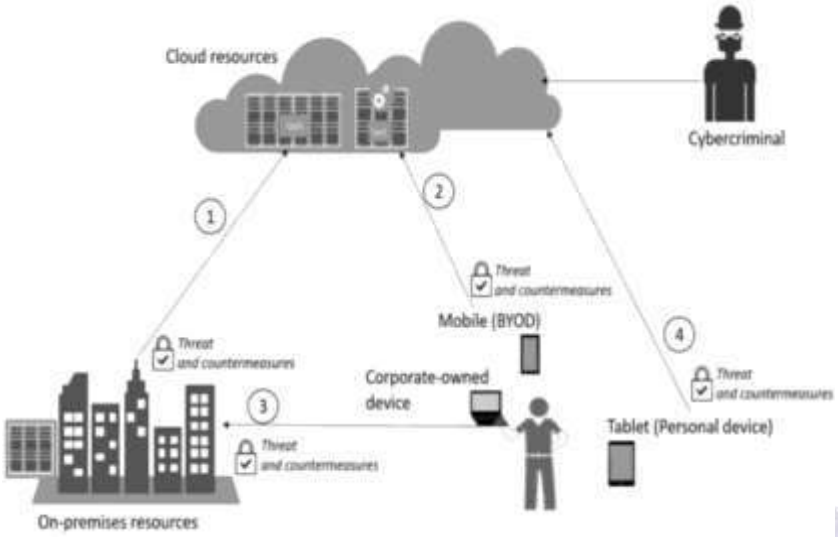

Fig. 1.1 Cyber attack scenarios and tactics

Fig. 1.1 illustrates different scenarios and tactics of cyber-crimes that include the whole spectrum of devices ranging from desktops and mobile phones to cloud systems.

1.1 Digital forensics

The application of scientifically established methods in collecting, preserving, validat-ing, identifying, analysing, interpreting and presenting digital evidence to the court of law after obtaining the evidence from reconstruction of events if possible. Digital foren-sic tools are application programs and utilities that automate various or specific digital forensic functions. These tools are credited for amongst other things reducing the time required to analyse large volumes of data, case management and standardized reporting and making it possible to carry out tasks that would otherwise have been impossible to complete manually. It is acknowledged that automation results in reduction in costs and significantly shorten the time needed for training forensic professionals.

1.2 Memory forensics

It is the forensic analysis of a computer's memory dump. Advanced computer attacks will use stealth techniques to avoid leaving traceable evidence data on the computer's non-volatile memory (hard drive, Solid State Drive (SSD) etc.). In those situations, the computing system's memory (RAM) dump is taken using OS tools or third-party tools for further forensic analysis. Using Operating System (OS) tools and symbolic debugging information of the OS components, it is possible to

ISSN: 2582-6433

substantially recreate the state of computing system to a reasonable analysis at the process and resource level.

1.3 Disk forensics

It is the analysis of storage devices which comes in numerous categories in terms of physical interfaces and storage technologies. The forensic analysis of disks mainly consists of application and operating system logs, picture analysis, signature / key-word analysis of known digital entities of criminal nature, timeline analysis, mailbox, databases, cookies, registry – virtually any persistent data that is commonly used by various application software and operating system.

1.4 Network forensics

It is all about the monitoring and analysis of computer network traffic for evidence col-lection, information gathering or even intrusion detection. Compared to the other areas of digital forensics, network forensics deal with more volatile data and thus it is consid-ered as a proactive approach of forensic investigation (Sammons, 2015). Network se-curity should be a huge concern to all of us, since the networks are under near-constant attack from lone hackers, organized criminals, and foreign countries. Cybercrime, cy-ber war, and cyber terrorism are major problems threatening not only our countries and companies, but our personal computers as well. Networks represent a far greater challenge, from a forensic standpoint. They vary wildly in size and complexity. There are several tools to help us protect our critical network infrastructure, including fire-walls and intrusion detection systems. Smart organizations plan for security breaches, enabling them to respond efficiently and effectively, minimizing the damage and in-creasing the odds that they can identify the perpetrator(s).

1.5 Cloud forensics

Cloud computing can be viewed as digital computing using shared collection of net-worked resources. So, it is evident that cloud forensics is closely related to network forensics. In a cloud, resources are shared and often duplicated (to avoid data losses) and a cloud service provider typically has hundreds to thousands of tenants from various jurisdictions whose computing needs are satisfied by the shared networked resources that the service provider owns. Information security in terms of privacy and access con-trol to these shared resources are of paramount importance in such a multi-tenant envi-ronment. Further to complicate the matters, huge sets of resources can be provisioned and de-provisioned dynamically in a cloud. Thus, it is apparent that legacy methods of digital forensics tend to be lesser effective in a cloud environment. Instead of trying to analyse huge amount of data for

ISSN: 2582-6433

evidence – which itself may require a cloud service in terms of required computing power, a proactive approach will be more practical. In a proactive approach (as it is given in section 1.4), we monitor and analyse the cloud system in real time using a distributed monitoring framework. We will see more of this proposed framework as we progress through the chapter.

1.6 Mobile forensics

Preponderance of mobile device in daily lives has led to their preponderance in daily crimes. Thus, the digital data collected from mobile devices has become one of the prin-cipal sources of evidence for investigations relating to civil crimes and criminal cases. These days it is meagre to carry out a forensic investigation that does not include a mo-bile device. Mobile forensics is a dvision of digital forensics that deals with obtaining and examining mobile devices to discover and retrieve digital evidence. In this context, the term "mobile devices" refers to a broad spectrum of devices which has communi-cation facilities and storage facilities for digital data. There are standard guidelines for the acquisition and analysis of mobile devices that are primarily targeted towards the preservation and non-contamination of digital data in mobile devices.

1.7 General data protection regulation

The European Union (EU) has acquired a set of new policies for the protection of per-sonal data entitled General Data Protection Regulations (GDPR). Personal data repre-sent all data (identifiers) relating to a known individual. GDPR do the discussions on the security of personal data are especially timely and convince people to alter proce-dures in conjunction with the handling of personal data by means of methods of public involution. GDPR focuses on the collection, processing, sharing and provisioning of data (Sullivan and Lewis, 2018). The work concentrates on the data interoperability regulations imposed by GDPR - namely, The Right to Inform (Article 12-14), Right to Access (Regulation EU) (Article 12, 15) and The Right to Data Portability (Article 12, A20). It explores the practical difficulties of data sharing using common data formats. The difficulties of data portability arise due to lack of contextual information that is available with common data formats and the work further article proposed the use of contextual metadata that is interoperable using a predefined syntax and semantics. This ensures seamless interoperability of the information flow between Data Controllers and Data Processors.

1.8 Goals of digital forensics

The basic objective of digital forensics is to analyse digital media in a sound manner to identify, recover, analyze and present facts and opinions about the information. The aim of the proposed and

ISSN: 2582-6433

implemented work is not to prevent the crime as and when it happens, but to identify the victim and criminal after the attack or incident occurs in the system or in the network, analyze it in depth and record it for further reference- ie. crime profiling. Computer forensics can be defined as "the application of computer investi-gation and analysis techniques in the interests of determining potential legal evidence". Bennett (2011) states that legal evidence might be sought constitute a wide range of computer crimes or misuses such as child pornography, use of abusive languages, audio or video, including theft of trade secrets, theft of or destruction of intellectual prop-erty and fraud. Usually digital evidences are the event logs generated by application software as well as operating system software. In modern Operating Systems, any ap-plication process will be running in a much-closed environment and Operating System will make sure that an application has minimal knowledge of any other application pro-cess that is running in the system. So, naturally, evidence data as event logs generated by such application processes lacks the overall system perspective. The data discovered is important in forensic analysis and in solving various computer crimes through proper log or record preservation which leads to profiling. Computer experts have many ways to recover data that remains in a computer system, or to retrieve information on deleted, locked, or broken files. So, the key consideration here is to find the most effective way to collect the evidence of a digital crime. Taxonomy of digital forensics is given in Fig.

1.2 including the proposed work.

ISSN: 2582-6433

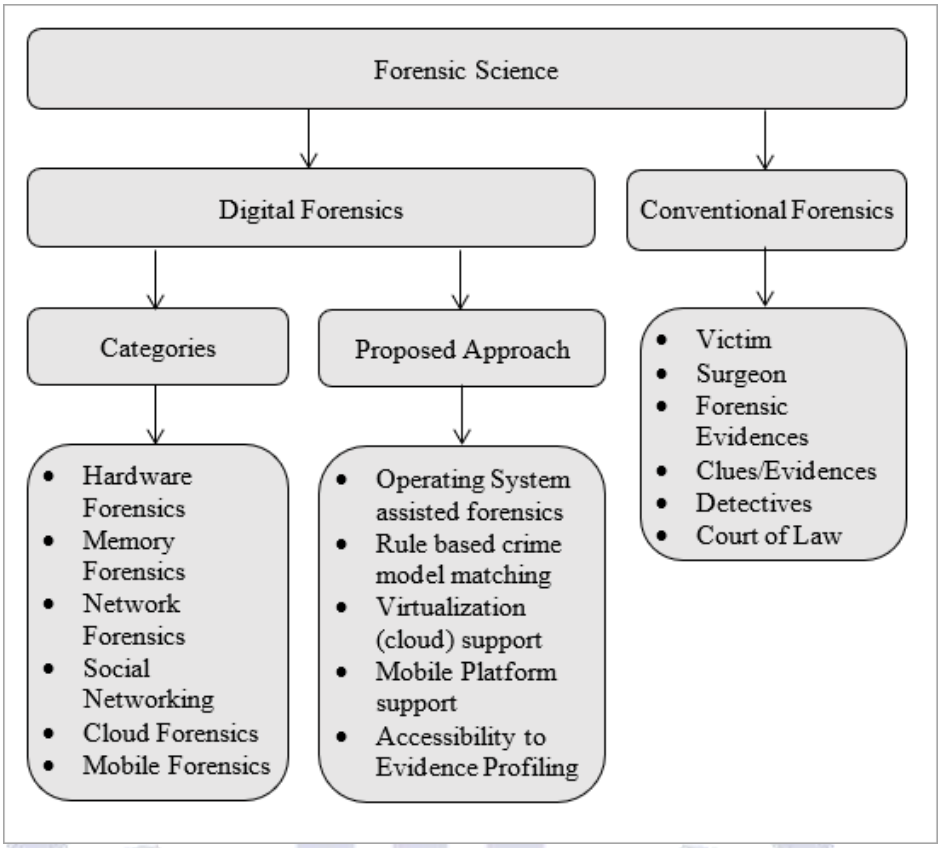

Fig. 1.2 Taxonomy of digital forensics

1.9 Crime profiling

Crime follows humanity from the Garden of Eden and human being is confronted with interesting mental conflicts such as whether to declare the world he is dared to commit a crime and get away with it or protect himself. This conflict, deepest in our minds manifests itself in actions: the criminal commits mistake and leave traces, always; ev-idence is the digital footprint left out during the commission of cyber/digital crimes such as terrorism, fraud identity theft or child pornography. Considering these aspects to get more from the interpretation of digital evidence, suggests for a new method - "crime and criminal profiling". Nykodym (2008) Point out that "the idea that an individual committing crime in cyber space can fit a certain outline (a profile) may seem farfetched, but evidence suggests that certain distinguishing characteristics do regularly exist in cyber/digital criminals". Tennakoon (2016) discusses the tools and techniques which might be worth testing in such a practical scenario. The steps/stages in criminal profiling are shown in Fig. 1.3.

ISSN: 2582-6433

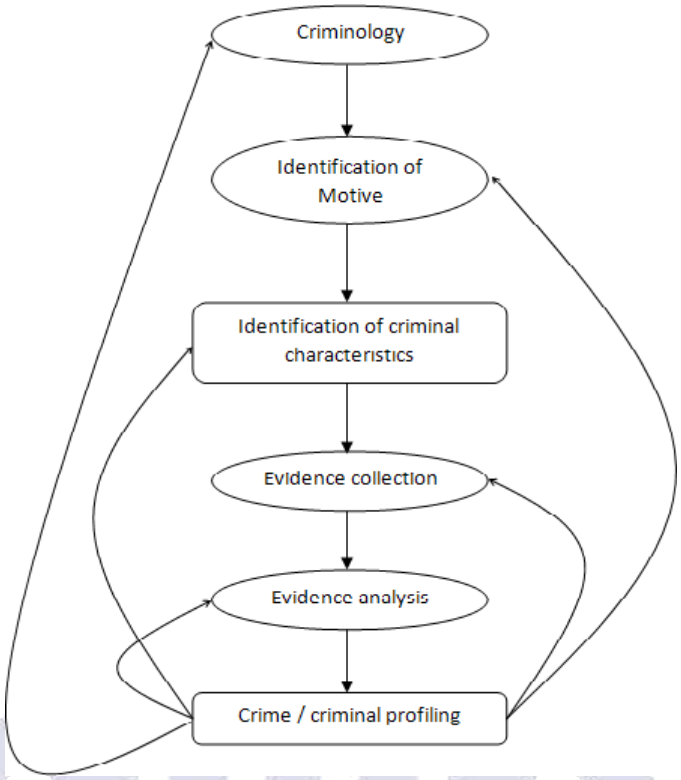

Fig. 1.3 Stages in criminal profiling

The criminal profiling has six stages:

1. Understanding what aspect of the victim attracted the criminals ("criminology")
2. Identification of a motive
3. Identification of characteristics of the criminal (expert, script-kiddie)
4. Collecting Evidence
5. Analysis of evidence
6. Repeat the above to refine the deductions.

From the research point of view, this analysis should give insights to what all data is to be collected from the system in the first place.

1.10 Motivation for the work

The following are some of the statistics of the study conducted on Cyber rimes in India. In the last 5+ years, about 200 zero-day exploits unleashed. 11.6 million mobile devices are infected at any given time. In 2014, more than 348 million identities stolen. Overall, about 594 million people were affected by cyber/digital crime. The statistics followed by the predictions by cyber/digital security analysts are as follows: Cyber security ana-lysts predicted that 2016 will be the year of online extortion. By 2016,

ISSN: 2582-6433

cybercrime will cost the global economy over USD 650 billion, climbing over to over USD 1 trillion by 2020. It is predicted that, by 2019, more than 30% of crimes by criminal networks will involve the theft or use of stolen data moved across international boundaries. It would be more than 1.5 billion people affected by data breaches by 2020. The cyber-crime rate has reached its peak in the year 2015. These details are some of the statistics presented during National Cyber Safety and Security Standards Summit, 2015 by the National Cyber Defence Research Team. The following Fig. 1.4 represent the recent statistics.

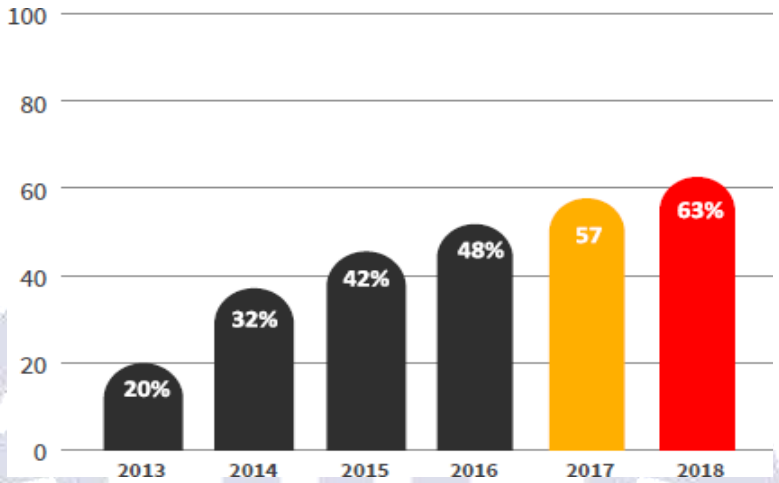

Fig. 1.4 Number of cybercrime cases reported

A graphical representation of rise of crime rate in India and specifically in southern part of India are given in Fig. 1.5.

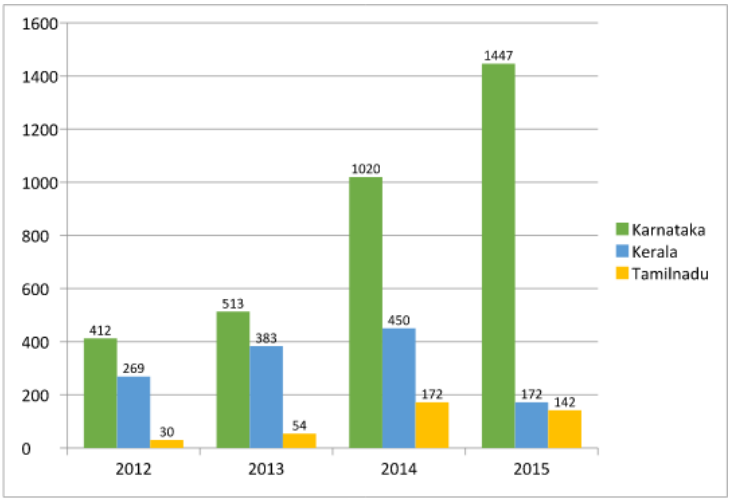

Fig. 1.5 Rise of crime rate in southern india

 ISSN: 2582-6433

1.10.1 Recent findings

Some of the more recent findings or the recent cyber threats identified in 2018-19 are:

1. Cyber-attack on Cosmos Bank, the has lost 94 crores.
2. Facebook Breach, 50 Million users were compromised.
3. Uber Data Breach, Uber had pay Euro 133 M to settle the legal penalisation
4. British Airways, 380,000 transactions were affected.

Small and Mid-sized Business (SMB)s, outlined as those with 100 to 1,000 employ-ees, are hardly immune to cybercrime. According to the recent Keeper Security survey, "The State of SMB Cybersecurity" report, a staggering 50 percent of small and midsized organizations reported suffering at least one cyber-attacks in the last 12 months. The average cost of a data breach totalled $879,582 for these SMBs. TAfter the booming attacks they spent another $955,429 to rebuild normal business. 60 per cent of workers use the very same password for all data they view for these SMBs. Meanwhile, a poor, default or stolen password effectively worked by 63 percent of reported data breaches. As shown in Fig. 1.6, by the year 2020 the costs associated to issues caused by cybersecurity breaches may reach $5 trillion and that is why it becomes crucial to make sure that every business infrastructure is up-to-date and ready to avert cyber crimes.

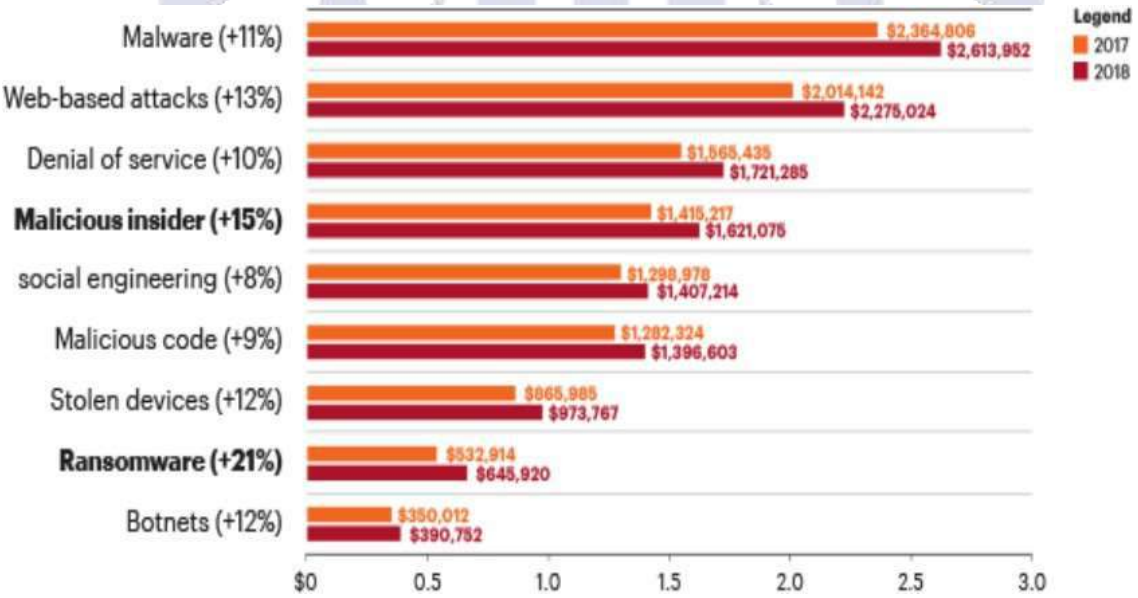

Fig. 1.6 Types of cyber crimes

1.11 Challenges in the field of digital forensics

Constant developments in Information Technology and Communication have posed many challenges in the field of digital forensics. Based on the advancements on ex-isting digital

ISSN: 2582-6433

forensic models, these are some of the major challenges in this field:

1. The lack of real data sources for study and analysis purposes
2. The lack of efficient and readily available tools to data acquisition and analysis
3. The limitation of the operating environment during the acquisition of data
4. The accessibility to the data – especially if the data is on distributed systems
5. The volume of data and the time taken to undertake an investigation
6. The ultimate lack and differences of laws across the countries
7. Multitude of OS platforms and file systems
8. Cloud system that has multi tenancy and involves multiple jurisdictions

Legal support and forensic standardization are also challenges encountered in net-work forensics. Chen *et al*., (2015) states that the real time and comprehensive audits in distributed environments like cloud are very difficult and post audits can be rather challenging. The capacity of comprehensive investigations and the collection of web exception information are also limited.

Evidence disappearance is also a major challenge in distributed digital environment, especially in cloud networks. Regional considerations such as the collection of evidence should be compliant with local laws and regulations that increase the time and cost dif-ficulties of forensic investigations. Privacy matters of established users are also a prob-lem which has come across in digital forensics. In a multi-tenant natural world, how to prove capable forensics range to protect the privacy of valid users is still a dispute. Evidence fixation/collection/preservation can be byzantine in cloud and distributed en-vironments, because investigation implies non-standard data sets, such as processes and workflow information.

1.12 Objectives

The main objectives of this work are:

1. Analyze the current digital evidence acquisition and analysis techniques.
2. Propose the Process Execution Context (PEC) analysis techniques and compare against existing approaches.
3. Apply the PEC techniques in standalone host systems.
4. Apply the PEC techniques in distributed system and cloud systems.
5. Application of PEC equivalent MDM technology in mobile platforms for GDPR compliance.

ISSN: 2582-6433

1.13 Research contributions

In this thesis, the development and enforcement of policy for protecting the data in the systems using digital evidence acquisition techniques based on PEC analysis which uses the crime pattern matching algorithm and Crime Pattern Matching (CPM) daemon process are proposed and implemented. Evidence acquisition in Advanced Resource Management System (ARMS) for Cloud which uses the distributed policy and rule en-gines are implemented which make use of the egalitarian stable matching algorithm.

We have done the study of existing mobile forensic approaches, proposed and imple-mented Mobile Device Management (MDM) based GDPR compliance for Android and iOS.

The future research will focus on improving the whole cyber forensic investigation process by introducing log-based profiling, built in as part of system software and in some cases, even partially or fully implemented in hardware.

1.14 Organization of the thesis

Chapter 1 explains the basic concepts of digital forensics and its applications. The growth of this field over the years, research challenges and motivation are also men-tioned in detail.

Chapter 2 provide a review of the related works accomplished in this domain with the various approaches, digital forensic modelling and tools used. Further the content about the need of the work is discussed.

Chapter 3 explains evidence acquisition techniques using PEC analysis, detailed ex-planation of Crime Pattern Matching (CPM) algorithm is provided and the performance also compared against other traditional methods.

Chapter 4 discusses the evidence Acquisition in ARMS for Cloud which gives a glance of the egalitarian stable matching algorithm used in ARMS cloud and finally the performance of PEC in ARMS cloud is compared against traditional method.

Chapter 5 depicts the traditional Mobile Forensics tools and the challenges encoun-tered while applying the proposed technique in mobile platforms. Also discusses about the MDM based GDPR compliance for Android and iOS – A future enhancement pro-posal in detail.

Chapter 6 concludes the thesis by giving various justifications for the proposed tech-niques and extension of the future work is also depicted.

1.15 Summary

In this chapter a brief introduction about the basics of digital forensics and the need and challenges faced in digital forensics are described. The motivation, objectives are clearly explained to make the

ISSN: 2582-6433

reader to get a flavour of this thesis in detail.

CHAPTER 2
LITERATURE REVIEW

Forensic computing and digital crime investigation emerged because of huge rise in dig-ital crime due to the expansion of the Internet and proliferation of digital technology. As part of the work, we reviewed the literatures in computer forensics and distinguished many divisions of activity research in computer forensics. A few research divisions are framework, trustworthiness, computer forensics in networked or virtualized environ-ments and acquisition and analysis of evidence data. The progression such as compo-nents, approaches, process of each subdivions have been examined and discussed.

2.1 Introduction

Small and medium-sized organizations (SMBs), described as having between 100 and 1,000 employees, are barely exempt from cybercrime. According to the recent study" The State of SMB Cybersecurity" by Keeper Security, an incredible 50% of small and medium-sized companies have reported experiencing in the last 12 months at least one cyberattack. For these SMBs the average cost of a data breach involving identity theft was $879,582. After the booming attacks they washed-out another $955,429 to restore normal business. 60 per cent of workers use the very same password for all data they view for these SMBs. In the meantime, 63 percent of corroborated data breaches effectively act as a poor, default or robbed password.

Today's massive volumes of data, disparate information and communication tech-nologies, and marginal cyber infrastructures create new challenges for security special-ists and law enforcement experts investigating digital crimes. Serious concerns have been raised about user privacy leaks in mobile apps, and a range of prevention strate-gies are suggested. (Wang *et al*., 2018). To ensure that no warning is made, new mo-bile malware imitates the confidentiality-cognized actions and the privacy leak with benign apps, to reduce the likelihood of being monitored. While traditional approaches primarily emphasize the advancement in privacy disclosure, these deceptive strategies can make it difficult to distinguish between malicious and benign privacy disclosures throughout the privacy leak review. In this study, the authors suggested Privacy Context to use context for malicious privacy leakage. Security Context can be used to distill the effects of security leak detection for self-regulation and casual making by permeating innocuous data disclosures. Experiments show Privacy Context can conduct an amaz-ing and knowledgeable static privacy enhancement analysis and filter out a malicious privacy leak at 92.73% true positive pace. Evaluation also suggests that, in order to maintain the consistency of the privacy categorization, these proposed contexts are all required.

ISSN: 2582-6433

Over recent years the Web has shown huge growth and the wallop, quality and number of threats to it also grew. Organizations aim for technological security against aggressive and increasing risks for their data and networks (Gupta *et al*.,2018). The security and monitoring program has become an inescapable feature of all the busi-nesses that wish to protect their data from network attacks. In the study, a categorical overview of the various research methods used to enhance the application of Snort's open-source intrusion sensing program for the detection and avoidance of intrusions was presented. All the strategies showed their advantages and disadvantages. In order to increase Snort's performance in a high speed network, an original parallel architec-ture was created. The architecture is assisted by the part network traffic protocols.

2.2 Digital forensic approaches

Garfinkel (2010) proposed a design for accomplishing an enhancement in the efficiency of forensic tools and operational efficiency by means of adopting of few taxonomic forensic evidence and forensic analyses identification methods. It summarizes a brief history of digital forensics, mentioning the early days, golden age of digital forensics and the emerging digital forensic crisis. It also discussed about the research challenges such as evidence-destined design, the profile, filter and report model and the difficulty of reverse engineering. This work further discussed about the monolithic applications and lost academic research. His work proposed a new research direction which in-cludes forensic data abstraction using the digital forensic XML which is a wide range of digital metadata used for compatibility. It discussed alternative analysis models such as stream based disc forensics. Garfinkel's work concludes with a statement stressing upon the need for more powerful abstractions with careful attention to co-operation, standardizing and communicating the progress of the research community with the goal of enhancing research efficiency.

Endicott (2006) depicted that, When an accident respondent gathers forensic net-work data, they often have to compromise between using the tools to capture forensic sound data and to restructure the network as quickly as possible. Organized foren-sic preparedness networks have now been established as an area for research, with suggested checklists, procedures and tools to complement these choices. This work suggested a methodology for the life cycle of the forensic preparation organizational network "operationalization." As an analytical context for making more professional, constructive contributions to digital network forensics, the theoretical framework and the resulting approaches are expanded.

Sikorski (2012) has clearly mentioned that attacks can cost a company dearly since malware analysis is huge business. When malware attacks the defences, it is advised to work implusively to heal presnt infections, look forward and prevent future ones from taking place. To setup a safe virtual environment

ISSN: 2582-6433

to analyze malware, key analysis tools like IDA Pro, WinDbg, olliDdg could be used.

O'Connor (2012) reveals the move to practical implementation from a theoreti-cal understanding of predatory computation. The python programming language helps build one's own weapons. He clarified how Python scripts can be written for the control of large-scale network emergencies, metadata processing and forensic objects analysis. Erbacher (2010) discusses the problems orbiting around the need for validation and error in digital world for the accession of evidence. It was discussed how digital ev-idence as such disagree and disputes with privacy protection that is essential to con-ventional computer security. Finally, the theoretical basis for the supply of validation and the computation of faults in digital worlds were laid. The need for validation and conclusion of error within digital forensics has been identified in his work. As can be understood from current research, there is emerging involvement in facets of error and validation related to digital forensics. However, recent research has not had the in-depth knowledge which is obligatory to make sure legal admissibility or examined all facets of validation and error in an integrated platform. This needs to be tremendously prolonged.

Nance *et al*., (2009) identified six research areas in Digital Forensic domain such as Evidence Modelling, network forensics, forensics control systems, processing and analysis of parallel data, acquisitions and forms of media. If a framework could allevi-ate all the areas of the digital forensics process, it could be possiblly used for the crimes available. The forensic analysis techniques generally handle the compilation and ex-amination of the storage media in the target system although the system's runtime state is generally restricted or not available. Thus, core data or information which are not part of the assessment can also be obtained, such as network connections, encryption keys, decrypted data or procedure lists. RAM research, methods for undermining the live acquisition execution and methods for carrying out live analyzes on devices without affecting the sequence of execution is introduced to the work group. This study further illustrates the development of digital devices, where the wide number of digital devices that often form part of a research process can be seen in this transition. The evolving nature of digital gadgets is also emphasized in this work.

Kyei *et al*., (2013) depicts that the advancement of technology and the rise of the crime rate has provided law enforcement authorities with a challenge / task on how to solve such Medieval lay offenses. They have stated digital forensic models should ensure the identification for all malicious events that are occurred and should determine the involvement of different parties.

Yusoff *et al*., (2011) says that the increase in criminal activities using digital devices or data as the means or objectives needs a a structured solution in dealing with them. In a number of ways, analysts collect data. A network or a group of nodes or computers can be detected. We do this in a variety of places on the network (for example, at the gateway or firewall), or on the server or computer.

ISSN: 2582-6433

The data can be collected in real time in the process of an autopsy analysis (as is common with a broken or corrupted intrusion detection system), or the researcher can anticipate the type of data it needs to prepare it for documentation. This is achieved in a standard way for logfiles on a damaged or disabled device. A variety of technical and non-technical parameters are applied to interpret the data as it is gathered. The deficiency in interpreting of how systems work can lead to errors.

Digital evidence comes from many places that require hard drives or archive files, real-time e-mails, chat-room logs, ISP documents, web pages, digital networking, local and remote directories, computer registry, telephone, memory and file cameras. Such material is not only available from the Internet but also from the Internet. A censorious metric which forensic analysts would find is the function of the rightful trust in this digital data. It is disturbing that even the beginner users of the machine are now easy to modify, kill or produce digital proofs in a convincing manner. The methods used today are dependent on individual ethical considerations, processes, protocols and protection of physical access. Such strategies are expensive, vulnerable to unintended or deliber-ate alteration, and prohibit the centralized use of digital evidence in important divisive roles. They are full of potential mistakes.

Walker (2009) depicts in his work, bringing the evidence to court, that the area of computer forensics is practiced by law enforcement officials, federal, state and local governments. And it's the "clean" of the shown data that is the explanation for this scan. It is essentially the use of the tools of modern crime investigation and research in order to find vital legal evidence. It reports on the procedure for identifying, gathering, preserving and reviewing facts to ensure its admissibility in legal proceedings.

2.3 Information flow control and provenance

Chen *et al*., (2015), discusses scope of a data security breach in terms of application boundaries. Securing confidential information using traditional means such as user-names and passwords or network firewalls along with cryptography are not effective to prevent the data leakage because an authorized program to access and decrypt con-fidential data can propagate that information to other unauthorized programs without any further checks. To overcome this limitation of traditional security systems, two ma-jor techniques are proposed for implementing digital security mechanisms in software systems. They are:

1. Information Flow Control (IFC)
2. Provenance of Digital Assets

ISSN: 2582-6433

Information Flow Control (IFC), will track information flows from one application to another once they are introduced in a network and exclude the flow when not needed according to a pre-defined policy. (Thomas and Dieter, 2014). The standard method has a sensitive (high) or a public (weak) security mark for the data, in which there is no low background in high data flows. The IFC can be enforced statically in the program source code by labelling each variable with types such as high and low and the compiler makes sure that no assignment is made from a variable labelled high to another variable that is labelled low (Mahmoud *et al*., 2015). IFC can also be implemented dynamically but the runtime cost is observed to be prohibitively high (Chen, 2013; Stefan *et al*., 2018). As mentioned by, Andrei (2018) and Andrei and Murray (2017), IFC is a more effective mechanism for information security compared to traditional access control. However, once a breach is found, IFC terminates the violating programs and whole system is stopped which is not feasible in real life because availability of programs is of utmost importance.

Compared to IFC methods, Provenance method concerns about various information: origin of data, who manipulated data and how etc. Obviously, provenance, concerns more about valuable evidence information and is the focus of this work. Provenance can be done in an application specific or a work-flow specific way – but these methods severely limits the effectiveness of the method from a digital-forensic point of view. Pohly *et al*., (2012), debated that interpreting interaction between processes and files were not enough to captivate provenance within an OS. It is essential to captivate the data swaps on all system calls inorder to understand the complexity of an OS and the complex interactions taking place. Hi-Fi acquires system-wide provenance data from kernel level, using the Linux Security Module solution, and consequently able to mon-titor all interactions between kernel objects.

Based on this work, Pasqueira *et al*., (2016) and Bates *et al*., (2016) put forth a Linux Provenance Module (LPM) using hooks like that defined by LSM (Linux Secu-rity Module), Smalley *et al*., (2001a; 2001b; 2001c; 2001d; 2001e; 2002; 2013) for preventing sensitive data loss from predefined corporate domains. It is noted that such policies can be easily represented in IFC (Tomoya and Makoto, 2017). This work pro-vides an in-depth analysis of security subsystems in Linux kernel.

2.4 Cloud and distributed environment

As many business applications and data migrate into the cloud platforms, technol-ogy ecosystems become easy targets for criminals searching for potential loopholes. (Youssef *et al*., 2018). The position of today's IDS generation has different limits on its deployment and could produce several false positive warning devices that would make it unsuitable for cloud computing

ISSN: 2582-6433

security. Examining the number of false alerts and improving the efficiency of IDS, based on attack dynamics and a risk assessment, has shown the efficacy of intrusion. Nonetheless, it lacks a true risk value in terms of the function of the same value of chance. This research has led to show a new probability and behavioral method for assessing the possibility of calculating cloud attacks. The main task is to improve the effectiveness of IDS and to reduce warning rates. Empirical results reveal that the approach of intrusion detection is successful in the cloud using state-of-the-art.

Safety experts and antivirus companies concentrate on Android ransomware, which can harm our phones and place Android businesses at risk. In these work, Droid ®, a scaled-in self-improvement tool designed to self automate signature collections, detect malicious apps at the level of source code, was suggested and created by its develop-ers. A malware detection model for software was developed, tested and introduced. It system has been applied and tested for almost 30 thousand programs, of which 27 000 benevolent and 3 670 malware. (Junaid *et al*., 2019). In various applications, DroidMD detects malware at absolute and partial level. Only the program code is tested to boost its usability. DroidMD found analog malware code fragments from innocuous programs in various malware families and user code directories. DroidMD often detects related fragments of code which can suggest malware in a number of applications. DroidMD's ranking shows that the system is highly skilled in large-scale malware detection with

95.5 percent accuracy.

The number of cyber security incidents that have been examined by Law Enforce-ment Agencies (LEA) is growing sharply in scale and density. Criminals may refuse to commit a crime, but LEAs are prohibited from determining this by limited human intelligence processing capacity. (Kao and Raylin, 2018). Although analysis at the first crime scene accentuates as early as possible the discovery of wrongful information, lab-oratory forensics reconstructs this event and cross-references the facts to find the truth. Both are crucial components of the cyber-security investigation response. The paper introduces a realistic, ISO 27043-based forensic data framework: 2015, dedicated to working with digital evidence on the crime scene and rising the caseload spirit in the laboratory. The writers intend to put their theory into practice for LEA's by recom-mending the intelligence-led approach to inquiries into the crime landscape and to deal with the analysis and resolution of cybersecurity accidents. The aim was to encourage LEA to build a solution to cyber crime by taking into account the various processes and practices of practical work.

Current cloud architectures do not abide by today's digital forensics procedures-mostly due to the basic changing nature of the cloud. In order to provide data integrity and admissibility, Data acquisition is the first and arguably most important method to digital forensics. Researchers are currently unable to rely on the cloud service providers (CSPs) to gather evidence for them. Clarke *et*

ISSN: 2582-6433

al., (2019) presents an approach to per-form acquisition in an IaaS infrastructure whilst maintaining the ”gold standard” acqui-sition model of acquiring a bit for bit copy. This work presents a series of experiments to exemplify and model how the new cloud FAAS would provide more rich and detailed information than the incumbent CSPs can get, guaranteeing customer retention of data ownership. The results also provide an insight into the operational costs of deploying Cloud FAAS.

Montsari *et al*., (2019) depicts in their work that, the several cases that demand Digital Forensic Investigations (DFI)s are growing, culminating in the conception of a reserve of cases for Law Enforcement Agencies (LEAs) globally. Hence, it is of pre-ponderant importance that new research methods be followed to handle these security threats. Their work appraises the current set of contexts encompassing the field of Dig-ital Forensics (DF). And this work makes two distinguished contributions to the field of DF. First, it examines the most critical technical issues that need to be advised by both LEAs and Digital Forensic Experts (DFE)s. Second, it suggests important precise future research directions, the attempt of which can help both LEAs and DFEs in taking over a new approach to combating cyber-attacks.

2.5 Mobile security and general data protection regulation (GDPR)

GDPR focuses on the collection, processing, sharing and provisioning of data (Sulli-van and Lewis, 2018). The work concentrates on the data interoperability regulations imposed by GDPR - namely, The Right to Inform (Article 12-14), Right to Access (Regulation eu) (Article 12, 15) and The Right to Data Portability (Article 12, A20). It explores the practical difficulties of data sharing using common data formats. The dif-ficulties of data portability arise due to lack of contextual information that is available with common data formats and the work further article proposed the use of contextual metadata that is interoperable using a predefined syntax and semantics. This ensures seamless interoperability of the information flow between Data Controllers and Data Processors.

Liapakis (2018) tries to combine the ethical, legal and technical points of view of GDPR on personal data. Insurance companies collect, maintain and store private data as well as special category data. They use this data not only for customer services, but also for potential profit by sharing this data to other business entities such as hospitals, claims management companies, sales channels, fraud detection services etc. The work tries to provide guidelines to evaluate the GDPR ”maturity level” or such partnerships so that the insurance companies can make quick logical decisions about selecting such business partnerships.

Patrick and Simone (2018) has conducted an extensive survey on GDPR. A funda-mental privacy policy and a right that is well accepted by GDPR is the transparency of personal data processing. The end users have the right to have perception about what data have been collected and refined about

ISSN: 2582-6433

them. They also have the right to know the feasible outcomes might develop after their data have been exposed - i.e. ex post. The objective of ex post Transparency Enhancing Tools (TET)s is to render such perception to the end user about his personal data. This survey assesses the serviceability of ex post TETs and analyses them in terms of their shared features and singular characteristics.

Cloud Computing moves data processing aside from general possession and man-agement to a third-party furnished, globally distributed service (Varadi, 2016). This ascents many legal problems related to GDPR. This work surveys and summarizes the most relevant changes GDPR conveys to the study of Clouds. It also finds parallels between GDPR and the former statute law called the Data Protection Directive. The ar-ticle covers essentially legal aspects of data mechanics, which are part of the operating of all systems, especially cloud environments.

Tzolov (2018) emphasizes the fact that the implementation of GDPR in organiza-tions should be perceived in the context of their business objectives. There should be a value addition to business by adhering to GDPR and it should not be taken as another restriction to the business operations. In the work, the author presents the usage of the ISO 9001:2015 standard, as a new methodology for GDPR implementation by bringing out a essential reward that is based on trust factor between the organization, employees, clients and partners.

The legacy databases that stock user authentication credentials in plaintext or utiliz-ing outdated encryption methods are non-compliant to best practice standards of GDPR (Furey and Blue, 2018). Substandard security implementations or the complete lack of them have made the databases that stores authentication credentials a frequent target of cyber-attacks. This work presents a fresh resolution for enhancing the security of non-GDPR compliant authentication databases. The best practice recommendations refer to the old and freshly created passwords that are stored in the files in the form of salt, one-way encryption and iterations. It claims the prospective to enhance system security and help the development of GDPR necessities.

Gokila and Baggili (2018) proposed a work of forensic on the Apple's iPhone, they developed a basic version of the software tool for forensic which they called it as FEAAS- forensic Evidence Acquisition and analysis system which bring together evidential data into legible format which can deduce user events. This is similar to our work. But have limitations such as it works only for one version of Apple iPhone and home pad. And if the data is already erased from the phone it will not do the extraction of evidence data.

Crompton and Jenson (2018) states that Fog computing is an extension to cloud computing to facilitate the development of Internet of Things (IoT) services. As Fog comprises of heterogeneous devices in term of capabilities, operating systems and com-munication protocols. These devices are dynamically sharing resources to render ser-vices that makes use of the low response capacities

ISSN: 2582-6433

of the regional edge tools and centralized cloud providers' high processing capacities. The heterogeneous and au-tonomous nature of devices on Fog computing that handles private data of end user presents a big challenge to ensure and demonstrate GDPR compliance. This work presents a prototype security library (in JAVA) that implements a subset of the speci-fications for computer security and privacy of Fog-to-Cloud systems and GDPR. This uses an authentication and authorisation PKI-based trust model. There are policies to ascertain data confidentiality, integrity and non-repudiation.

Contextual data security and threat notification standards are relevant to organiza-tions settled or in the market of the EU. Heims (2016) in his work compares the GDPR regulation to corresponding US and Canadian standards. Although each regulation dif-fers, the articles demonstrates that all these regulations explain the situational risk and damage to individual data subjects and strongly promote encryption.

EU General Data Protection Regulation (GDPR), debates on preserving personal data are especially timely and ensure that the mechanisms of alteration in personal data related to public engagement approaches be checked in advance. (Diamontopauluo *et al*., 2018). The through use of social media has made these into valuable tools for addressing and supporting decisions in the development of public policy; this has led to new democratic engagement components, such as crowdsourcing strategies, which have contributed to much more inferential exchanges between policymakers and indi-viduals or experts, so that their knowledge, viewpoints and insights can be used. In this work, Three innovative crowdsourcing approaches in public policy systems are rig-orously evaluated towards this direction, analyzing the data collection and processing schemes they comprehend. The research imparts to the identification of problems that crowdsourcing, e-participation methods enforce reckoning to privacy protection.

An anchpred work on data protection assurance anticipating GDPR is conducted by Altorbaq *et al*., (2018) and the new GDPR allows cloud-based organisations to se-cure specific rights for the data objects, such as entry, order erasure and correction of their records. Owing to the technological ramification and collaborative cloud service environment, the flow of personal cloud data must be handled and controlled from its original collection, through processing to its actual, organizationally and technically difficult expunction. This research discusses the challenges associated with the partner-ship, as well as theoretical latent approaches for organisations which are to effectively demonstrate conformity with the Legislation and respond to data subjects' rights de-mands and contributed a polished model rendering phases of a personal information life-cycle. These results are expected to be obtained both from consumers and cloud services providers and from the data subjects whose interests are assured. Romansky and Kirilov (2018) presented the procedure of

ISSN: 2582-6433

contriving a web-based framework to assist in the understanding and enforcement of the new regulation on data protection. The developed system has been exploratory formalized and a sample analysis has taken place using the Petri nets apparatus.

Ducato (2018) discusses about his research set for General Data Protection Regu-lation about the health cloud and data protection issues. The study aimed at outlining the driven guidelines for the new GDPR to ensure data protection in cloud settings, and to tackle big unresolved issues seriously, with particular focus on treatment in the healthcare sector. Cloud computing is becoming a competency in the infrastructure for saving, accessing and using data on web-based remote devices. Consumers can monitor nearly full electrical power on need, do not have to invest heavily to meet their needs and access their data throughout the internet from anywhere. The cloud is particularly exciting for applications in many various sectors and businesses, including healthcare. In order to separate such a significant set of information sources and tools and to use advanced data mining techniques for processing health data, Cloud computing is the technical prerequisite under consideration.

The integration of Information and Communication Technologies (ICT) in the Euro-pean Union has contributed to substantial changes in management and industry. Modern ICTs also drive the digital economy through the daily life of people (Zdzislaw, 2018). The aim of this work is to illustrate the way GDPR is applied in selected organizations and management. The first part of the article explains the GDPR's underlying assump-tions. The presentation of the methods of implementing the GDPR and a description of the selected case studies are described as analysis of the literature and the legal regu-lations on this matter. The practices undertaken revealed that IT experts, attorneys and administrators have the best results when applied by teams.

General data protection regulation — Security of personal information in an enter-prise: Personal data corresponds to all data (identifiers) associated with an identified individual, The European Union (EU) has taken up a new framework for the protec-tion of personal data entitled General Data Protection Regulation (GDPR). Tijan *et al*.,

(2018), in their work analyzed the differences between the new GDPR and the existing Data Protection Directive from 1995, which is still active.

Fischer *et al*., (2018) states that, Blockchain allows new ways to solve privacy is-sues in distributed systems, yet also poses new questions about the transparency and immutability of distributed systems. The European Union has taken several steps to ad-dress data protection concerns and identify data subject rights and obligations of con-trollers and processors. They anticipated the work to result in a standard for GDPR

-conforming Blockchain technology innovations. Through the freedom to receive in-formation on

ISSN: 2582-6433

the collection, for whom data is stored, and by asking for manipulation or erasing at any time, data processing should be more transparent for subjects. The GDPR is applied in situations in which services are provided to EU citizens to all organizations in the EU that handle their personal information, and to third-country businesses. The public authorities that have expanded access rights to the collection operations for per-sonal data are also required to comply with the data protection provisions.

Using the GDPR as an example, the value of privacy policies for improved reality usage / methods implementation in best practice is analyzed. (Phil, 2018). It aims to understand how privacy rights can further improve inclusiveness. Augmented Reality (AR) relies on technologies that have to obtain information from their environments on a real-time basis and are therefore fundamentally affected by such regulations.

For Blockchain Infrastructure for Personally Identifiable Information Management the EU GDPR ask for the right to forget and should delete privileges Lee *et al*., (2018) in their Work suggested an off-chain blockchain architecture which uses a trustworthy life cycle using both the local database and distributed leadgers. In view of the key criteria of GDPR, the dominant architecture of Blockchain was modified and the suggested ar-chitecture formalized using multi-chain 2.0 and, along with the GDPR privacy control, the proposed consumer of software would improve Blockchain safety and stability.

2.6 Summary of existing approaches in literature

A summary of the review of existing approaches in digital forensics is given in Table 2.1.

Table 2.1 Summary of the review of existing approaches in digital forensics

Author	**Year**	**Key concepts/Methods**	**Challenges/Issues not resolved/mainly discussed**
Endicott-Popovsky *et al*.	2005	Case Study Analysis	Was a case study
Barabara Endicott *et al*.	2006	Life Cycle Methodology	Civil litigation and Lack of proactive approaches
D H Kim and H Peter In	2008	Markov Model-NEPA Algorithm	Estimating the user's behaviour in terms of increased modelling accuracy
Micheal Losavio *et al*.	2008	Analysis and Categorization of crimes	Lack of expertise

ISSN: 2582-6433

Kara Nance *et al.*	2009	Modelling the investigative process and case modelling	Run time state of the system not accessible
Robert Erbacher	2010	Validation and computation of errors	Software implementations with errors are not well defined
Curran and Cassidy	2010	Analysis of network traffic	Suppression hearing, tools were not fully developed
Yunus Yusoff *et al.*	2011	Comparative study by activity phase	Comparative study
Simson L Garfinkel	2010	Comparative study of DF	Need of powerful abstraction
Bin-Hui Chou *et al.*	2009	Secure virtualized logging scheme	Maintenance of log repository difficult
David W Bennet	2011	Evidence admissibility chain of custody	Differences in cyber law
Jingsha He *et al.*	2013	Forensic in different scenarios	Comparative study
Cornell Walker	2013	Evidence preservation and Analysis	Lack and Differences in cyber law
Fakeeha Jafari and R S Satti	2015	Exploratory testing	Lack of experienced staff in investigation
Lei chen *et al.*	2015	Cloud security analysis	How to reduce the acquisition time when retrieving the mass amount of data.
Okechukwu Wori	2014	Categorization of criminal activities	Blending of organized and unorganized cyber attacks

Author	**Year**	**Key concepts/Methods**	**Challenges/Issues not resolved/mainly discussed**
Roderic Broadhurst *et al.*	2014	Cyber Criminology	Tracking criminal activities
KwakuKyei *et al.*	2013	Introduced anti-forensics	Total error rate calculation
Ibrahim Baggili and Frank Breitinger	2015	Challenges in CF	Lack of real data sources

ISSN: 2582-6433

Hemamali Ten-nakoon	2016	Profiling cyber Criminals inductive and Deductive profiling	Lack of usage of proper tools and techniques
Gupta *et al.*	2018	Survey on various techniques	Performance of snort in high speed networks
Youssef *et al.*	2018	Probabilistic and behavioural approach for likelihood determination in cloud	Superior then regular IDS in cloud
Wang *et al.*	2018	Data protection and provenance model for Cloud of Things	Improved k-anonymity, good robustness
Junaid *et al.*	2019	Droid MD scalable self-improvement tool	Detect malware, analyzes only the application code
Kao and Raylin	2019	Digital forensic framework based on ISO/IEC	Lab forensics, LEAs involvement
Gokila and Baggili	2018	Forensic Evidence Acquisition and analysis System	Works only for iPhone and homepad, if data is erased no extraction of data
Clarke *et al.*	2019	Forensic Acquisition and analysis System	Rely on Cloud Service Providers
Montsari *et al.*	2019	DFI and LEA combating cyber attacks	Combating cyber attacks
Roderic Broadhurst *et al.*	2019	Artificial Intelligence and Crime	Predictive policing using ML

2.7 Key concepts and approaches from literature

Sikroski (2012) emphasized about the tools and techniques used by professional ana-lysts, mainly applicable for windows domain. Clarke (2012) showed how vulnerable we are as a nation and as individuals to the looming web of cyber criminals. O'Connor (2012) showed the development offensive computing concepts.

Endicott (2006) has implemented a forensic corporate network as a separate disci-pline. Objective of Kim and Peter (2008), during a given time period, was to obtain such proof as remarkable and unusual

ISSN: 2582-6433

cycles of incidents, estimating how much criminal ac-tivity is evolving over time. Erbacher (2010) addressed the issues of authentication and mistake in digital systems and the gaps in digital evidence and data protection. The domains considered are civilian legal admissibility and military need. The domain was mobile devices and the aim was to develop software applications for mobile forensic since the existing software for the same thing is not often 100% forensically sound. Kyei (2013), Jafari (2015) and Yusoff (2011) presented and talked in detail about the digital forensic investigation models and best practices of them. Aim was to improve or enhance the whole investigation process. Walker (2009) conveyed about the lack of standards on retrieving the data, preserv-ing the evidence and the government's approach to digital records. Jingsha (2013) tried to examine the security breaches in whole steps of digital forensics considering the in-tegrity and non-misuse of evidence data retrieved from mobile phones. The domain used by Curran and Cassidy (2010) was clouds and social networks and the goal was to review research in cloud and social network contexts of systems, problems, solutions, techniques and tools in digital forensics.Baggili (2015) Discussed about the challenges faced in digital and cyber forensics.

Sikroski (2012) extracted network signature and host-based indicators and set up a simulated framework for detecting and solving ransomware techniques, including disassembly, anti-debugging, and anti-virtual machine technologies. And tools used were IDA Pro, OllyDbg and WinDbg. O'Connor (2012) uUsing python scripts on the popular websites of social media, evade current antivirus programs and investi-gate forensic artefacts. The key concept used by Kim and Peter (2009) was the NPEA which is a markov chain for learning, inference, optimizing for veracity of illegal ac-tivities. Erbacher (2010) described an implementation of SSH protocol and introduces anti-forensic methods while calculating total error rate. Kyei (2013), Jafari (2015) and Yusoff (2011) performed comparative studies including the hierarchical modelling and chronologically representing DF data. Lei Chen (2015) suggested the key concepts of adding the network audit nodes, survey local terminals and survey of the sub clouds.

Sikroski (2012) proposed an approach to implement a technique for unpacking mal-ware and get practical knowledge and use this new experience of Windows internals for malware analysis. O' Connor (2012) developed the python network traffic intercept and review framework.Endicott (2006) proposed a lifecycle methodology for opera-tionalizing organizational network forensic readiness with a proactive approach. Jafari proposed an investigation models with activities/ phases added with the existing mod-els. Li Chen (2015) proposed the dynamic forensics process model which they claim to have the features of high performance, activeness, automatic data migration, intelligent analysis and mass data extraction. Jingsha (2013) proposed specific methods per the particular situations to handle with the security breaches and to ensure the authenticity and non-misuse of the evidence of the infromation

ISSN: 2582-6433

retrieved. Kim and Peter (2009) pro-posed the modified Noise Page Elimination Algorithm (NPEA) to effectively prioritize the criminal activities.

2.8 Challenges faced by forensics investigators

In his work, the challenges faced by forensics investigators during criminal investiga-tions, Bennett (2011) outlines many issues; Proof is the target of a forensic investigator. Admission of evidence is the term used to obtain a judge's acceptance of evidence. Evidence admissibility includes legitimate investigation and robust adherence to the custody decision chain including proof collection, retention of evidence, analyzes and documentation. A professional data forensic expert provides a major role in criminal investigation by carrying out mobile phone forensic analysis of witnesses, evidence, victims or by monitoring network traffic in response to cyber safety accidents(Curran and Cassidy, 2010).

As Mislan (2011) depicts in his work, the aim is to ensure that the investigators use the correct methodology to support the criminal case and carry out forensic analy-sis in an effective way. Training of a forensic investigator in upholding guidelines on facts, ownership standards and legal problems is critical when it comes to collecting information from a mobile device. The forensics expert has to be up to date with cur-rent scientific tools and laws concerned with the admissibility of evidence and must be vigilant with the recent efforts made by offenders to jeopardize the forensics process.

In Li Chen's work (2015), Digital Forensics in cloud, cloud computing and storage, such as Amazon's EC2, S3 and Drop box provides users with huge data storing space and enormous computation power at reasonable costs. From forensic point of view, the organization of data from the cloud and social networks has common aspects: typically, data is not stored on a single server location, data storage and communication often spans over multiple jurisdiction regions, and user profiles and data may have strong social behavior related characteristics.

Realizing connection between offender patterns is one of the most essential accom-plishment of an expert analyst. Kim and Peter (2009) used forensic techniques to mea-sure the degree of criminal activity in a given period, using the markov chain. Noise Page Algorithm for removal (NPEA) is used to decrease an error in the prediction of probabilities.

Profiling is one of the many tools that can be applied in an investigation. Shinder (2010), who was a police officer and criminal justice instructor now turned to IT pro-fessional, says about crime and criminal profiling in her paper as 'knowing what types of people generally prctise specific types of criminal offenses can be very encouraging in spotting and prosecuting the culprit of a specific crime and says that the information can be very useful in securing our digital assets from cyber criminals'.

ISSN: 2582-6433

Moreover, pro-filing supports limiting the field of suspects and help omit some people from suspicion. Profilers use both inductive and deductive profiling.

The Cyber Forensics (CF)/Digital Forensics (DF) domain is historically known as an IA branch and deals with incident response (IR). The area based on IR, where infor-mation is only gathered following an incident. In other terms, only after the accident, the jurisdiction deals with automated proof obtainment, verification and analysis from programs. There are several issues outlined in various papers such as mentioned in O'Connor (2012), Rogers and Seigfreid (2004), Ruan *et al*., (2013) and Baggili (2015). Baggili *et al*., (2015) argued one issue that could be made available by the social media in strengthening the cyber forensic environment–the absence of actual data sources for future research. With the changing technology and the existence of many channels, such implementations are likely to leave behind digital forensic objects that may be implicit in an inquiry.

Crucial examples of digital evidence include multimedia forensic artefacts from so-cial media apps. For example, in Mutawa and Marrington (2012), mobile apps on Blackberries, iPhones and Androids were forensically examined by Facebook, Twit-ter and MySpace. The result was that it was possible to extract user and friend de-tails, photo URLs, time stamps, posted commentary, username and password (only for MySpace), uploaded photos, viewed pictures, posted tweets, tweets, and other forensic digital devices.

In the work, robust cybercrime analysis approach Tennakoon (2016), the author compares crimes in physical world and the digital world, brief about the criminal be-havior. Handling e-crimes using common means is a challenge because of the natural world in which they happen and of other parameters such as anonymity on the Web, virtualized/distributed storage, geographic and legal concerns etc. In order to treat the offences of the physical world, forensic psychologists make an informed judgment on the characteristics of offenders by using inductive or deductive reasoning. Crime prefer-ences for inductive behavior, and the demographic characteristics exhibited by offend-ers are established by analyzing statistical data. Deductive profiling requires a wide range of data, including physical records, documentation of a crime scene, victimol-ogy, suspect traits etc. Nevertheless, their applicability could be questioned in the cyber world. This may explain the very little consideration given by practitioners and schol-ars to the identification of cybercriminals where some find it "a promising, but untimely science"(Bednarz, 2004).

2.9 Existing challenges

The issues still existing in Clarke's (2012) work is the possibilities to lose already es-tablished findings when a new threat is encountered. The challenge as well as the issue not solved in the work of Endicot (2006) is record situation of due care during civil proceedings and the lack of

ISSN: 2582-6433

proactive approaches to digital forensics. Kim and Pe-ter (2009) has faced the issue of predicting the actions of consumers in terms of high modeling precision based on the hidden markov model and generalizing the approach in different situations. Erbacher (2010) found that software performance errors are not clearly defined, and there is still a need for studies to see how to measure empir-ically the error linked to software performance. Data provenance issues are still also not resolved. Sikroski (2012) encountered the major challenges of practicing and syn-thesizing the skills of Digital Forensic practitioners when the rules in the domain are constantly changing. Jafari (2015) encountered the issues of lack of experienced staff in investigation using the proposed model and the recording of step by step activities in the form of chain of custody was incomplete since the information about the legal investigators is not known. Bennett (2011) and Curran and Cassidy (2010) emphasize the challenges encountered during the investigation process and most instruments have not been fully developed. Civil litigations, electronic discovery and Intellectual prop-erty disputes are the issues not covered. Walker (2010) finds that alteration of digital records is still possible and there is the supreme lack and differences of laws across the countries when it comes to establishing the authenticity of digital records. Li Chen (2015) encountered the problem of how to reduce the acquisition time when retrieving the mass amount of data.

Erbacher (2010) speaks about problems related to the need to verify and error proof in emerging environments. We also address how digital evidence varies and as such contrasts even with the protection of privacy that is fundamental to traditional computer security. The theoretical groundwork for validation and error measurement in digital environments was provided by the author.

2.9.1 The challenges in profiling cyber criminals

O'Connor (2012) compares crimes in physical world and the digital world, brief about the criminal behaviour. We require the knowledge about the natural world, with that when creating cyber-criminal identities we ought to be able to understand not only the social, criminology and law problems, but also the technical aspects associated with the ' crime scene. ' O'Connor (2012) emphasizes an interdisciplinary approach should be followed while handling such an issue. There should be visible difference between cyber- crimes and non-cyber-crimes. Based on these one might seek to produce a profile that might be of some use to the law enforcement.

The author recommends a four stage method to build a cyber-criminal profile fo-cused on the use of existing deductive profiling technologies. This is the first move. It's a helpful initial step, also known as' victimology,' to examine what opportunities the individual or organization named for the offenders. This phase is almost affiliated with the motif and leads to the next step. Victimology may help to understand the origin of the incident. The' victimology,' the motive and the attributes

ISSN: 2582-6433

of the perpetrator, bring us to the third stage. Digital forensic evidence could be analyzed in the fourth stage of deductive cyber profiling.

The significance in digital forensics is obvious as it is the only way to track the suspect when there is no physical evidence. The proposed four-stage strategy is possibly a repetitive process because in the course of an investigation, new information about a suspect may emerge, the intent and the perpetrator together with forensic evidence. It is noteworthy also that the methods for inductive profiling can be used to produce better results by the above deductive approach.

2.9.2 Current research challenges

Consistent growth in the field of information technology and communication have brought challenges for those profiling cybercrimes. Due to the application of computer used to investigate computer-based crime has led to evolution of this new field called computer forensics.

The lack of actual data sources is a critical problem in various fields of computer science. Most agencies, vendors, suppliers (must) maintain privacy and security of their data. It can be remembered that machine learning requires a training package, and real cases in ciber forensics need a proper training set. We can not devise and test new methods and theories using fake, inaccurate and uncertain evidence. A question that is quite hard to solve has been posed in the papers of McClelland and Marturana and only a few established research projects have tried to learn from past real data to enhance the state of the domain or in the so-called push-button forensic method in which the data on a judicial picture are automatically analyzed by a device with little or no investigator intervening (Baggili, 2015; Endicott, 2006).

2.9.3 Typical scenario

To illustrate the fundamental concepts on which the proposed architecture is conceived, the following scenario is considered:

An attacker gets all the credentials of a victim's internet banking account - including his mobile phone or an illegally duplicate SIM. With the security measures currently in practice, such an attacker can have open access to the victim's bank account – because even the 2-factor authentication using mobile One Time Password (OTP) will be cir-cumvented by the attacker. However, the proposed architecture can detect, log and even alert the authorities in runtime when this happens. This is how it is proposed to achieve: The proposed system is installed in the server where the banking application server runs. The banking server application does not have any dependency or relation with the proposed software framework. For simplicity, we are assuming that the server is not part of a distributed system. To maintain anonymity, such an attacker will almost always try to login to the bank account from many

ISSN: 2582-6433

public proxies available in Internet. We can get an exhaustive database of such proxy servers from many government authorities' private sources. Have such a database ready for the forensic model matching component (fraud detection) in the architecture. The kernel network subsystem hook detects that a TCP connection is initiated to a socket belonging to the banking server process and notifies the model matching component that a connection attempt is made to the banking server process. The model matching component notes that the connection is made from one of the proxies in its database. The username and password information are encrypted end to end from the attacker's host to the server process and hence our framework cannot access such details, but we do have a kernel process subsystem hook which can monitor file access and network access of each process in the server. The security model matching component tells this process subsystem hook to watch out for imminent local or network database access from the banking server process.

In the cases such as, the scope of the digital crime is not limited or only if the OS kernel has access to all events; a trigger is made by the model matching component as soon as these happens in a configurable time window (some hundreds of milliseconds). The logs generated by the banking server process and all other relevant logs for that time is tagged and archived for further analysis. This way, the evidence of a possible crime is collected in real time, without the burden of a huge data-set and low rate of false positives. More than that, none of the existing server applications are to be modified.

Operating system is the most powerful software, the brain of the computer system, so how can it assist in cyber forensics? From a conventional criminal forensics' per-spective, it is very well equivalent to the most intelligent and knowledgeable person performing an autopsy. Being the master software running on a digital computing plat-form, the Operating System software is the one having the ultimate knowledge and control over any event that is happening in the system. In other words, any software running as a part of Operating Systems has the capability to monitor all events from a system-wide perspective. At the same time, popular general-purpose Operating Sys-tems has minimal security mechanisms enforced by default because it will affect the overall system experience by the end user (e.g. the infamous User Authentication Mod-ule – UAM – in Windows) and event logging from a cyber forensic perspective is not even a secondary priority of popular Operating Systems.

Our work reviews the existing forensic models, defines cybercrime, focuses on chal-lenges and move on to proposing an enhancement of cyber forensic approach which includes an operating system assisted profiling and evidence preserving using virtual-ized secure logging scheme which can be applied to majority of technology platforms. The target of this work is to find out and classify if are there any cyber security /digital forensic models in place for general purpose Operating Systems at

ISSN: 2582-6433

present. If there are, in what way it can further be made more effective? If not, propose a practical approach and model for it. For profiling crimes and criminals, access to digital evidence data is most important. Since real life evidence data for analysis of cyber-crimes are difficult to come by, - a problem that is practically very difficult to take care of - mechanisms that can enable sophisticated logging and tracing in existing systems is identified as a very important area where much research is not done. Nance *et al*., (2009) detailed and Tennakoon (2016) and Chou (2008) mentioned the access to evidence data has severe limitations. It is difficult to get access to the run-time state of the systems, and thus there can be important information that is not part of the analysis, such as network con-nections, encryption keys, decrypted data, process lists, and modified code running in memory. According to recent surveys, it is noted that, more and more data is stored and managed in distributed hosts (mostly hosted in clouds using virtualized hosts). Hence the monitoring and logging of events that are related to cyber security in a distributed environment has become more complex and important. Chou (2018) emphasizes on a new methodology for securing the logs using virtualization tools and comparing it with kernel module approach.

The evidence data acquisition from a computer system can be accomplished in two distinct methods: One is using logs generated by the applications like web server, FTP server etc. and the other method is kernel mode analysis and logging system that functions as a part of operating system and thus having exclusive access to all events and data in the system. The second approach is significantly different from the first because, in operating system kernel, the data and events can be analyzed from the perspective of the whole system – whereas in the first case the information in the logs are severely lim-ited by the scope of the concerned application. However, the second approach involves additional complexity of kernel mode implementation which is significantly more ad-vanced and less documented than application level implementations.

The problem further extends to how the event logs generated by the Operating Sys-tem can be used for forensics analysis. In other words, how the above described security mechanisms and models can be further extended so that the evidences are made more useful in criminal profiling, another related domain in digital forensics. Obviously, this work needs access to design and development details of a typical general-purpose Operating System. Considering the Open Source development model which gives us complete access to all such information, Linux is selected as platform for all practical purposes for this work. Chou (2018) briefly mentioned the research area of evidence data acquisition system in kernel mode. Here, we put forth a proposal which accom-plishes the crime and criminal profiling, using the data collected from a sophisticated operating system level evidence acquisition scheme thus achieving integrity and cor-rectness of the forensic analysis results from distributed and non-distributed systems.

ISSN: 2582-6433

2.10 Summary

After conducting extensive literature review, it is understood that lack of effective mech-anisms in place to collect the data, lack of effective frameworks to classify the data, the volume of evidence data and the time taken to undertake an investigation based upon the data are key limiting factors for future advancements in this domain. Further exploring techniques and technologies for potentially reducing these issues resulted in focusing upon approaches such as criminal profiling and better methods of tracing and logging events in the system under observation. To achieve that we have introduced an Oper-ating System assisted Forensics approach, which involves the following three different analysis techniques for evidence collection.

1. Evidence acquisition by analyzing the Process Execution Context – Temporal data
2. Evidence acquisition by analyzing the Process Execution Context – Application domain data.
3. Evidence acquisition by the Process Execution Context – External Parameters

There are no released works that analyse digital evidence collected from distributed system using OS kernel while designing this forensic analysis methodology. So, this work fills a gap in the field of digital forensics. The proposed techniques will be ex-plained in the following chapters in detail.

CHAPTER 3
EVIDENCE ACQUISITION TECHNIQUE USING PROCESS EXECUTION CONTEXT ANALYSIS

1.1 Introduction

Digital forensics is a major area where researches are still being conducted on a large-scale basis as the growth of computer-assisted crimes are innumerous and the fine-tuned approaches to investigate cybercrimes are still in its infancy. The related publications were collected from previously published literature on the problems that occur in the market, from the escalation of the volume of information to different platforms and applications in the technology sector. We have carried out a comprehensive research and have concluded that the various technology and their usage mechanisms are the major constraining variables, given the absence of successful data acquisition approaches and the absence of effective frameworks to process large amounts of data.

Evidence data acquisition is a key area and there is a lack of effective and stan-dardized methods

ISSN: 2582-6433

and tools. The data volume and the time required to investigate are main limiting factors in conducting digital forensic investigation. Criminal profiling and automation approaches on which extensive research is not done so far. There is the need for a reliable security system which can perform real time attack detection for the distributed systems. Currently available tools can do post-mortem analysis of digital crime using logfiles from different application in a server. The features are limited and depends on logging methods and the third-party mechanisms.

Solution is to develop a security suite that is independent of installed applications and monitor the system in OS level. Real time analysis of data will use the process execution context (PEC). Linux is selected for this which is most widely used OS in high performance servers. VVirtually any common resource for digital forensics relies on proof usability. The creation of information records is complicated once a computer offence is committed. Digital evidence collection can be performed satisfactorily by a security enhanced operating system kernel. The target of this work is evidence collec-tion and application of digital forensic modelling on the collected evidence that further leads to crime and criminal profiling.

Forensic experts have sevaral methods to retrieve the data that is present or restore removed, locked, or disabled information from the file on the computer system. So, the key question is, what is the most effective way to collect the evidence of a digital crime. Usually digital evidences are the event logs generated by application software as well as operating system software. In modern Operating Systems, even a privileged application process will be running in a restricted virtual environment and Operating System will make sure that an application has minimal knowledge of any other applica-tion process or, in general, about the host system. So, naturally, evidence data as event logs generated by such application processes lacks the overall system perspective. The data discovered is important in forensic analysis and in solving various computer crimes through proper log or record preservation which leads to profiling. The primary purpose of this review and study is to emphasize the challenges faced in digital forensics such as lack of fine-tuned data acquisition methods and the deficiency of frameworks to process larger volumes of data to examine. The reasons for these challenges are the diversity of technology platforms and the growth of technology horizontally and vertically; while the problem seeks it horizon, the solution does not grow accordingly.

1.2 Crime pattern matching based on process execution context

Once a digital crime is committed, the availability and collection of evidence data are becoming major challenges. This is because of large amount of data to analyse as well as complex data flow patterns in contemporary software systems. Compared to tradi-tional methods of evidence collection

ISSN: 2582-6433

which usually rely upon analysis of application and system logs, a security enhanced operating system kernel can make the evidence collection more authentic and comprehensive. We have proposed such a security so-lution, Crime Pattern Matching based on Process Execution Contexts (CPM-PEC) that includes a process monitoring mechanism that is implemented in OS kernel. The kernel mode process monitors report potential security sensitive events to an application counterpart that analyses the events to find matches with potential crime patterns –which are pre-defined sequences of security sensitive events. This combination of kernel mode and user mode components makes sure that every process in the system is monitored from its creation to termination for various events in its lifetime and data flow between processes are also monitored. For evaluation purposes, the proposed solution is imple-mented and integrated to Linux Security Module (LSM). It is observed that less than 2% overhead is incurred by the addition of this proposed solution in Linux kernel. The future work shall focus on enhancing the digital forensic investigation process by dis-tributed pattern matching to prevent the crime before the damage is widespread.

Operating system manages all resources in a computing system. So, operating sys-tem is the software that can assist digital forensics the most. Being in control of the digital computing system, Operating System has the knowledge over any event that is happening in the system. When a digital crime is committed, the scope of a digital crime may be spread across many different processes (and even hardware) and only the operating system kernel has access to all the processes and events in the system. Because of these reasons, a kernel-oriented approach can co-relate all the events in the system and make a coherent security decision. From a conventional criminal forensics' perspective, it is equivalent to the most intelligent and knowledgeable person in forensic science assisting an autopsy.

There are many forensic software suites available that can monitor security aspects of local and distributed computing environments. This includes commercial software suites like Nagios, Splunk, Paessler PRTG and Solar Winds. Tatara (2009) and Kim and Peter (2008) mentioned these software suites either make use of standard monitor-ing protocols (e.g. Simple Network Management Protocol (SNMP)) or otherwise make use of their proprietary application agent software to perform the monitoring of various measurable parameters of the computing system - like network bandwidth usage, appli-cation availability, application logs analysis etc. Since these monitoring suites are using application software components (agents) to do the monitoring, they are not able to do a system-wide coordinated event monitoring and analysis completely that an OS (or an OS level software extension) is inherently able to perform. Also, none of these mon-itoring software suites currently provide a configurable mechanism that can logically map the monitored events to a known digital crime pattern.

ISSN: 2582-6433

We proposed and implemented a technique which makes use of the algorithm we have designed for the purpose of evidence acquisition. We show how the events can be created and added and their execution context are being analysed to find a match between predefined crime patterns. Our solution is applicable for any OS that follows classical Unix architecture. The technology to hook into the OS is different for each OS Application Programming Interface (API)s - but the fundamental architecture of the proposed solution holds good even for OS like Windows. For demonstration and evaluation purposes of the proposed solution, Linux Operating System is used. At the time of report preparation this, there were no released work that analyzed digital evidence collected from distributed systems using the OS, while designing this Forensic analytics methodology-a vacuum filled by our research.

1.2.1 Crime pattern matching using process execution contexts modules

Securing confidential information using traditional means such as usernames and pass-words or network firewalls along with cryptography are not effective to prevent the data leakage because an authorized program to access and decrypt confidential data can propagate that information to other unauthorized programs without any further checks. To overcome this limitation of traditional security systems, two major techniques exists for implementing digital security mechanisms in software systems. They are:

1. Information Flow Control (IFC)
2. Provenance of Digital Assets

IFC, when introduced in a framework, the flow of information from the software to the other can be controlled and the flow can be prevented if the protocol is not necessary. (Thomas and Dieter, 2014). A protection mark for private (high) or public (low) is assigned for the standard model, where the system guarantees that high data does not spill into low contexts. The IFC can be enforced statically in the program source code by labelling each variable with types such as high and low and the compiler makes sure that no assignment is made from a variable labelled high to another variable that is labelled low (Mahmoud *et al*., 2015). IFC can also be implemented dynamically but the runtime cost is observed to be prohibitively high (Chen, 2013 and Stefan *et al*., 2018). IFC is a more effective mechanism for information security compared to traditional access control. However, once a breach is found, IFC terminates the violating programs and whole system is stopped which is not feasible in real life because availability of programs is of utmost importance.

Compared to IFC methods, Provenance method concerns about various information: origin of data, who manipulated data and how etc. Obviously, provenance, concerns more about valuable evidence information and is the focus of this work. Provenance can be done in an application specific or a

ISSN: 2582-6433

work-flow specific way – but these methods severely limits the effectiveness of the method from a digital-forensic point of view. Pohly *et al*., (2012), reasoned that apprehending interaction between processes and files were not enough to captivate provenance within an OS. To interpret the complexity of an OS and the complex interactions taking place, it is necessary to captivate the data interchanges on all system calls. Hi-Fi acquires system-wide provenance data from kernel level, using the Linux Security Module solution, and consequently is able to monitor all interactions between kernel objects.

The proposed security solution in this work, Crime Pattern Matching using Process Execution Contexts Technique (CPM-PEC), tries to combine the basic principles of the above described IFC approach and Provenance approach into a unified solution in a typical Operating System kernel. As explained earlier, the target of this work is forensic evidence collection and application of pattern matching on the collected evidence in real-time. Similar works (Bates *et al*., 2016) and Arati. *et al*., (2017) such as "Trustworthy Whole-System Provenance for the Linux Kernel" states that it is very hard to obtain complete provenance of the system just by monitoring a subset of events by an application. It is because certain incidents outside the device may occur that impact its output and such instances do not appear in records of provenance. Bates concludes that without the aid of provenance-aware applications working hand in hand with kernel support, it is hard to obtain 100% system provenance. This work is an attempt to design such a system where whole system monitoring is done in kernel by various kernel modules and crime pattern matching of the provenance data collected by those kernel modules is done by the user mode application modules.

The proposed solution has both kernel mode and user mode components, by virtue of which, From its creation to its termination, every process on the system is monitored. (Arati *et al*., 2017). The details of a process and the monitored activities of it are collectively named as the Execution Context of that process. Each of such monitored action and associated data is defined as an Event in the lifetime of the process. Thus, every process Execution Context has a sequence of Events associated with it which is called its Event History. A crime pattern is a pre-defined ordered list of Events that can potentially lead to a security threat. Whenever a process activity results in an Event that changes its Execution Context, its Event History is analysed using a crime pattern matching algorithm. The result of such analysis is categorized, ranked and then logged. Thus, the proposed solution is also a proactive digital evidence collection mechanism because potential security evidence data can be identified and logged before the crime takes place. For evaluation purposes, crime patterns are defined as simple sequences of security sensitive events. E.g. repeated attempt to open security sensitive files (e.g. the password file in Linux) is treated as a potential crime pattern.

In this work, digital crime pattern definition and matching are done based upon the following

ISSN: 2582-6433

postulates: In a computing environment under the scope of our analysis, data is always manipulated either in the context of a process (or any schedulable entity like a thread). A process in a computing environment is always executing under the context of either a user or the system. In other words, in a computing environment, data is always associated with a process and the process is always associated with a user (or it is a system process). In this work, these two contexts together called as "Execution Context" (EC) of a process. Since we are focusing on the events and dataflow in the computing environment, the Execution Environment of processes is the principal entity on which further discussion is based. Under the CPM-PEC solution, every event and every dataflow across process boundaries are always associated to an Execution Con-texts of one or more process. The access control rules enforced on the user by the OS is assumed to be in place. The CPM-PEC solution does not consider or include those rules. This is because digital crimes are often made regardless of the access controls in place (Broadhurst *et al*., 2014). The perpetrators either find vulnerabilities in cur-rent access restrictions (administrative mistakes) or use process or program exposures to access the presented tool (software bugs).

Our solution is applicable for any OS that follows classical Unix architecture as mentioned by Watson (2010, 2007). The technology to hook into the OS is different for each OS APIs - but the fundamental architecture of the proposed solution holds good even for OS like Windows. For demonstration and evaluation purposes of the proposed solution, Linux Operating System is used.

1.2.2 The crime pattern matching algorithm

The CPM algorithm makes use of crime patterns expressed as sequence of events which are derived from common digital crimes. Each of these patterns has parameters which are readily available in the EC and event history associated with it. This includes (but not limited to) the list of known server processes in the system, the database of safe IP addresses which can act as valid source and destinations of network connections, the list of blacklisted Internet Protocol (IP) addresses which are generally proxy IP addresses and attack sites, the network ports to which connections are made from outside, the network ports to which connections are made from the host, the checksum of known malicious binaries and so on. A sample pattern definition is as given below in Fig. 3.1.

ISSN: 2582-6433

```
[pattern]
name=cloud_local_client;
rule_id=1001;
type=file_monitor;
process=dropbox;
monitor=open,read,write,execute,delete;
directory=$home/*;
rank=1;
dependency=nil;
```

Fig. 3.1 A sample pattern definition

This pattern specifically monitors "dropbox" client process, which is a client of the Dropbox cloud storage service. As specified in the pattern definition, whenever the Dropbox client tries to access any file under the home directory of the users of the system, a pattern match happens.

The algorithm shown in Fig. 3.2 makes use of the unique process ID assigned by the OS to each of existing processes to distinguish them from one another. The process ID of each new process created in the system itself is noted by the user mode application to initialize a new EC and associated event list.

An event in kernel is always labelled with the of the process that caused the event. This ID is used by the algorithm to find the associated Execution Context (EC) of the event and process it. Once a new event is added to event history, the pattern matching algorithm is applied, and a result score is obtained.

ISSN: 2582-6433

```
Require: Event_k                                   ▷ The event from kernel module
 1: Compute rank for Event_k
 2: EC_k ← 0                                       ▷ EC corresponding to this event
 3: for EC_i ∈ ECList do
 4:     if EC_i.processId = Event_k.processId then
 5:         EC_k ← EC_i                           ▷ EC found
 6:     end if
 7: end for
 8: if EC_k = 0 then
 9:     Create and add new EC
10: end if
11:                                                ▷ Add event to event history list of
EC_k
12: if EC_k.history.length ≤ MaxHistoryLength then
13:     Create and add new EC
14: else
15:     Remove oldest Event
16:     Create and add new Event
17: end if
18: for Event_i ∈ EventHistory do
19:     Matching Event_i with pattern              ▷ A pattern is a predefined event
sequences
20:     if MatchScore ≥ Threshold then
21:         Matching pattern found
22:     else
23:         No matching pattern
24:     end if
25: end for
```

Fig. 3.2 Crime pattern matching algorithm

As illustrated in Fig. 3.3, the kernel mode components of the CPM-PEC solution work with other kernel subsystems to keep track of various events in the system from every process creation to its termination. This information is fed as inputs to a user mode component that implements the CPM-PEC algorithm. The sets of events that are related to a known crime pattern are identified and that is the output of this user mode component. All software components illustrated in Fig. 3.3 are described in detail below.

ISSN: 2582-6433

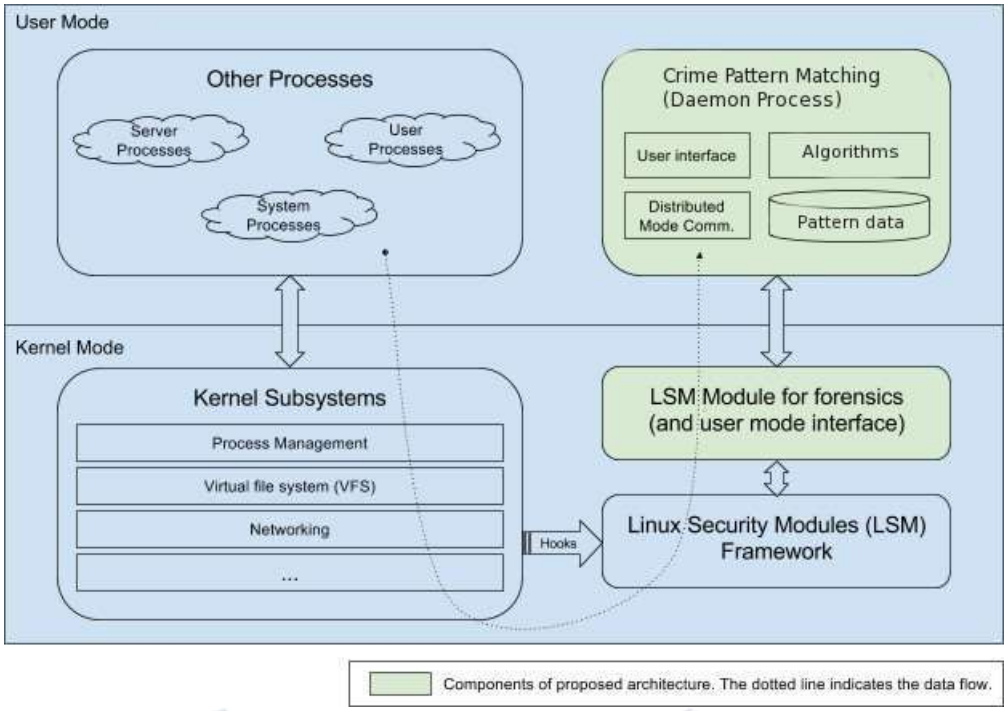

Fig. 3.3 Crime pattern matching using process execution contexts

1.2.3 Kernel mode components

Linux kernel comprises of the following major subsystems that are relevant to the pro-posed work (Smalley *et al*., 2001a; 2001b; 2002), (Morris *et al*., 2002) and (Greg, 2002).

Process management subsystem: This module has a duty to ensure that all operations are carried out. The Scheduler, which manages the programming or execution of each operation, is the main part of the process management subsystem.

Memory management subsystem: This module stores the system's memory and co-ordinates any process' storage order. It helps to map the cycle digitally to physically. It's available in /Linux/mm.

Virtual file system: APIs such as **open**, **read**, and **write**, etc. are included in this sub-system regardless of file system type. User does not have to think about forms of filesystems. Virtual File system (VFS) is responsible for transmitting the user's request to various file systems for which user application increases the request.

Networking subsystem: It administers the Linux IP network or, say, the network sub-system handles everything related to the network.

1.2.4 LSM module for forensics

ISSN: 2582-6433

This is one of the two core components of the CPM-PEC solution. This module acts as a kernel mode counterpart of the Crime Pattern Matching Daemon (CPMD) process which is a user mode component of the solution (Miroslaw, 2002; Xiaolan, 2002). It makes use of the LSM framework to monitor all relevant creation and access of kernel objects (files, network interfaces, network data packets, Inter Process Communication (IPC)s) by other processes in the system. These events are reported to the CPMD with all relevant details using a simple **ioctl** system call interface.

1.2.5 User mode components

User mode components of the system are depicted in particular in the succeeding sub-divisions.

1.2.5.1 Crime Pattern Matching Daemon (CPMD)

This is the most important component in the CPM-PEC solution. This module runs as a daemon process. It provides the configuration interface using which patterns pertaining to a specific cyber-crime can be defined as an ordered list of events. It also implements the crime pattern matching algorithm discussed earlier. It uses the kernel mode counter-part to facilitate the required fine-grained access to all objects maintained by the kernel in the system. The crime pattern matching mechanism is illustrated in Fig. 3.4.

1.2.5.2 Input to CPM-PEC module

As shown in Fig. 3.4, the output from the kernel subsystem (LSM Module for forensics) is given as input to the pattern matching module. Depending on the nature of the action of the process that made the LSM module capture its details, the input will contain all relevant information of the particular action which will include the process identifier, time, file / socket descriptor (and path) involved in the event, result of the operation (e.g. file open succeeded or failed) etc.

ISSN: 2582-6433

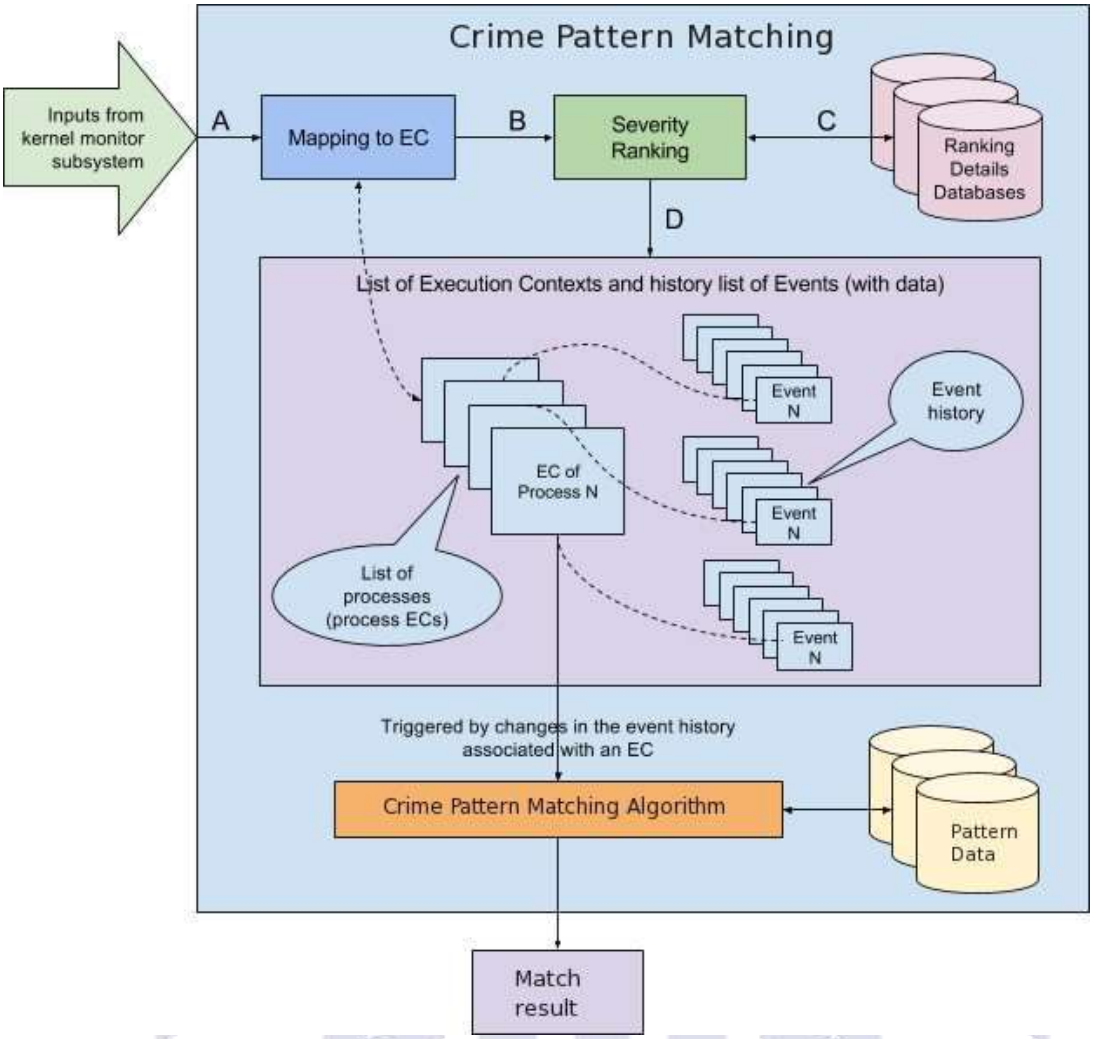

Fig. 3.4 Crime pattern matching mechanism

1.2.5.3 Mapping to EC

Firstly, the EC of the process that triggered the event will be identified. If the process is not in the list of ECs already present, a new EC will be created.

1.2.5.4 Severity ranking

There will be predefined severity score (on a scale of 0-1) for a particular event. Each of the process classes (Castro, 2013; Gianluca, 2002) (known system processes, user processes, server processes etc.) will also have a severity score (again, on a scale of 0-1). Combining both of these scores, the overall severity of the particular event will be calculated.

1.2.5.5 List of ECs and event history

The core part of this module is the list of ECs and the list of events associated with each EC (called "event history" of that EC). Inputs from kernel subsystem contain fun-damental information

ISSN: 2582-6433

about the EC of the process that caused it and other details of the particular event. This information is used to:

1. Create and maintain the list of EC (if the input is a process creation event or from a new process that is not yet there in the list).
2. Create the event history for each EC (if the event is from an already existing EC in the list of ECs).

It can be noted that the data inputs are also considered as events and will be added to event history associated with the EC that it belongs to. The severity ranking makes use of the ranking details database to assign a rank of severity to each input. It takes inputs from associated EC also to arrive at the final ranking score. The functionality of this sub-module is best understood with an example: A network connection attempt from internet to a banking application process is an input event. The IP address of the source computer is also available with the input from the kernel subsystem. If this IP address belongs to known blacklisted IP address range in the threat ranking database, then severity rating will be very high.

Figure 3.5 and Fig. 3.6 show pictorial representations of process tree in a typical desktop system.

ISSN: 2582-6433

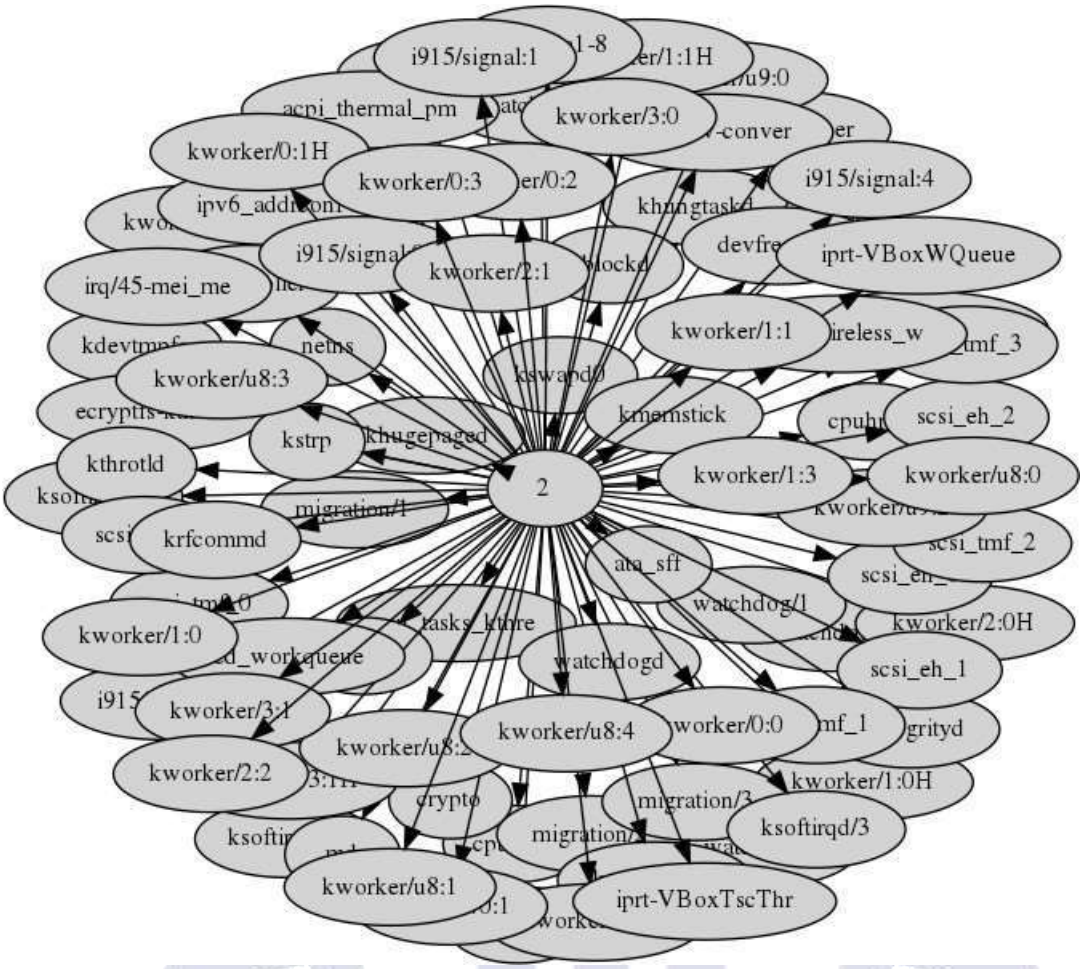

Fig. 3.5 Pictorial representation of process list in a desktop system - 1

ISSN: 2582-6433

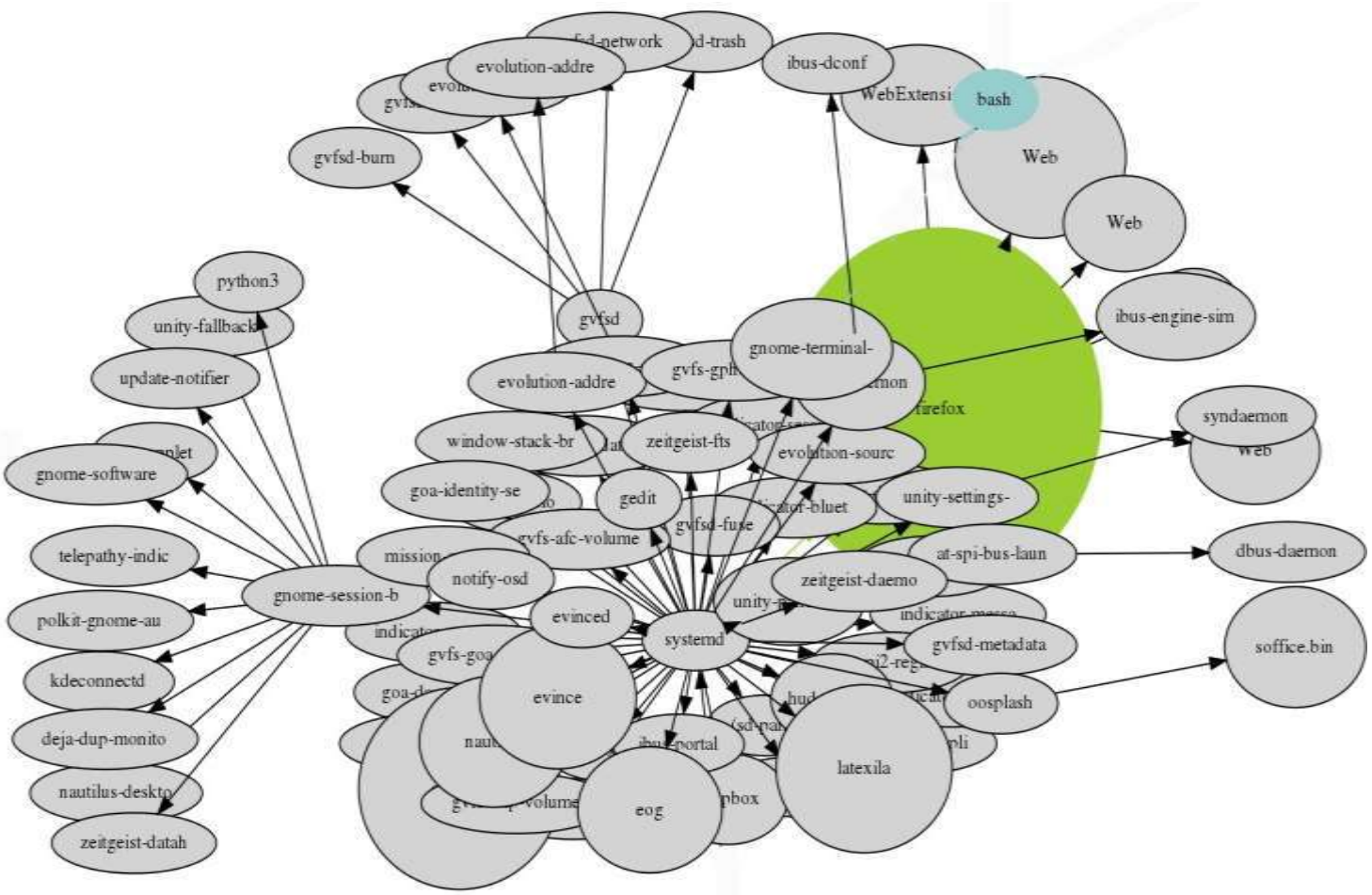

Fig. 3.6 Pictorial representation of process list in a desktop system - 2

1.3 Results and discussion

From a digital forensic perspective, we have proposed and implemented a proactive solution that can identify a crime as and when it is committed and collect relevant evidence data on the fly. The pattern matching mechanism in the proposed solution is easily customizable for specific data flow requirements across different processes in the host system. It also bring down the overhead of irrelevant data and keeps only the information that is related to the specified crime patterns. An example of a reported match for the pattern definition discussed earlier is as shown below in Fig. 3.7.

 ISSN: 2582-6433

```
Pattern match: name=cloud_local_client, id=1001,
type=file_monitor
timestamp= 1517761351 (04/Feb/2018 4:22pm UTC)
process=dropbox, process id: 12876, user: testuser1
file_path=/home/testuser1/MyDropbox/test.txt
file_action=open [flags: read | write] [success]
```

Fig. 3.7 A sample pattern matching report

The kernel system monitor and process control have, as can be seen, hooked and transferred the file creation as an event to the user mode component of the proposed solution that can easily incorporate to match crime patterns related to possible data breaches in cloud client applications.

The important aspect of the crime pattern matching system is the event history kept for each execution context. The time-window of this history will be configurable and will be limited only by the available system resources (most importantly, available RAM). This history window, along with the information contained therein provides some unique possibilities for evidence collection. E.g. a connection attempt from a blacklisted IP may try to get a malicious binary file into the system and later delete it to clean the crime scene. With the event history mechanism, as soon as the rules detect the connection from blacklisted IP address or the known checksum of a malicious binary file created, the details of connection attempt as well as the binary data can be tagged, logged and archived for later analysis. The selection of crime patterns to be used with the above described crime pattern matching algorithm and the possibilities of defining new crime patterns using the same mechanism are two major targets of the work. The given Fig. 3.8 below illustrates a sample rule and event.

```
[rule]
Name=local_application;
rule_id=1004;
type=file_monitor;
process=*;
monitor=open,read,write,execute,delete;
directory=$home/*;
rank=1;
dependency=nil;
```

```
Event: Rule match: name=local_application, id=1004,
type=file_monitor
timestamp= 1517761351 (04/Feb/2018 4:22pm UTC)
process=gedit, process id: 12876, user: testuser1
file_path=/home/testuser1/docs/test.txt
file_action=open [flags: read | write] [success]
```

Fig. 3.8 Pattern matching - sample rule and event

ISSN: 2582-6433

1.3.1 Performance analysis tools

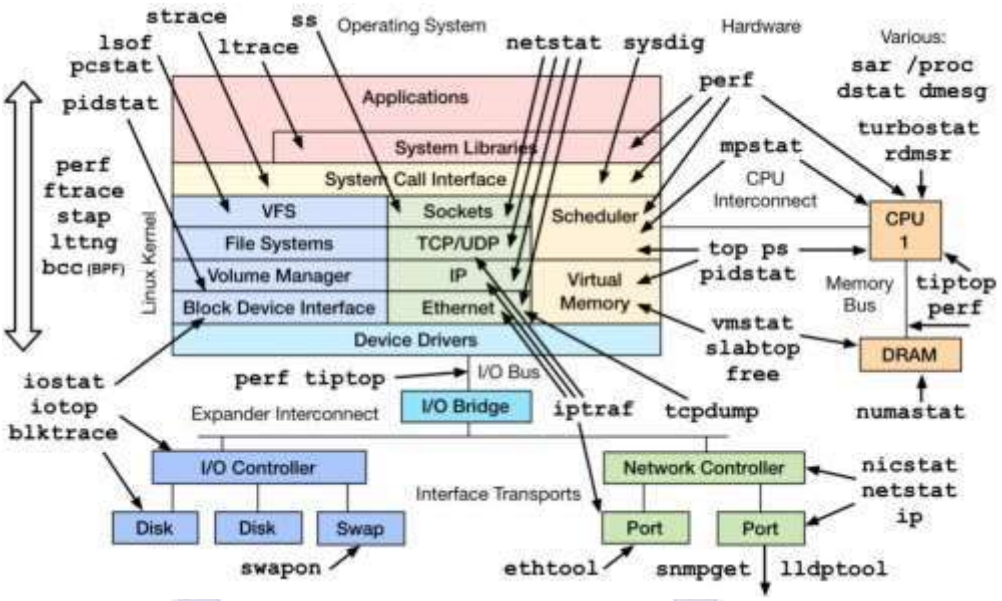

Fig. 3.9 Performance logging and tracing tools in Linux

Figure 3.9 shows popular logging and tracing tools for common hardware, Linux kernel and applications. Some of these mechanisms needs special kernel modules (e.g. lttng) while others have built in support in Linux kernel (e.g. kprobe). In this work **kprobe**, **ftrace** and **perf** tools are used for performance analysis.

1.3.2 Overall performance analysis

The performance critical components in the CPM-PEC solution system are:

1. The LSM based event monitor kernel module
2. The crime pattern matching algorithm in user mode daemon process

Of these, the performance of the former - LSM based event monitor kernel module

- is most critical. Since this module is intercepting almost every kernel control path, any performance drop in those control paths will have an impact on all processes in the system and thus on the whole system performance. On the other hand, the per-formance of the pattern matching daemon will affect only in some low-ranking events being dropped and the real-time nature of the mapping will be lagged - none are critical such as the whole system performance. So, for the time being, the performance analysis is only done for the LSM based kernel module. The evaluation is conducted based on the following criteria to determine the performance of the solution and its

ISSN: 2582-6433

impact on Linux kernels:

1. Effect of introducing the CPM-PEC solution on performance on Linux kernel control paths (system call handler code paths in kernel, where LSM has hooks for monitoring).
2. Comparison of the performance drop due to LSM module and other well-known LSM based security modules (such as SELinux).

We performed the evaluation on an Intel Core i7 Intel PC, running Linux 4.10 (Ubuntu 16.04 LTS). Using standard development tools (gcc etc.), a simple C appli-cation is developed that continuously tries to open and write a line to the /etc/passwd file is developed as a dummy attack process. The system performance monitoring is done using LMBench (standard Linux tool for kernel performance measurement). Ta-ble 3.1 below shows the rate of increase in time for file operations in Linux kernel

3.16 as measured by LMbench (all units are in microseconds) and the corresponding performance graph is shown in Fig. 3.10.

Performance impact on common process execution related operations when tested with and without the kernel LSM module is as given in Table 3.2. All performance measurement is done using **lttng** and **perf** tools, shown in Fig. 3.11. Times are in microseconds (smaller is better).

Table 3.1 Comparison of impact on performance of file system operations

Operation	**Normal**	**CPM-PEC Solution**	**SELinux**
Stat	1.892	2.114	2.521
Open and close	3.101	3.313	4.292
Read	0.310	0.328	0.335
Write	0.290	0.306	0.312

ISSN: 2582-6433

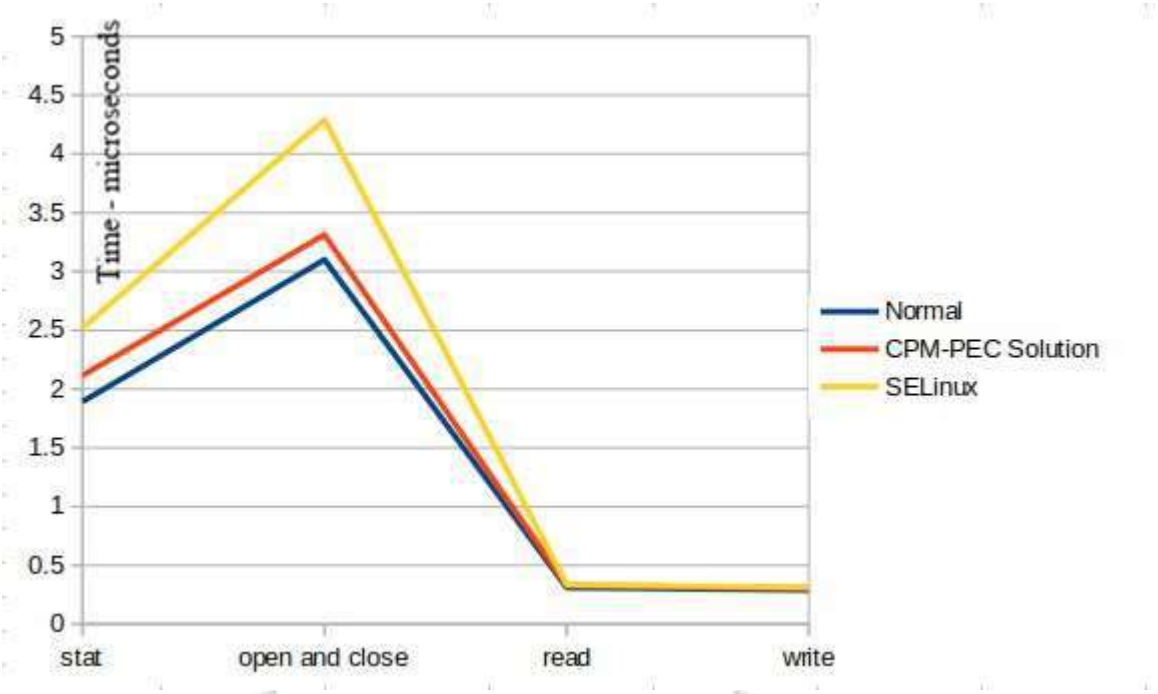

Fig. 3.10 Performance impact of PEC on file system operations

Figure 3.12 shows the performance impact on system calls in server type system. As seen in the observed data, the performance of the CPM-PEC solution is comparable with other LSM based security solutions and less than 2% overhead is observed for file system and process related operations.

Table 3.2 Performance impact on common process execution

Operation	**4.10 kernel without proposed LSM module**	**4.10 kernel with proposed LSM module**	**Percentage overhead because of proposed LSM module**
Stat	5.34	5.45	2.06
Popen/Close	6.95	7.23	4.03
Select TCP	42	45	7.14
Signal Sending	1.28	1.30	1.56
Signal Handling	4.30	4.31	0.23
Fork	190	195	2.63
Exec	720	719	-0.14

ISSN: 2582-6433

Shell Process	3540	3611	2.01

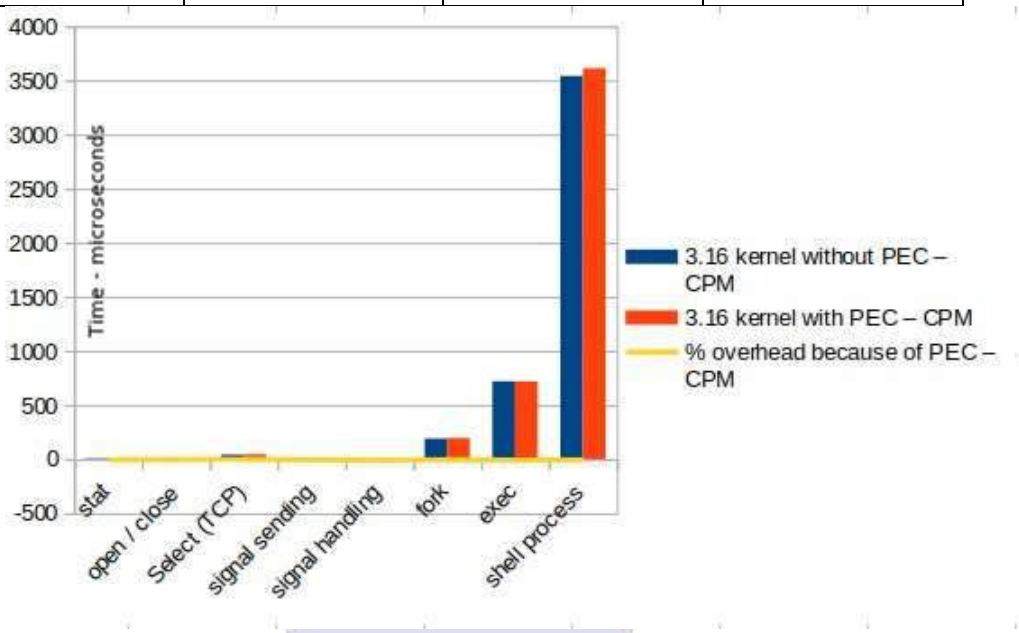

Fig. 3.11 Performance impact of PEC on common system calls on a desktop system

Table 3.3 Performance impact on system calls in a server type system

System Call	**Time (us) without PEC**	**Time (us) With PEC**	**Count**
open	22.063	24.410	1141
poll	964.456	964.464	5086
read	53.037	53.935	2904
futex	47.939	48.118	2543
sendto	7.515	8.509	1512
recvmsg	9.815	10.737	16261
close	0.905	1.684	959
mmap	6.97	7.167	889
write	6.517	7.014	777
newfstat	1.114	1.300	647
writev	8.29	8.588	563
newstat	2.953	3.100	527
access	6.378	6.769	517
madvise	19.04	19.799	495
munmap	14.185	14.832	307

ISSN: 2582-6433

mprotect	11.107	11.997	228
fcntl	1.155	1.673	208
fstatfs	0.596	1.452	158
getpid	1.148	2.132	143
readlink	3.421	4.196	122
unlink	5.672	6.595	86
ftruncate	4.236	5.062	73
fallocate	119.26	119.981	72
dup	1.392	2.057	72
sendmsg	7.376	7.789	64
clone	161.178	161.588	34
recvfrom	3.693	4.637	23
lseek	1.986	2.099	15
getuid	0.9	1.160	12
geteuid	0.798	1.249	12
wait4	398.688	399.031	12
getegid	0.603	1.549	11
getgid	0.701	0.792	10
socketpair	14.195	14.227	10
pipe	8.592	8.652	8
dup2	2.234	2.451	7
ioctl	3.105	3.411	7
socket	8.421	8.923	7
brk	3.177	3.362	5
connect	14.379	15.200	5
statfs	6.527	6.620	4
symlink	18.083	18.669	4
shmget	9.892	10.537	4
execve	3184.755	3185.707	3
sysinfo	18.471	18.769	3
setsockopt	2.396	2.782	2
mkdir	43.568	44.367	2

ISSN: 2582-6433

kill	3.376	4.002	2
getppid	2.402	2.894	1
getpgrp	2.234	3.154	1
creat	5.969	6.534	1

ISSN: 2582-6433

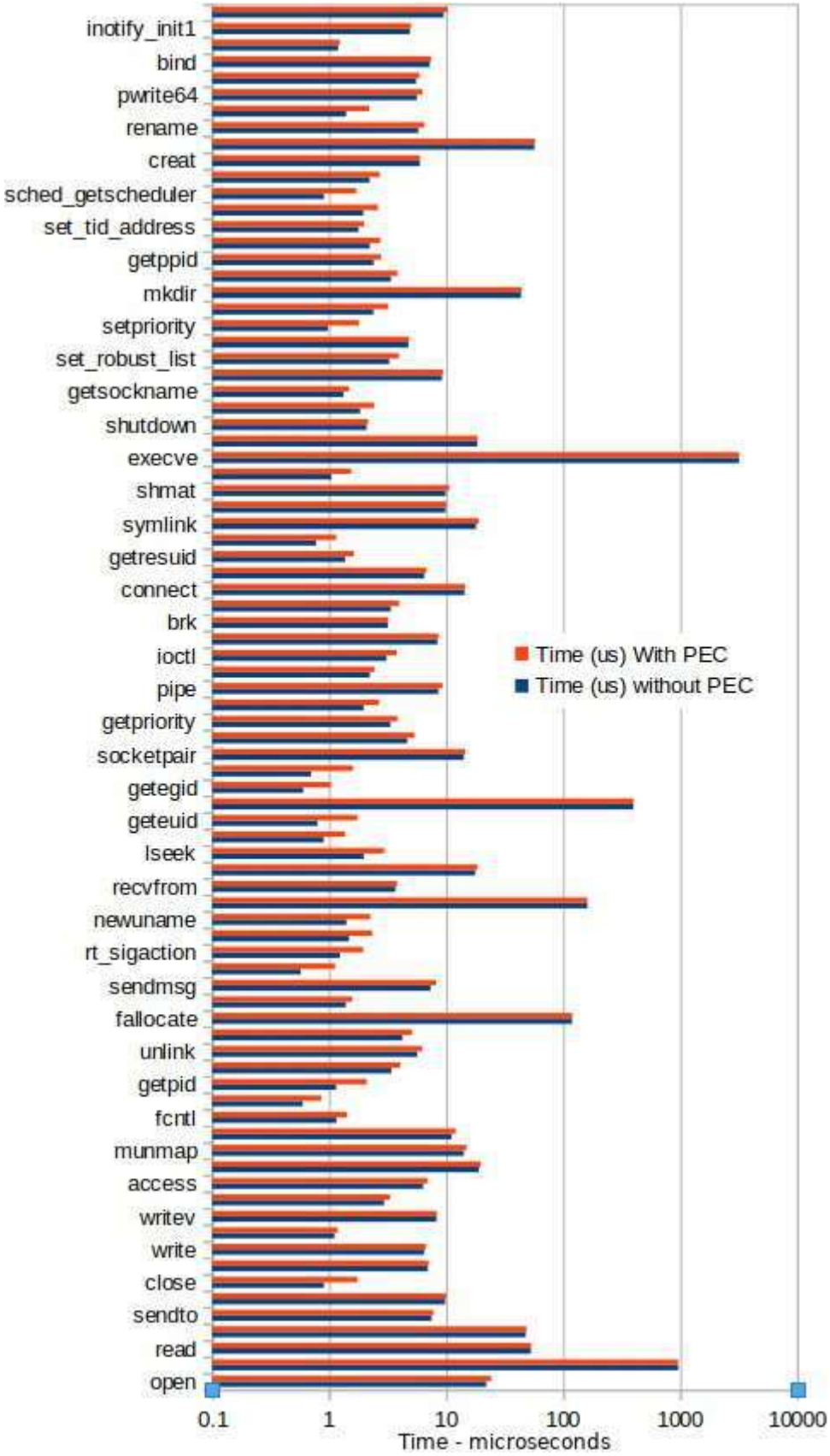

Fig. 3.12 Performance impact of PEC on system calls in server type system

ISSN: 2582-6433

1.4 Summary

The implementation of this CPM-PEC solution is trying to bridge the gap between ex-isting security tools and more effective evidence collection using known digital crime patterns. At present, other solutions are virtually non-existent that combine the crime patterns to existing security tools – especially making use of operating system level monitoring that provides complete access to virtually all events in the system or any-thing which make use of the execution contexts of the processes. This work aims on completed the following milestones during this research. Classification of threats and crimes that comes under the scope of this solution is identified first. Further, cybercrime patterns are analysed to define them as ordered list of events. The detected real-life events are identified. Carrying out the detection of identified events using correspond-ing Linux kernel system entities that are related to LSM solution are studied in detail. The study of LSM solution also included a detailed analysis of SELinux which is one of the most popular LSM modules currently. As a future work, integration of other forensic tools (once evidence data is collected) is also planned.

The focal point of future work will be on improving the digital forensic investigation process, which involves research into more efficient evidence acquisition techniques which uses crime-pattern matching algorithms and tools that should be ultimately built in as part of system or kernel and in some cases even partially or fully implemented in hardware, and to extend the solution to prevent the crime before it is or about to be committed. We foresee the probability of applying neural networks and genetic algorithms for crime pattern matching.

CHAPTER 4
EVIDENCE ACQUISITION IN ADVANCED RESOURCE MANAGEMENT SYSTEM FOR CLOUD

4.1 Introduction to distributed environment

The system we discussed so far has the boundaries set solely by the host on which it is implemented. The decision-making algorithm can be easily extended to be a node in a computing cluster, grid or even a cloud. Here in this chapter, we are considering cloud environment for such an analysis. We will analyze a proposed technology and frame-work to monitor and manage resources in a cloud environment which can be readily extended to include the previously explained forensic features.

Cloud computing is often heterogeneous because the underlying large-scale stor-age system is not only affordable and efficient to support all servers, network devices and power supplies in one and one configured configuration., e.g. workflow extensive computing might need standard and cheap

ISSN: 2582-6433

hardware; scientific computing might need specific hardware other than Central Processing Unit (CPU) like General Processing Unit (GPU) or Application Specific Integrated Circuit (ASIC).

There are kinds of resources in the large-scale computing infrastructure need to be managed, CPU load, network bandwidth, disk quota, and even type of operating systems. To provide better quality of service, resources are provisioned to the users or applications, via load balancing mechanism, high availability mechanism and security and authority mechanism. To maximize cloud utilization, the capacity of application requirements shall be calculated so that minimal cloud computing infrastructure devices shall be procured and maintained. Given access to the cloud computing infrastructure, applications shall allocate proper resources to perform the computation with time cost and infrastructure cost minimized.

To implement flexible and fine-grained resource monitoring and management in a cloud deployment scenario, such an Advanced Resource Management System (ARMS) must have the following characteristics.

Firstly, it shall be able to provide a well-defined method for the cloud operator and his clients to properly communicate with each other and arrive at a set of Service Level Agreements in terms of resource usage.

The heterogeneous nature of physical resources (in physical hosts) shall be manage-able by a resource management paradigm which can be used to define the conceptual entity which can be used uniformly by the resource allocation algorithm. This paradigm must be made simple enough so that the cloud operator and clients can use the underly-ing concept in their resource negotiations.

The system shall be distributed across the cloud so that it must run in each of the host system where virtual machines are run by one or more hypervisors. This component integrates itself with host OS as well as the hypervisor (and hence the Virtual Machine (VM)s and virtual networks present in the host), providing complete control over the host system and hosted VMs. The distributed system shall be able to communicate together in the cloud whenever a resource management decision is taken which has global impact to the cloud operation.

A heterogeneous world of multiple production processes and diverse managers must be able to run for the resource management system. In popular server class operating systems, the specification will therefore be versatile and can support all popular hyper-visors. Such specifications were satisfied in this earlier work in the field of cloud by designing and developing these ARMS for clouds.

The fine-grained control and monitoring capabilities over resource usage such as bandwidth and memory based upon user defined rules and conditions demands some components that are a part of the host operating system. Without direct interaction of the host OS as well as with the hypervisor, this kind of control is not possible in a virtual hosting environment. This kind of a component referred to

ISSN: 2582-6433

as ARMS, as shown in Fig.

4.1 is the key part of the proposed solution.

To provide the complete access control over the cloud system, it is required to have control over the physical network of hosts within the cloud (the real LAN of hosts) as well as over the virtual networks managed by the hypervisors residing in the hosts. In

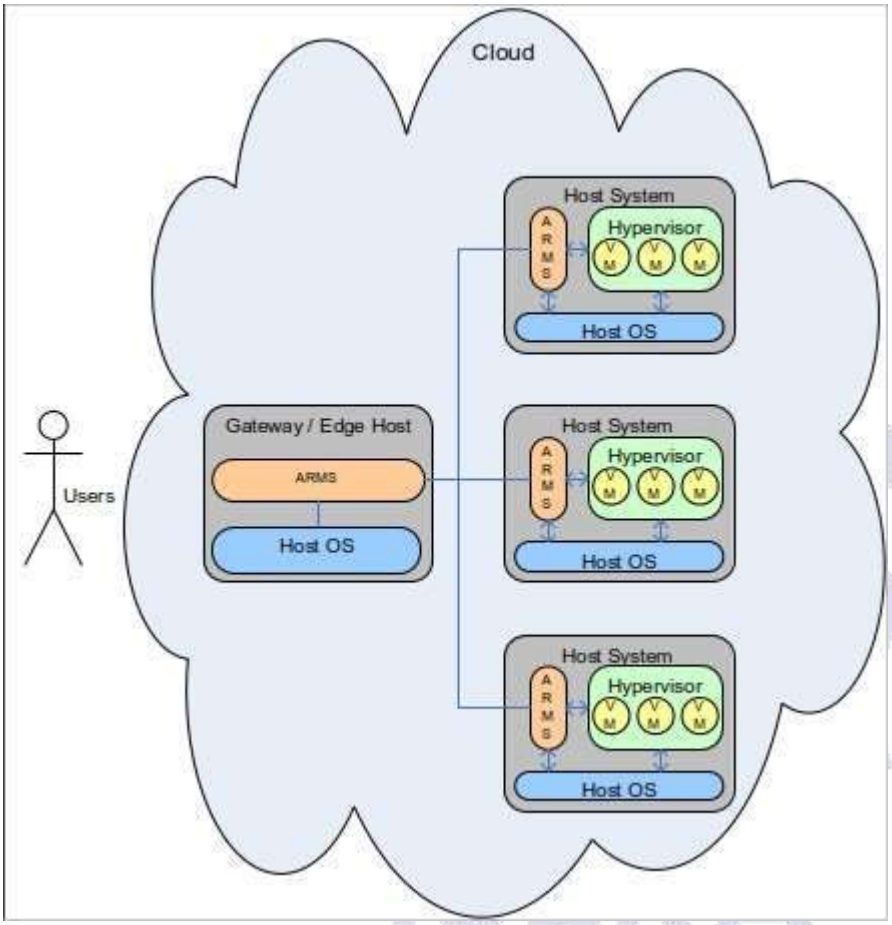

Fig. 4.1 Advanced resource management system (ARMS) architecture

order to achieve this, ARMS is designed as a distributed system, running on all physical hosts in the cloud setup. This distributed nature of ARMS is also illustrated in Fig. 4.1 Thus, ARMS has access control and resource management over the whole cloud in a physical and virtual level by distributing itself over the host network of the cloud. Also, being present on the edge host device (gateway), ARMS can also act as a highly efficient firewall, which has reaches to the whole host network with its distributed architecture.

As shown in Fig. 4.2, the ARMS solution comprises of the following modules:

4.1.1 The host module

The major component in this architecture is the host OS module as shown in Fig. 4.2. The rule

ISSN: 2582-6433

engine sub-module and resource control sub-module of the host OS module must implement the guidelines and policies. For configuring the host OS module, the user interface and the communications module are used to set the rules and policies

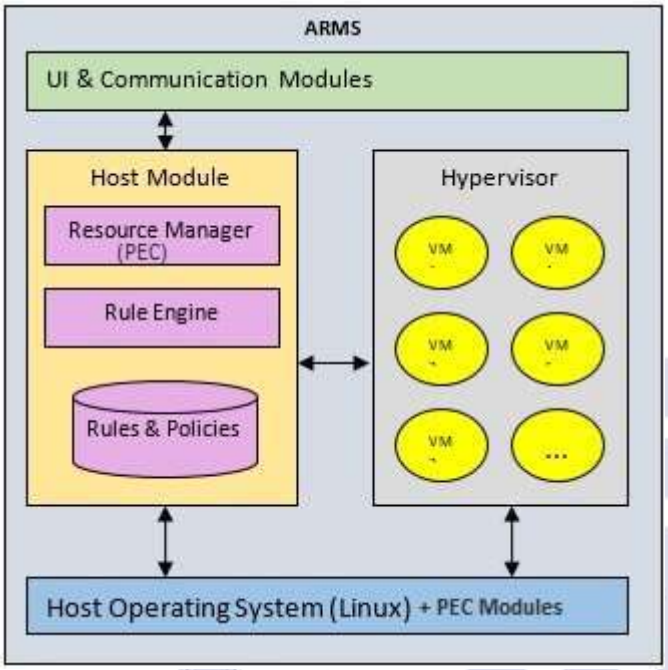

Fig. 4.2 ARMS functional modules

which in turn communicate with hypervisor and host OS to execute them. As shown in Fig. 4.1, ARMS is a distributed system of similar modules. This hierarchical design of the rules and policies on resource management provides Weapons freedom in every cloud computing market implementation.

The interface between the host operating system module and the hypervisor is based on the hypervisor APIs. These APIs include control and configuration of VMs and vir-tual networks, host networking, host memory management, file management, security features and so on. The OS module interface with the host OS would be as defined by the host operating system APIs. As shown in Fig. 4.2, the following are the major sub-modules in the host module:

4.1.1.1 Rule engine

This module preserves and controls the rules in the order in question and offers a swift response. It is very critical that the logic is structured and that its answer is very rapid. You have to retain the rule set and request other modules for the search APIs. The rule engine has the following features:

1. Set and extend the command line control configuration and GUI configuration rules

ISSN: 2582-6433

according to user needs.

2. Fast response time
3. Easy to use – the most critical aspect of the program is as a standard user interface and it should be easy to use by admin.

It is to be noted that, the proper derivation and implementation of rules (and policies) in terms of cloud user requirements and cloud operator requirements are crucial to the success of a resource management system like ARMS.

4.1.1.2 Resource manager

The resource manager uses the host OS and hypervisor provided API to control and monitor the resource usage in the host system. Using the hypervisor provided API, the resource manager monitors and manages the virtual machines and virtual networks in a host system. Using the host OS API, it manages the resources in the host system. Using the communication module, the resources in the entire cloud is monitored and policies are enforced.

4.1.1.3 Rule/Policy database

There is considerable consistency in the rules / policies of the programs introduced. The law storage is to exist on or spread over various virtual machines on the same host computer. The platform to be used is of importance to this work as the following technologies had to be used by the industry:

1. The architectural configuration of the servers.
2. The software you want to use is open access ideally.
3. Support of different host OSs.
4. Performance.

4.1.1.4 UI and communication module

This module implements the user interface of ARMS system. It also handles the com-munication over cloud network between different hosts running ARMS. Any ARMs node can be used as a starting point of resource search in the ARMS managed network. Thus, the communication module provides the capability of working as the server and client in ARMS network communication. When a node initiates the resource manage-ment related query, it acts as a client and all other ARMS nodes acts as servers.

4.1.2 The host operating system

APIs for use by applications and for kernel modules (e.g. system drivers) are supported in the host

ISSN: 2582-6433

Shell. This API is used for managing management of resources such as network traffic, system memory, access to data etc. Please notice that the Virtualization Software (VMs) hypervisors inside the host OS do use this API. The fact that ARMS host OS module has control over the host OS resources, just like the hypervisors do, provides ARMS the extra control over host resources that is otherwise not manageable using hypervisors alone.

4.1.3 Hypervisor

Two types of hypervisors are basically there: the first is a host OS that gives the tools to build and manage virtual machines. We have stock control frameworks with APIs. Popular hypervisors for use in a machine such as ' Virtualbox ' are strong examples of this type of hypervisor. The latter is called "Bare-metal" hypervisors which are standalone systems with a well integrated host OS and is usually aHost OS is available from the manufacturer as a bundled hardware unit. An example of this is VMware ESX. These are rather expensive.

Also the first type of hypervisors are considered in this work for simplicity. A Web-based API package for the end user is typically usable for the widely used hyper-visors. Many hypervisors can manage the VMs more seamlessly via a device level API package. Each of these can be used for further monitoring of fine seed over the VMs operating within it. E.g. creating new VMs, managing the VM configuration, creating and managing virtual networks and so on. The APIs may be used even by modules of third parties such as ARMS.

4.1.3.1 Virtual machines

That is the center of cloud network technology.VMs are independent guest machines, and are usually grouped into different virtual networks within the hypervisor. This method of virtual networking provides the hypervisor with a full network environment.

To build such a computer network, computer routers and switches are supported by the hypervisor. Hypervisor includes the network access API.

This method of virtual networking provides the hypervisor with a full network en-vironment. To build such a computer network, computer routers and switches are sup-ported by the hypervisor. Hypervisor includes the network access API. As described above ARMS is designed to manage such a network of virtual networks in terms of access control and resource management.

This is particularly effective in a cloud environment as a proactive forensic approach if it can be integrated with the cloud resource provisioning system as shown in ARMS where resource usage allocation and monitoring are implemented using agent software running on each physical host in the cloud. If the proposed system is integrated with the agent module of a system such as ARMS, it

ISSN: 2582-6433

has the potential to become a viable solution as a proactive digital forensic framework for any distributed system.

4.2 Design of ARMS

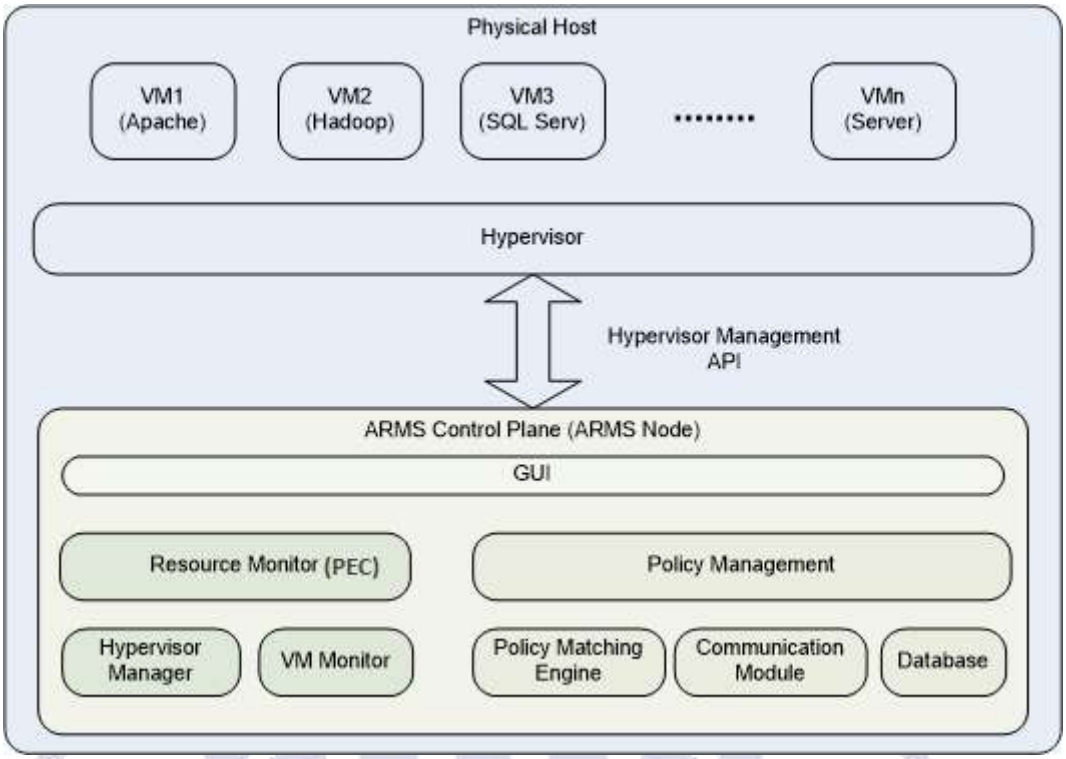

Fig. 4.3 ARMS system design block diagram

Figure 4.3 illustrates the design of ARMS. The ARMS framework contains two main technical components: a resource monitor and a module for policy manage-ment. The operator will customize resource management policies based on perfor-mance, costs, and so on, as the policy manager deems necessary. When VM assignment and location requests arrive, the policy manager samples the resources control details and feeds it with the matching engine policies. The resulting method addresses cloud operators ' conflicts of interest and creates a match between VMs and servers.

The matching mechanism between resource requirements and resource allocation policies is based on the stable economic matching system that elegantly achieves all design goals.Specifically, The expectations definition is used to authorize stakeholders (cloud operator and cloud clients) to express various policies of simple lists organized to satisfy the generality and expressiveness criteria. Instead of optimality, consistency serves as the key approach to resolve stakeholder conflicts of interest in order

ISSN: 2582-6433

to satisfy the necessity of equity.

The novelty of the stable matching mechanism designed for the project is in strict cloud heterogeneity management. In fact, here, Classical stable theory of matching can not be applied directly. Every VM has a different ”size,” which corresponds to its CPU, power, and memory needs. However, the literature on economics suggests that agent has standardized sizes. Heterogeneity of scale makes the problem even worse, as in this situation even the concept of equilibrium is vague. We devise a general stable matching problem that is consistent with the heterogeneity of the framework in our model by a new concept called ”Unit VM”, to effectively find and prove convergence and optimum performance, to generate algorithms that fit the new definition stably.

It is to be noted that ARMS is a distributed system. Thus the ARMS module il-lustrated in Fig. 4.1 is present in all physical nodes of the cloud that are managed by ARMS. So, the resource allocation request is handled by each of the distributed ARMS node modules. For this purpose, a simple, yet efficient communication module is developed. The physical cloud network details (hostnames, IP addresses) etc. and the policies and resource management information is stored in a database. In order to create and maintain this database as per the designed database schema, a database management module is present in the system.

4.3 The classical stable matching algorithm

The stable matching (SM) algorithm is also known as Stable Marriage algorithm. Though the algorithm was first presented by Gale and Shapley (1962), applications in a variety of current reality conditions include algorithms used to find the solutions using stable matching. Most notably, for the principle of the stable allocations, and the analysis of business management, Lloyd S. Shapley and Alvin E. Roth were honored in 2012 with the Sveriges Riksbank Award in Economic Sciences in Honor of the Nobel Prize in Economics.

4.3.1 Mathematical analysis of classical SM design

SM is about having two sets of elements in a secure matching number. For each element, a set of preferences is defined. A match is an association between one group’s members and the others. When it is not the case, a match is considered stable that both:

1. One of the elements A of the first set favors another of the element B of the second set, which A matches already
2. B prefers A over the element already corresponding to B

In other words, if there is no alternate pair (A, B) where both A and B are indepen-dently well off

ISSN: 2582-6433

than they are with the element they are currently coupled, a match is secure. The stable matching problem is popularly described as:

Provided *n* males and *n* females each with a separate rank between the first and the second sex, marriage the males and the females in order of precedence with each other. such that there are no two persons of other gender who would both would like have each other than their current spouse. If there are no such persons, all the pairings are "stable". In mathematical terms SM can be conveyed as follows: An occurrence of I of SM is made up of both men and women in the same amount-say *n*. Every individual has a list of priorities that all members of the other sex correctly order. If a man prefers *m* *w*1to*w*2,then *w*1 > *mw*2will convey it. For female tastes, the same notation is used. A play with M of I is a disjoint pair of I for men and women. In this chapter we are only looking at the optimal matches, that is, matches of *n* scale. When a *m* pair is combined with *m* male and *m* female, the *m* pair is represented in $m(m) = w$ and $m(w) = m$. A *m* male and a *w* girl, we say, is a *m* blocking pair,(or in other terms, (*m, w*) blocks M) if the three constraints given in the equations Eqn. 4.1, 4.2 and 4.3 are satisfied:

$$M(m) \models w \tag{4.1}$$

$$w > m.M(m) \tag{4.2}$$

$$m > w.M(w) \tag{4.3}$$

M is not stable if there is a blocking duo for M, and stable in other ways. Gale and Shapley suggested the Gale-Shapley Algorithm, which has complexity $O(n^2)$, finds a comfortable fit at all times. It is also good proof that there is at least one consistent match in any individual event. The SM algorithm can be expressed as shown in Algo-rithm 1.

Algorithm 1 Classical stable matching algorithm

1: **for** $m = 1$ to M **do**
2: $pair[m] = NULL$
3: **end for**
4: **for** $w = 1$ to W **do**
5: $pair[w] = NULL$
6: **end for**
7: **while** TRUE **do**

 ISSN: 2582-6433

8: **if** there remains no male *m* such that $pair[m] = NULL$ **then**
9: return;
10: **end if**
11: take such a male *m* randomly;
12: *w* = the first female on m^rs choices to whom *m* hasn't proposed yet;
13: **if** $pair[w] == NULL$ **then**
14: $pair[w] = m; pair[m] = w;$
15: **else if** *w* likes *m* more than *partner*[*w*] **then**
16: $pair[pair[w]] = NULL;\ pair[w] = m;\ pair[m] = w;$
17: **else**
18: ; // no action means rejecting *m*;
19: **end if**
20: **end while**

The SM framework has the advantage of its overall viability. The generic preference notion covers many diversified and complicated deliberations that network administra-tors and cloud appliances may have. The traditional delayed consenting algorithm can be used in a centralized way with minimum difficulty. The execution speed of SM is comparable to that of an optimization perspective, in spite of its use of ordered infor-mation.

In the context of ARMS, the role of men is analogous to the policy groups and unit VM definitions set for each physical host by the operator. The role of woman is anal-ogous to the customer whose requirements are expressed in terms of an Service Level Agreement (SLA). This scenario does not match 100% with classical definition of SM where each entity involved in one side of a matching has a preference list which consists of a strictly ordered list of all entities on the other side. Another issue with the delayed consenting algorithm is that it can only produce two radical results, one of which is VM optimal and another is server optimal (Irving and Scott, 2008). It is considered sta-ble overlapping polarization. The network operator looks for a "equal" match in most cases that does not skew either end as the network machine feature level, in which the VMs run speeds and the resource use of the data center are far more controlled. Effi-cient implementations are therefore important to answer such pragmatic requirements. Thus, we need to design a variant of SM that suits ARMS. This is elaborated in the next section.

4.3.2 Design of egalitarian stable matching algorithm variant for ARMS

The stable matching algorithm has many variants (Irving and Scott, 2008). Note that the classical

ISSN: 2582-6433

SM algorithm get to a stable matching in time $O(n^2)$. This algorithm basi-cally is a sequence of proposals between men and women, finding a secure relationship with the ultimate property that makes every male his best probable partner in any secure match. The match is then called the masculine-optimum competitive match. Of exam-ple, the resulting stable pairing of men and women is better for women if we switch positions of men and women. Unfortunately, owing to the existence of stable matches each woman gets the worst possible mate at the same time. The male-optimal stable pairing is the women-pesimal stable match. Therefore, it is very common to seek to find a match that is not just ”fair” but also ”fair.”

The standard of stable matches is improved by several steps, but here we consider the one which is known as egalitarian solution. For find a successful competitive match, there are some potential fairness requirements. One specific choice is to maximize the total number of partners of all agents in the match, as initially defined for single match problems (Iwama and Miyazaki, 2008). It means maximizing the overall ”happiness” of the dedicated agents. Since however, a server ranks itself over individual VMs can not suffice to decide their preferences over combinations because many VM can be reached by our scenario server.

4.3.3 Mathematical modelling of egalitarian SM algorithm

Given a range of $\mu(s)$ VMs matched with a stable collection of μ servers, we consider the $dS(\mu(s)$ of s for the dissatisfaction score to be the average of the $\mu(s)$ ranks of */ps* preferences,as in (Iwama and Miyazaki, 2008). It is denoted using Eqn. 4.4.

$$DS(\mu(s)) = \sum_{v \in \mu(s)} Rs(v) \quad (4.4)$$

Where $Rs(v)$ shows the s level of v. VM v's dissatisfaction value is just $DS(\mu(v)$ $= Rv(\mu(v))$. The disappointment value of the successful μ match is then the sum of all the participating agents. It is denoted in Eqn. 4.5.

$$DS(\mu) = \sum_{v \in V} DS(\mu(v)) + \sum_{s \in S} DS(\mu(s)) \quad (4.5)$$

Iwama and Miyazaki (2008) stated the following results for servers. They also relate symmetrically to VMs. Thus, we can make the following propositions and theorems:

Proposition 1: For all stable matches, VMs, are assigned the same server $s \in S$.

Therefore, in all stable matches, when $ns < qs$, s has the same range of VMs.

Proposition 2: Suppose that μ and $\mu*$ are various stable match allocated to the server s by

ISSN: 2582-6433

various VM collections. So one suit say μ, if $(v, s) and \in \mu$, $s \in \mu * \mu, Rs[v] < rs(v*)$. There is one fitting, say μ. A useful corollary of Proposition 2 is that when a server in different stable matches selects same collection of VMs, the lesser chosen VMs have to be special for both of them.

Corollary 1: Assume the stable matches of μ and $\mu*$ to the same question, say, (VxS, PV, PS). Or $s \in S$, $\mu(s) = \mu*(s)$, or $min(\mu(s)) \vDash min(\mu*(s))$, is available on each $s \in S$ computer. The most famous VM among those matched s in μ, namely
$min(\mu(s))$. Please note that it is simple for VMs because a VM is connected to the same or separate server in separate matchings. We can prove the following theorem for both propositions and Corollary 1 which essentially eradicates the first case of complexity.

Theorem: Suppose μ and $\mu*(s)$ are unlike stable matches allocated by a $s \in S$ server of opposite VM sets. The $DS(\mu(s)) \vDash DS(\mu*(s))$ is inserted in the following style.

Proof: Proposition 1 allows s in μ and $\mu*$ to be equal to the same number of VMs. We should assume that $Rs(min(\mu(s))) < rs(min(\mu*(s))$. Every VM from the prefer-ential list ps below $Rs(min(\mu(s)))$ would be equal to a maximum number of VMs for
s (among which it is the least favored VM).

Place the first VM in ps below $Rs(min(\mu(s))$ which is a secure match with a mini-mal VM s, say $\mu**$. iBy proposition 2 any VM in $\mu**\mu$ must be under any VM $v \in \mu$ in ps. In proposition 2 any VM v is a substitute for any $v \in \mu$, above v for pd. A combi-nation of v^r with v results in an rise in s frustration such that $DS(\mu(s)) < DS(\mu**(s)$. The discontent value rises.

Therefore, each server in various secure matches has a separate cumulative rank-ing number of its VM paired. And by comparing the dissatisfaction ratings, we can unambiguously compare two sets of consistent tests. The resource allocation using Egalitarian SM Algorithm is shown in Fig. 4.4.

ISSN: 2582-6433

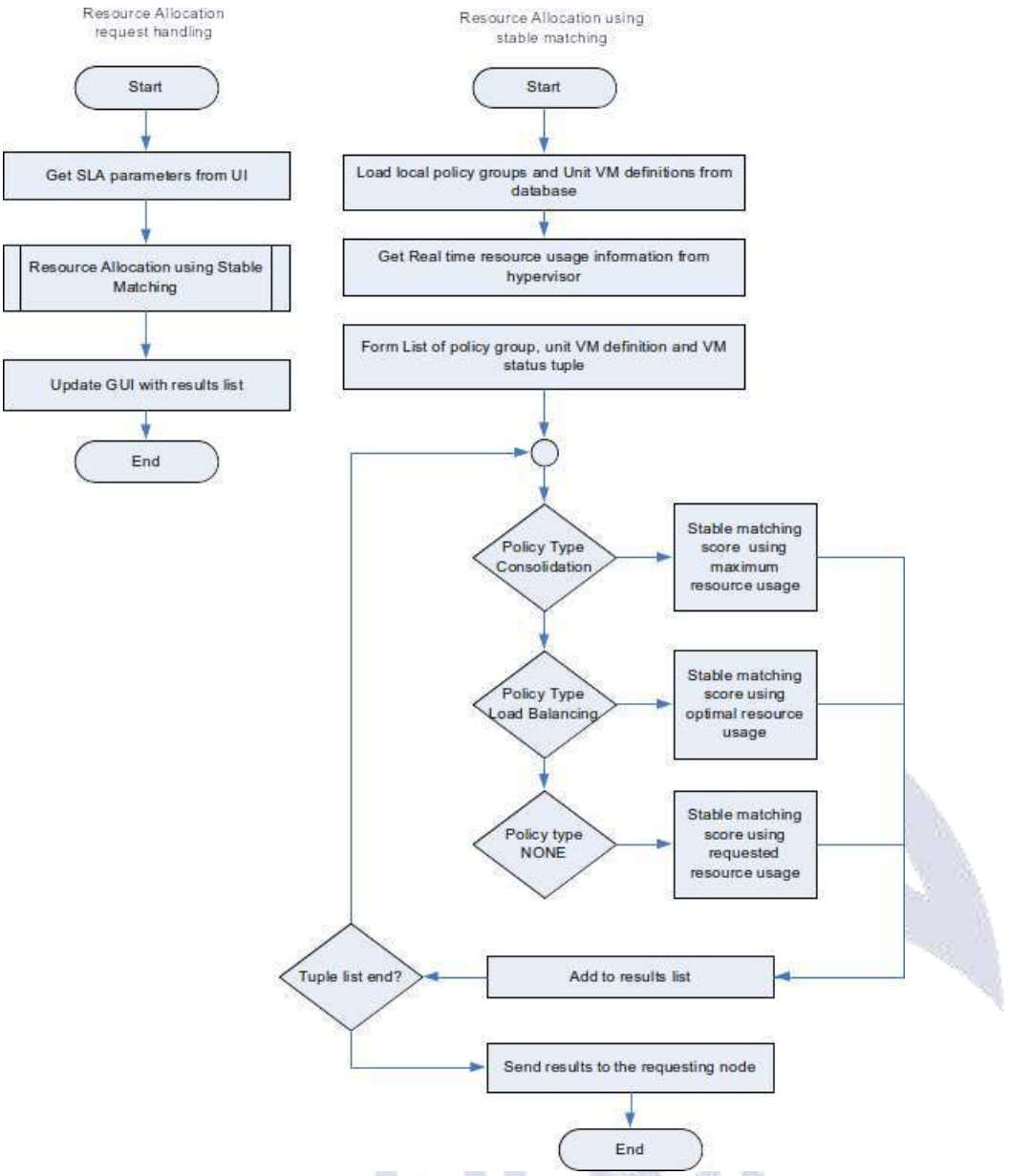

Fig. 4.4 Resource allocation using egalitarian SM algorithm

4.4 Results and discussion

The sample event logs from ARMS system is shown in Fig. 4.5. From the logs, we can see an instance of Firefox browser from a local host trying to access a cloud resource (Google drive). The kernel mode network monitor is able to intercept and track and get the complete information about the communication between Firefox and google servers.

The ARMS system is equipped with a GUI where we can see the policy definitions, unit VM definitions. Using ARMS, we can monitor every VM instances in the host and

ISSN: 2582-6433

```
Event: Policy Match: name=cloud_local_client, id=1002,
type=network_monitor
timestamp= 1488648660 (03/04/2017 5:31pm UTC)
process=firefox, id: 12876, user: ashajoseph2015
url: https://docs.google.com/document/u/0/create?
usp=docs_home&ths=true
type: request
rank=1;
dependency=nil;

Event: Policy Match: name=cloud_local_client, id=1002,
type=network_monitor
timestamp= 1488648662 (03/04/2017 5:31pm UTC)
process=firefox, id: 12876, user: ashajoseph2015
url: https://docs.google.com/document/u/0/create?
usp=docs_home&ths=true
type: response 302
rank=1;
dependency=nil;

Event: Policy Match: name=cloud_local_client, id=1002,
type=network_monitor
timestamp= 1488648665 (03/04/2017 5:31pm UTC)
process=firefox, id: 12876, user: ashajoseph2015
url: https://docs.google.com/document/u/0/d/1CdAfCImh-
0oIIWOEM8w1PXZtwsBC56WdpjUNaq5WmSU/edit
type: request
rank=1;
dependency=nil;

Event: Policy Match: name=cloud_local_client, id=1002,
type=network_monitor
timestamp= 1488648669 (03/04/2017 5:31pm UTC)
process=firefox, id: 12876, user: ashajoseph2015
url: https://docs.google.com/document/u/0/d/1CdAfCImh-
0oIIWOEM8w1PXZtwsBC56WdpjUNaq5WmSU/edit
type: response 200
rank=1;
dependency=nil;
```

Fig. 4.5 Sample event logs from ARMS system

The Fig. 4.6 shows the main GUI screen of the system.

Resource allocation for Unit VMs can be done using ARMS GUI as shown in Fig.

4.7. Number of CPUs, Maximum memory, bandwidth reuirement etc. and the priority of their availability can be specified in this GUI screen.

The CPU usage, memmory usage, hard disk utilization and bandwidth consumption of the Virtual Machines can be monitored in real-time using the ARMS GUI as shown in Fig. 4.8.

ISSN: 2582-6433

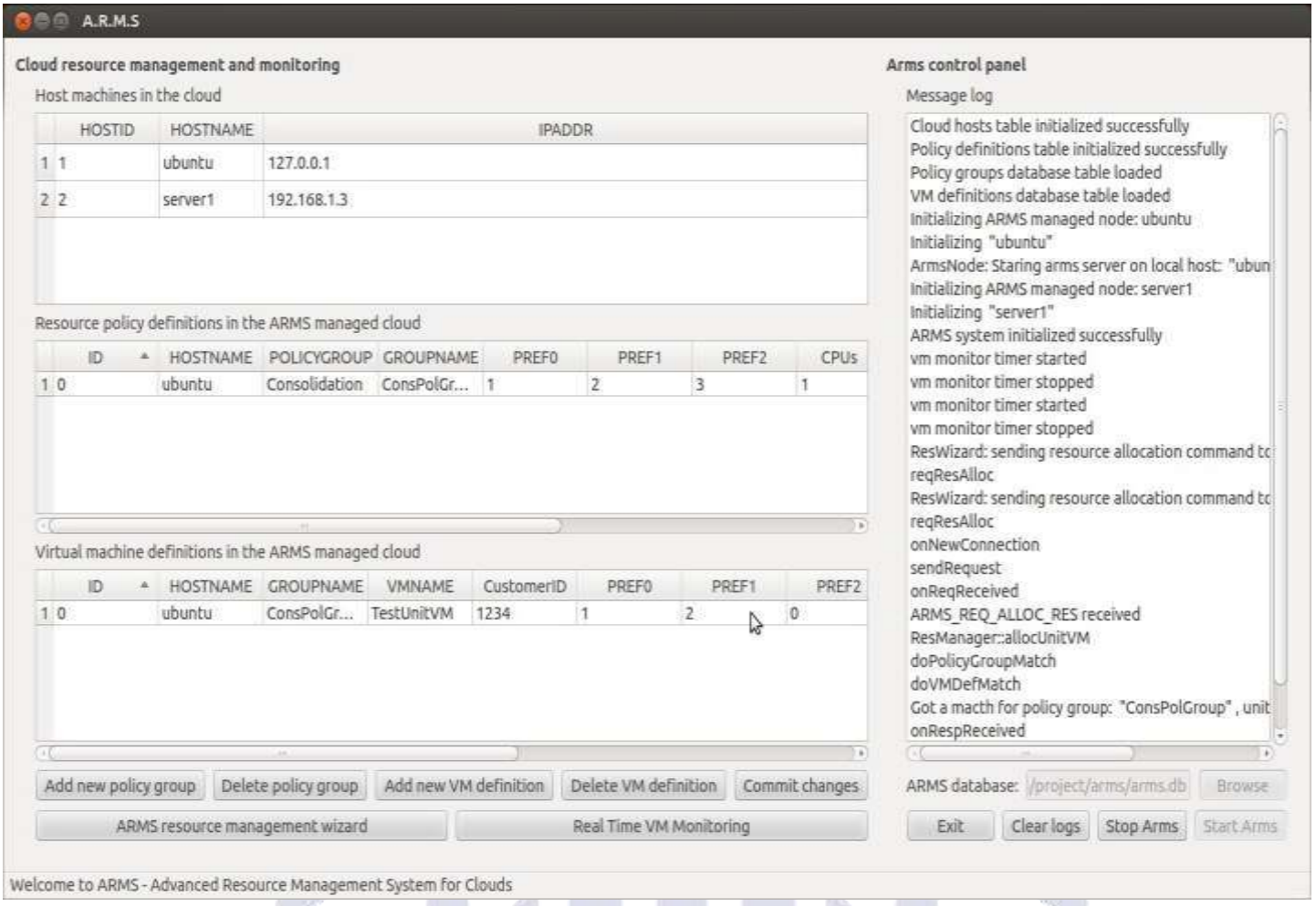

Fig. 4.6 ARMS GUI main window

ISSN: 2582-6433

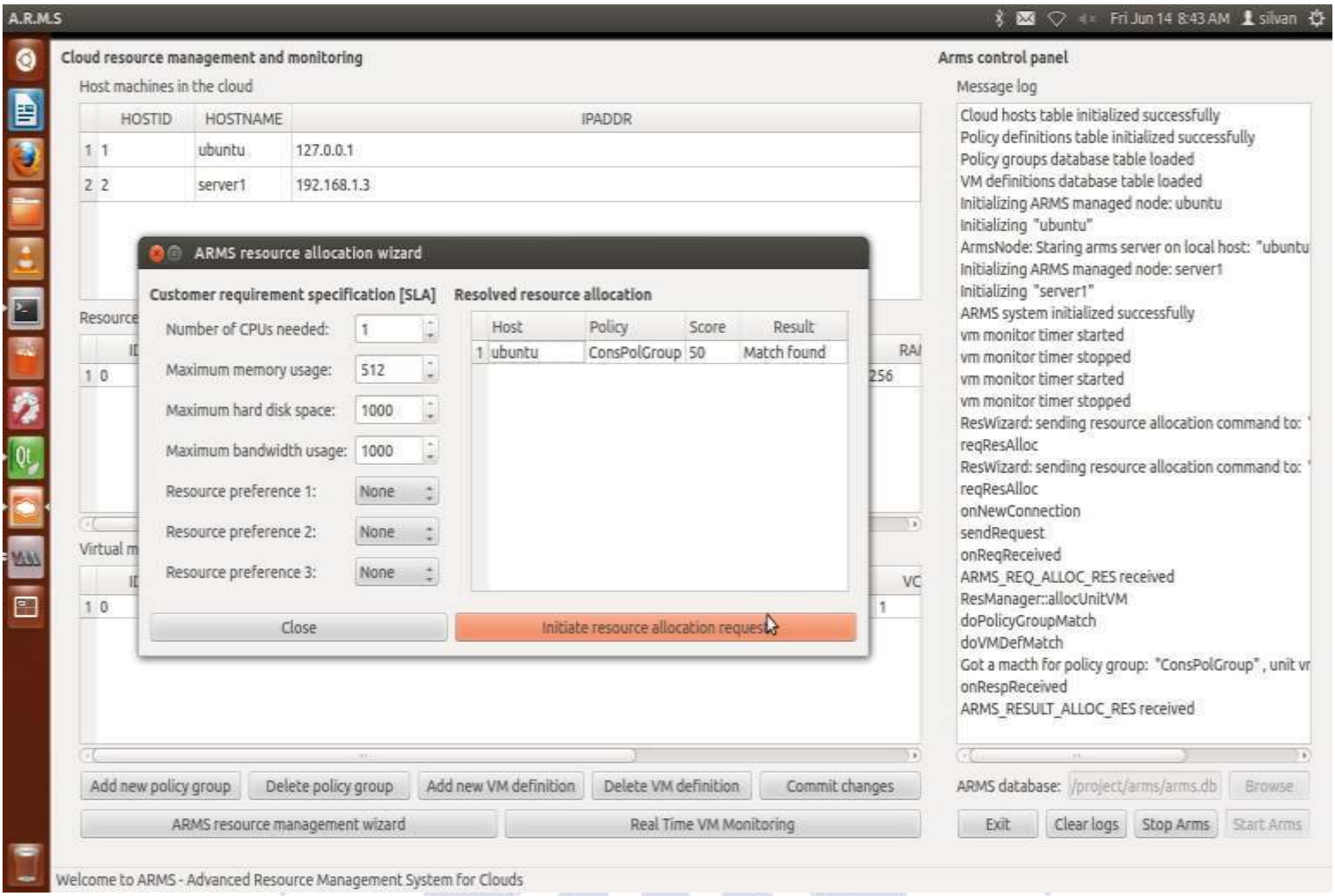

Fig. 4.7 ARMS GUI for resource allocation

ISSN: 2582-6433

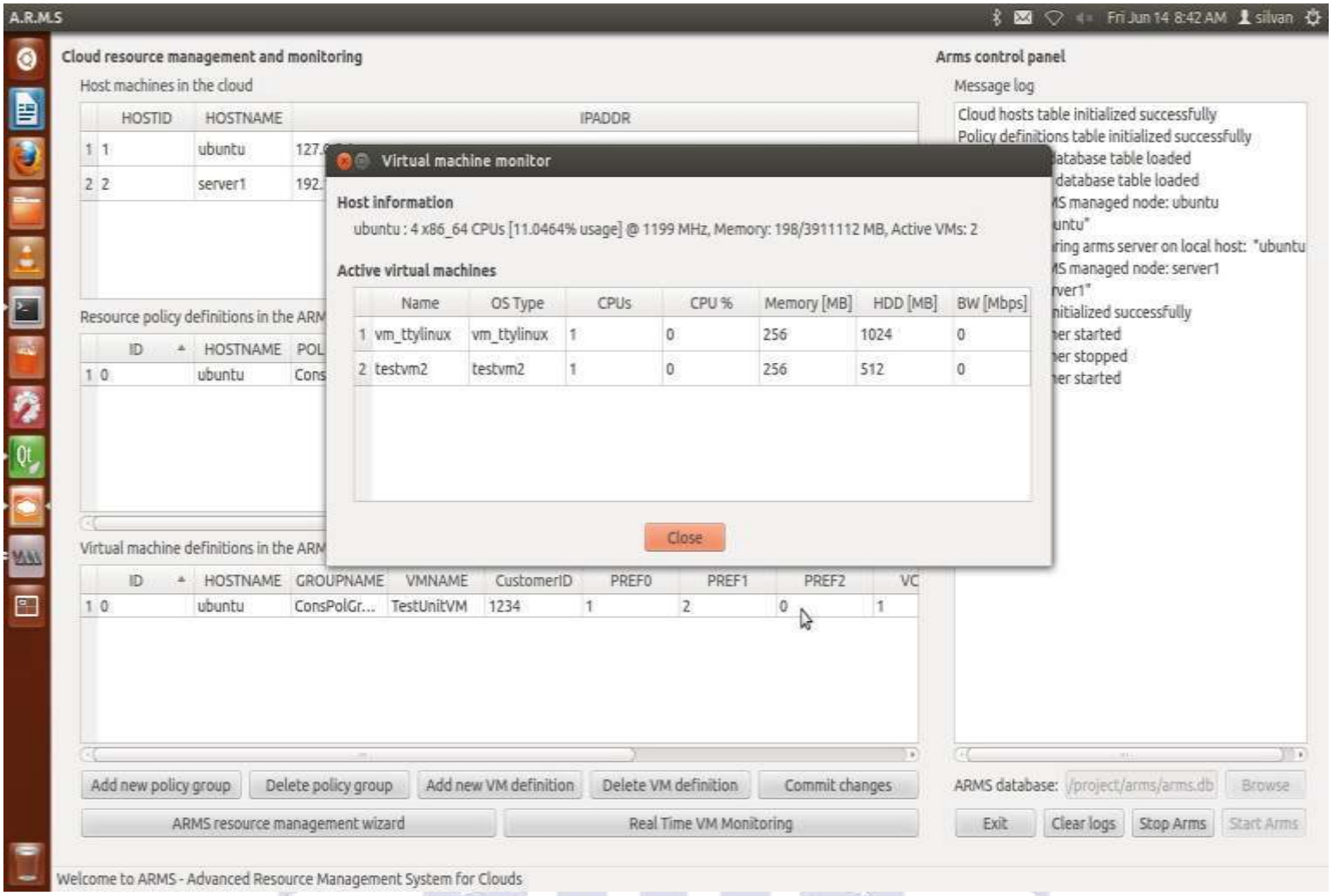

Fig. 4.8 ARMS GUI for virtual machine monitoring

4.5 Performance metrics

Performance of the system is expressed by the gvien metrics:

1. $Max(P, U)$ where
2. P is the number of policy groups in a physical host
3. U is number of unit VM definitions in a physical host
4. Time taken to complete a resource allocation request (in microseconds)
5. Number of physical hosts

Table 4.1 shows the performance metrics in terms of number of policy groups and time taken to find one or more stable matchings in a physical host. The observed data is plotted as shown in Fig. 4.9.

ISSN: 2582-6433

Table 4.1 Number of policy groups vs. time taken

Max(P, U)	**Time (us)**	**Max(P, U)**	**Time (us)**
1	1	26	682
2	5	27	738
3	9	28	794
4	10	29	841
5	19	30	898
6	39	31	966
7	46	32	1021
8	74	33	1083
9	85	34	1148
10	100	35	1233
11	129	36	1304
12	138	37	1359
13	160	38	1440
14	201	39	1516
15	218	40	1607
16	261	41	1690
17	283	42	1763
18	320	43	1844
19	356	44	1929
20	399	45	2027
21	440	46	2107
22	475	47	2209
23	523	48	2299
24	568	49	2391
25	620	50	2493

ISSN: 2582-6433

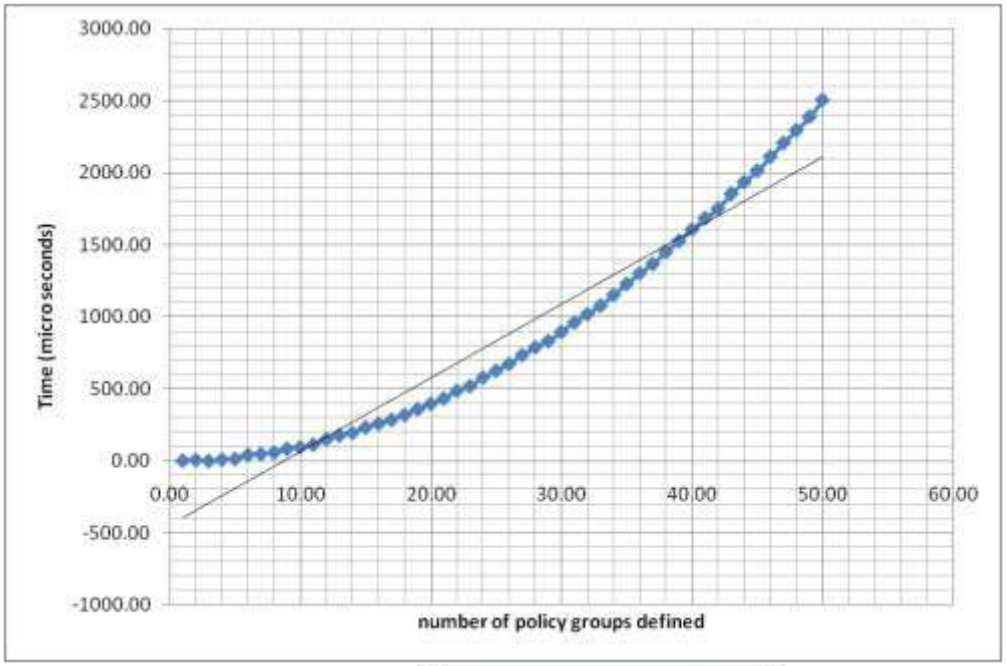

Fig. 4.9 Number of policy groups vs. time taken

Table 4.2 shows the performance metrics in terms of increasing number of managed physical nodes with number of policy groups and unit VM definitions kept constant and time taken to handle a resource allocation request. Note that the time taken are considerably greater than the single host case as this scenario includes the network communication related latency and overhead. The observed data is plotted as shown in Fig. 4.10.

Table 4.2 Number of physical nodes vs. time taken

Number of physical nodes	**Time (us)**	**Number of physical nodes**	**Time (us)**
1	8	26	17566
2	10	27	19681
3	20	28	21958
4	74	29	24381
5	133	30	27006
6	226	31	29784
7	353	32	32775
8	503	33	35943
9	723	34	39301

ISSN: 2582-6433

10	1006	35	42880
11	1339	36	46660

ISSN: 2582-6433

Number of physical nodes	Time (us)	Number of physical nodes	Time (us)
12	1727	37	50654
13	2194	38	54864
14	2736	39	59325
15	3376	40	63995
16	4090	41	68923
17	4916	42	74082
18	5840	43	79512
19	6861	44	85189
20	7991	45	91120
21	9260	46	97333
22	10654	47	103822
23	12177	48	110599
24	13818	49	117644
25	15627	50	125001

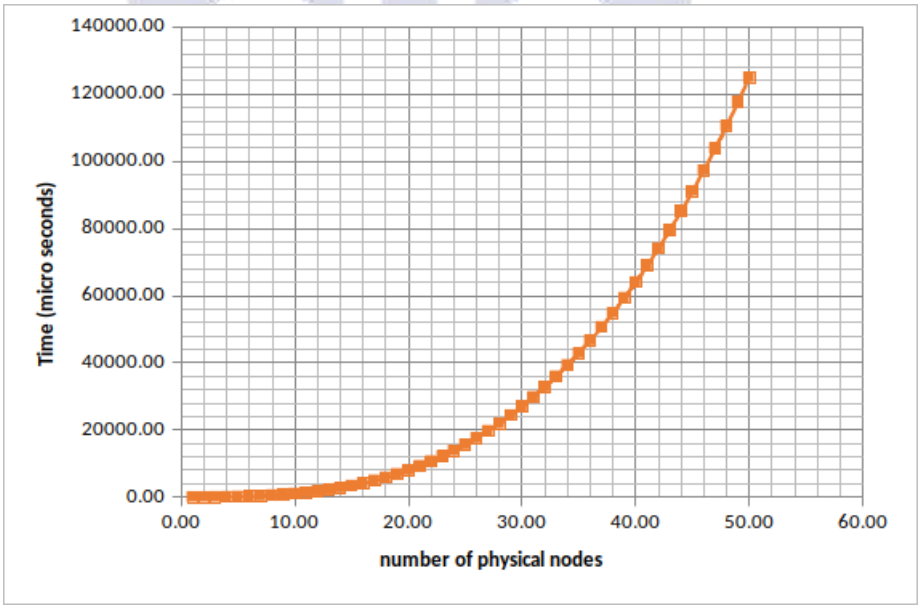

Fig. 4.10 Number of physical nodes vs. time taken

4.6 Summary

ISSN: 2582-6433

The performance evaluation discusses about the results drawn by considering the most important performance metric like the time complexity of the algorithm implemented in the system in terms of varying number of VM definitions as well as varying number of physical nodes. The tests are conducted in a small-sized private cloud setup as well as using simulated cloud environment with more than 50 physical hosts. Forensic comput-ing and cyber/digital crime investigation emerged because of increase in digital crime due to the development of the Internet and proliferation of computer technology. We have reviewed the literatures in cloud and forensics and identified many categories of activity research and a few of them are framework, trustworthiness, computer forensics in networked /virtualized environments and acquisition and analysis of evidence data. In this segment, we suggest a crime and criminal profiling approach using data obtained from the online environment in particular from virtual hosts so that the forensic inves-tigation outcome from online or un-distributed networks is central and accurate. The report contains details. Once combined with the agent module of a program like ARMS, the device suggested could become a feasible alternative for any hierarchical network, as a pragmatic automated forensic platform.

CHAPTER 5
MOBILE SECURITY AND FORENSICS

5.1 Introduction

Today's smartphones such as the Apple iPhones and huge variety of Android phones are concise forms of powerful computers with superior performance involving nearly a dozen CPUs (multi-core), gigabytes of storage, and enhanced communication facilities such as Software Assisted GPS. As new characteristics and applications are integrated into mobile phones, the amount of data stacked away on the devices is continuously growing. Mobile application business has turned the mobiles devices into portable data carriers, and they keep track of almost all moves of the user. Preponderence of mobile devices in daily lives has led to their preponderence in daily crimes. Thus, the digital data collected from mobile phones has become one of the principal sources of evidence for investigations relating to civil crimes and criminal cases. A forensic investigation, not involving a mobile device, is actually difficult to carry out, nowadays. Mobile foren-sics is a digital forensics branch devoted to collecting and analyzing mobile devices to identify and restore digital evidence of crime. In this context, the term "mobile de-vices" refers to a broad spectrum of devices which has communication facilities and storage facilities for digital data. There are standard guidelines for the collection and analysis of mobile devices that are principally targeted towards the preservation and non-contamination of digital data in mobile devices.

The security ecosystem of mobile applications are illustrated in Fig. 5.1. Progres-sive Web

ISSN: 2582-6433

Application (PWA) are mobile applications that are partially installed locally on mobile devices and has a server counterpart in a cloud systems. PWAs are get-ting more and more popular because it is independent of official application stores like Google's Play Store and Apple's iTunes Store. Hence both of these types of apps are included in Fig. 5.1.

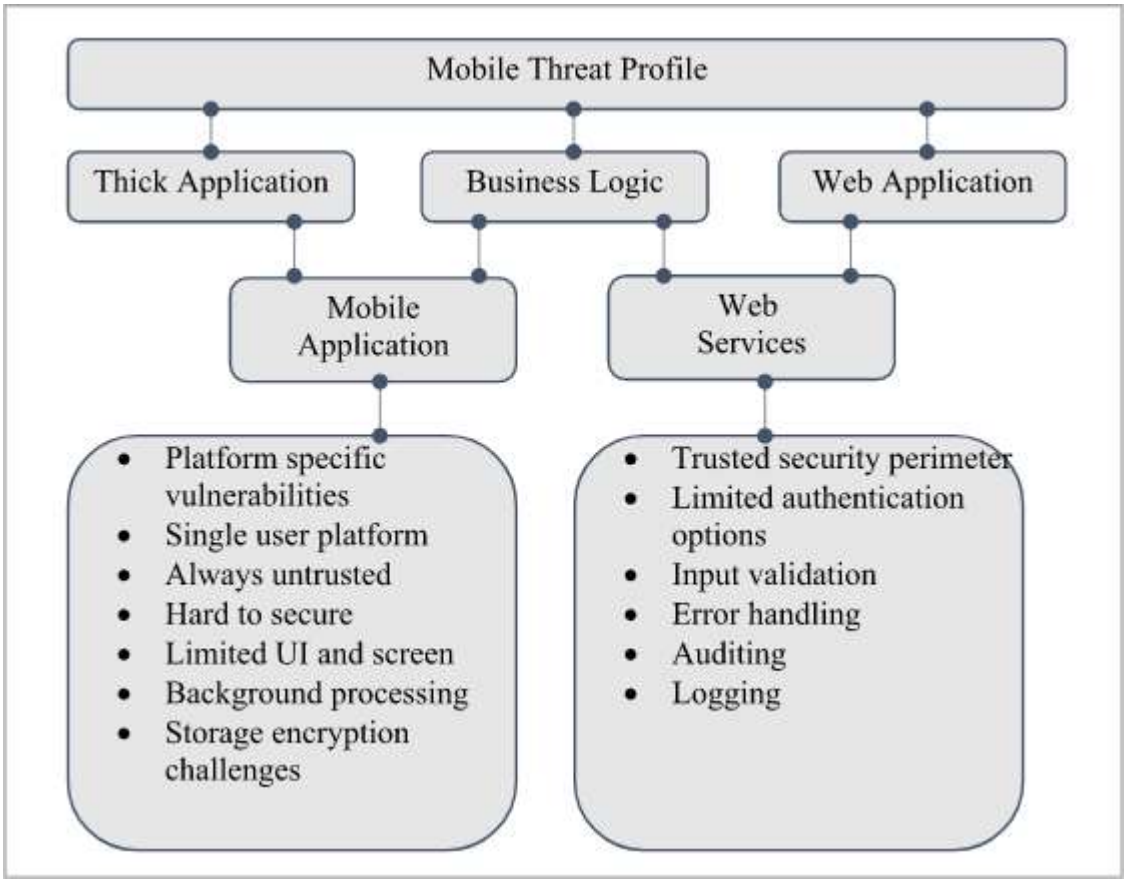

Fig. 5.1 Security ecosystem of mobile and web apps

The continuous evolution of mobile devices is happening at an explosive rate. The hardware and software components used in this industry is numerous. The amount of data that can be stored in modern mobile devices are huge. The data stacked away in the mobile phones can be application specific. Often the investigation method and tool used to communicate with the mobile device can make the evidence invalid in the court because it can affect the evidence integrity and repeatability. **Forensically sound** is the term for the use of forensic equipment or technique used in the modern forensic circles. The core concept of sound forensic examination of digi-tal evidence is that the original evidence shall not be altered. This is highly difficult with mobile devices. Most forensic require a duplex communication channel with the mobile device and hence the device cannot be kept write protected throughout the acquisition. Other evidence acquisition methods may imply replacing the bootloader

ISSN: 2582-6433

software on the mobile device or replace a chip in order to facilitate accessing the evidence data. Whenever a change is required in the device, the process and the resulting changes must be corroborated and documented. As with any evidence collection, not following the approprite procedure during the analysis can lead to loss or damage of evidence or furnish it inadmissible in court. All these challenges make the use of digital forensic analysis tools on mobile devices difficult.

It is to be noted that ISO 27037 specification namely "Guidelines for identifica-tion, collection and/or acquisition and preservation of digital evidence" (2012) defines methods and techniques in digital forensics that are accepted in many jurisdictions.

5.2 Mobile devices and evidence preservation

Evidence collection at the crime site includes the preservation of devices state such as:

1. A turned-on device must be kept turned ON
2. It must be safeguarded from Wi-Fi signals from outside while keeping the state of the phone's Wi-Fi status.
3. It must be isolated from telecommunication signals (2G, 2.5G, 3G, 4G, 4.5G or in other words, GSM/UMTS/LTE etc)
4. It must be isolated from GPS signals
5. IT battery must be kept charged (preferably at the same battery level)

If a mobile device on a crime site is not isolated from all such factors listed above, it will become very easy for the attacker to gain access to the device and lock or destroy all evidence in it. This is typically done using the facilities provided by the mobile device's operating system such as iOS from Apple and Google's Android. The given Fig. 5.2 shows how simple it is for the owner (or, the criminal) to remotely locate, access, lock and erase a typical iPhone.

ISSN: 2582-6433

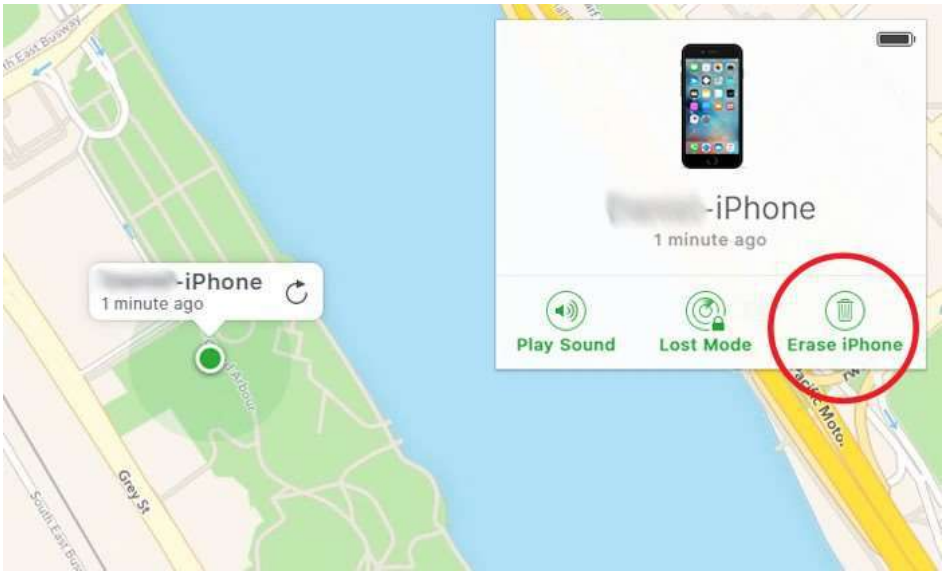

Fig. 5.2 Remotely locate and erase all data in iPhone

5.3 Mobile forensics process workflow

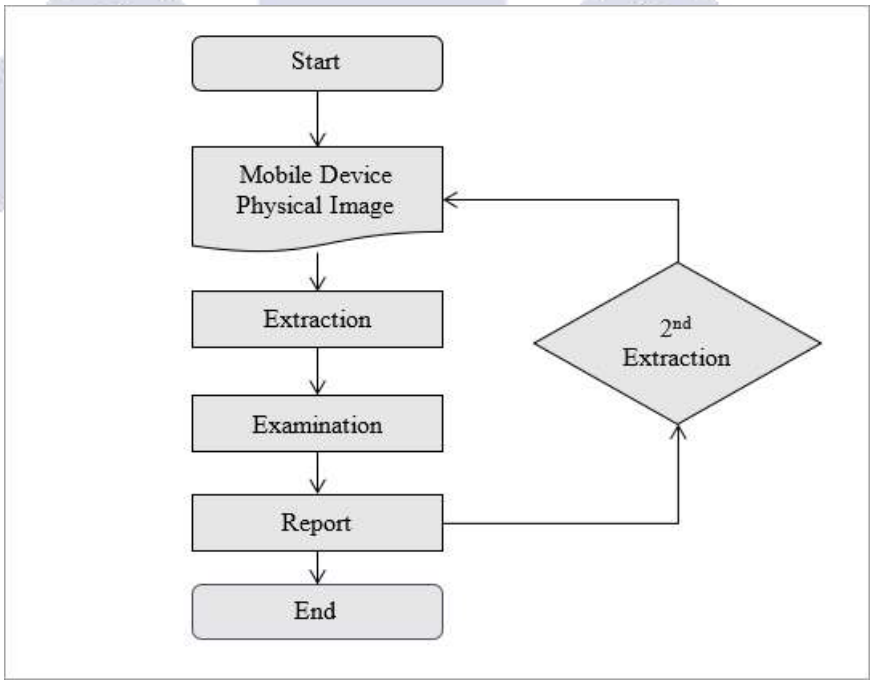

Fig. 5.3 Mobile forensics workflow

The mobile digital forensics process as shown in Fig. 5.3 can be grouped to three main categories:

1. Seizure / Isolation / Identification
2. Evidence Acquisition

ISSN: 2582-6433

3. Examination / analysis / reporting

Each of these operation categories are described in the following sections.

5.3.1 Seizure, isolation and identification

At the time of the seizure, it is important to document with pictures, the various state information of mobile - including not limited to the power state (turned on or switched off), lock status, presence or absence of memory cards and so on. All hardware and soft-ware accessories including cables, chargers, Subscriber Identification Module (SIM) cards data, any clues or hints of PIN or any password shall also be collected.

As seen already, it is fundamental to secure the device from communicating with external agencies - that covers Short Message Service (SMS), Wireless Fidelity (Wi-Fi), Bluetooth and phone calls, but not limited to Global Positioning System (GPS).The old messages can be overwritten by a call or SMS or email during the retrieval of proof. A device that can be accessed over internet can be readily wiped clean remotely. Thus, it is necessary to make use of the following equipments like Faraday bag and / or radio jammer that prevents all electromagnetic communication with device.

Many a times, smartphone features like ”Airplane mode” can also be used to prevent radio communications to outside world. Also, features such as ”Stay awake” can be used to keep the unlocked (display turned on) state of the mobile phone.

5.3.2 Evidence acquisition and analysis

Extracting data from SIM needs hardware tools such as PC/SC Reader that acquires data objects defined by the Global System for Mobile (GSM) 11.11 standard. Data in internal memory (e.g., a memory chip) of the bit by bit copies of the entire physical store can be copied to the device. This permits erased files and any data remnants present to be examined, which otherwise would go unaccounted. The other method of copying logical entities such as files and directories may turn out to be an easier method during examination.

There are different software tools that can extract the data from the memory image. There are specialized forensic software products that can be automated or there are generic file viewers such as hex editors. Some of the specialised tools are Access Data and Sleuth kit to analyze memory images. Since one tool cannot extract all possible information, often it is advised to use two or more tools. When the acquisition becomes more forensically sound, tools will become more expensive, analysis will be longer, tools requires more training.

5.3.3 Data acquisition types

ISSN: 2582-6433

Manual acquisition: In this method, the user interface (UI) of the mobile is used to investigate the content of the device's memory.

Logical acquisition: A clone of logical storage objects (e.g. file system partition), such as folders and data in a logical database.

File system metadata acquisition: When user's data is organized in database, they are referred to as metadata. Such metadata databases can give valuable information about the device usage. E.g. call log is a simple single file SQLite database in Android and iOS.

Physical acquisition: It is the whole file system binary dump. This can contain infor-mation about existing as well as deleted file system objects.

Brute force acquisition: This is used to extract passwords or PINs. Brute force tools are connected to the device and they will generate and submit different combination of character and non-character data as password or PIN until it succeeds. This is time consuming - but often effective depending upon the complexity of the original password or PIN.

On Android phones, the evidence acquisition is much simplified once the Android Debug Bridge (ADB) is enabled. This option is arguably the best weapon for the foren-sic analyst during the retrieval of data from an Android without otherwise affecting or altering the state of the phone. This option can be seen in Settings — Development of almost all Android phones. Android Software Development Kit (SDK) includes this powerful tool named **adb** that is to be used to communicate with the ADB enabled phone over Universal Serial Bus (USB) and Wi-Fi.

Using adb, almost all the information listed above can be accessed from the inves-tigator's desktop. For details, please refer to the elaborate documentation for this tool that also comes with Android SDK. Please keep in mind that 99% of the features of **adb** can be used without root access to the phone which makes **adb** one of the best tools to be used for Android phone forensic collection and analysis.

ISSN: 2582-6433

```
C:\Users\arun\AppData\Local\Android\Sdk\platform-tools>adb devices

List of devices attached

3bc1e02b        device


C:\Users\arun\AppData\Local\Android\Sdk\platform-tools>adb shell

shell@P1a42:/ $ pwd

/

shell@P1a42:/ $ cd sdcard/DCIM/Camera

shell@P1a42:/sdcard/DCIM/Camera $ ls -l *.mp4

-rw-rw---- root     sdcard_rw 10196885 2019-04-11 15:24
VID_20190411_152450.mp4

-rw-rw---- root     sdcard_rw 224922992 2019-04-28 12:20
VID_20190428_121839.mp4

shell@P1a42:/sdcard/DCIM/Camera $ ls -l *.jpg

-rw-rw---- root     sdcard_rw  1986151 2019-03-29 07:30
IMG_20190622_115021.jpg

-rw-rw---- root     sdcard_rw  3230246 2019-03-29 07:31
IMG_20190329_073120.jpg

shell@P1a42:/sdcard/DCIM/Camera $ exit

C:\Users\arun\AppData\Local\Android\Sdk\platform-tools>adb pull
sdcard/DCIM/Camera/VID_20190411_152450.mp4 c:\Camera\

sdcard/DCIM/Camera/VID_20190411_152450.mp4: 1 file pulled. 6.5 MB/s
(10196885 bytes in 1.494s)

C:\Users\arun\AppData\Local\Android\Sdk\platform-tools>adb pull
sdcard/DCIM/Camera/IMG_20190622_115021.jpg c:\Camera\

sdcard/DCIM/Camera/IMG_20190622_115021.jpg: 1 file pulled. 3.9 MB/s
(1986151 bytes in 0.485s)
```

Fig. 5.4 ADB logs

Figure 5.4 shows a sample ADB session from a Windows PC with an Android phone. The commands we use in this session are shown in bold typeface. The log clearly shows the ADB detecting the connected mobile phone. Using ADB, we then log into a Linux shell in the Android phone. We are then able to list all the videos and photos in the phone's camera directory. Exiting from the shell, we are able to use ADB pull command to copy one of the videos and photos to the Windows PC. In a similar way, we can take out most of the data from Android phone.

On Apple mobile systems such as iPhone, the best tool for evidence collection is **libimobiledevice** (http://www.libimobiledevice.org) that will work with iPhone, iPad, iPod Touch and Apple TV.

ISSN: 2582-6433

This software tool does not need Jailbreak. You can read information, backup and restoration of Apple device and the corresponding logical ma-chine installation options. You can import and use them in Linux, are embeded in many digital forensic oriented live distros like **santoku** (https://santoku-linux.com/).

Hardware tools such as JTAG (an industry standard for verifying designs and testing printed circuit boards, by Joint Test Action Group) can also be used for this purpose - but their usage is limited because most mobile devices does not provide such hardware interfaces in a commercially sold mobile device. They are mostly used in research and development centres of phone manufacturers.

5.3.4 Examination and analysis

Once evidence data is acquired in many forms as described above, the following are the most common logical entities that are the potential source of evidence in a mobile device. I.e. these are the potential logical entities that are to be examined in a mobile device.

1. Phone book, Call log, Calendar, Messages (SMS, MMS), To Do list
2. Equipment identifiers
3. Email, Instant messages, Web history
4. Downloaded Documents
5. Photos, Videos, Audio, Graphics
6. Last active location (voice calls and data)
7. GPS logs and stamps on photos
8. Other networks (Wi-Fi hotspots, Access points etc)

With the evidence data, two types of forensic investigations are possible:

1. The criminal's identity is unknown and the crime has already occurred(e.g., a hacking incident).
2. The crime and criminal are both known (e.g., investigation of a child pornography case).

ISSN: 2582-6433

Prepared with the background of the incident and evidence collected, the forensic expert may proceed toward accomplishing the following objectives:

1. Who all are involved: Collect information about the person(s)?
2. What is the exact nature of the events?
3. When did the events related to the crime occur?
4. Why did the offender(s) commit the offence?
5. How did the offender(s) carried out the offence (tools and methods used)?

5.3.5 Reporting

The coverage requires, in fact, a detailed record of all the actions and findings made during the prosecution of a crime. A good report will have precise documentation, notes, relevant photographs and content generated by tools used. Any details necessary to identify the crime should also be included in forensic investigation papers - namely, from where it is reported, by what agency it is reported, statistics, observations and proofs of the individual(s) responsible for the contents of the Docu ment are checked and the name (or signature) proven. Since digital evidence, the instruments, procedures and methods used in a test shall be challenged in court, whenever customized tools are used for examination and analysis, it is advisable to make a copy of the relevant software if it become necessary to reproduce forensic analysis results.

5.4 MDM based GDPR compliance for Android and iOS

Contrary to desktop and server type systems, mobile systems using Android and iOS does not allow its kernel to be modified by third party developers. This means device drivers or kernel modifications are impossible. Since Android has Linux as its ker-nel, implementation of PEC is theoretically possible. However, it is still not feasible in commercially available mobile phones from vendors like Samsung. In the case of iPhones, the operating system is proprietary Unix and modification of that kernel is legally impossible for third parties.

Under the circumstances described above, the most feasible mechanism to imple-ment a security monitoring and policy enforcing mechanism is by making use of the technology called MDM. MDM frameworks are supported by Android and iOS and is mainly used to provision, monitor and manage devices used in corporate environments. Using this technology, an agent software can be installed in mobile devices and that can be used to control the devices and implement device operation policies by administrator using a central server.

ISSN: 2582-6433

5.4.1 European union general data protection regulation - GDPR

The GDPR allows many European Union-wide organizations, to conform with new requirements designed to protect personal data for their customers. The responsibili-ties of the organizations and the penalties affiliated to the securing of private user data is both organisationally and technically challenging. Under the GDPR's "privacy by design" and "privacy by default" requirements, organizations need to prove that they are in control of user data and have taken steps to protect it. There are a large num-ber of organizations that makes use of mobile devices to process personal data of their customers. GDPR mandates that the organization shall be able to manage all devices that handles sensitive data so that the company can implement group updates, restrict apps and networks, and enforce security measures. In this work, we propose a Mobile Device Management solution using the built-in frameworks of Android and iOS mo-bile platforms which incorporates GDPR articles relevant to a small to medium sized organization.

From a technical point of view, apart from all legal aspects, GDPR is all about the Secure storage and transfer of data, Access control and monitoring of data, Intrusion or breach detection and notification within the shortest time possible. This work explains the key features of the proposed MDM solution. The document will also map the key features in the proposed MDM solution with the relevant GDPR articles. The proposed solution targets the GDPR compliance requirements of small to medium sized compa-nies (10-1000 employees) in a limited time with a limited budget. The mobile devices of employees can be fully owned by the company, dedicated for company apps, fully owned by company, also allowing personal apps and data and for "Bring Your Own Device (BYOD)" based operation.

5.4.2 MDM concepts

The following are the key concepts in MDM specifications by Android and Apple: **MDM Server** This refers to a PC/Laptop, which will be used by the organization's IT administrator to protect, monitor and control all the devices and data associated with the company. The OS running on the server could be Windows or Linux. The MDM server software can also be easily hosted in a cloud.

Managed Device This refers to any Mobile phone/Tablet running on iOS or Android platform.

Vault App This refers to a standalone app installed on the managed device. This will help in monitoring, protecting and controlling the data stored in the Managed device. **Data Protection Suite (DPS)** This refers to the MDM software and Vault App, which run on the MDM server and the Managed device respectively.

ISSN: 2582-6433

BYOD Bring Your Own Device mode of operation of institutions where employees are encouraged to bring their own devices for business or work purposes.

5.5 Methodology

This section describes the realization of GDPR compliance using MDM framework.

5.5.1 Prerequisites

The MDM server software will run on Windows/Linux/MacOS, assuming that the ma-chines have enough processing power to handle a typical Server/Application like en-vironment. The MDM Server software can also be hosted in a cloud. In which the Android OS version should be 5.0 and above to run the Vault App and iOS version should be 9.0 and above to run Vault App.

5.5.2 Architecture

The high-level architecture of the Data Protection Suite (DPS) is as shown in the figures Fig. 5.5 and Fig. 5.6. As shown in these figures, the DPS consists of three functional entities namely The MDM server, which is deployed in company Local Area Network (LAN), the push notification server that belongs to Apple or Google and the managed device(s) in LAN or in Internet that acts as client(s) to MDM server.

ISSN: 2582-6433

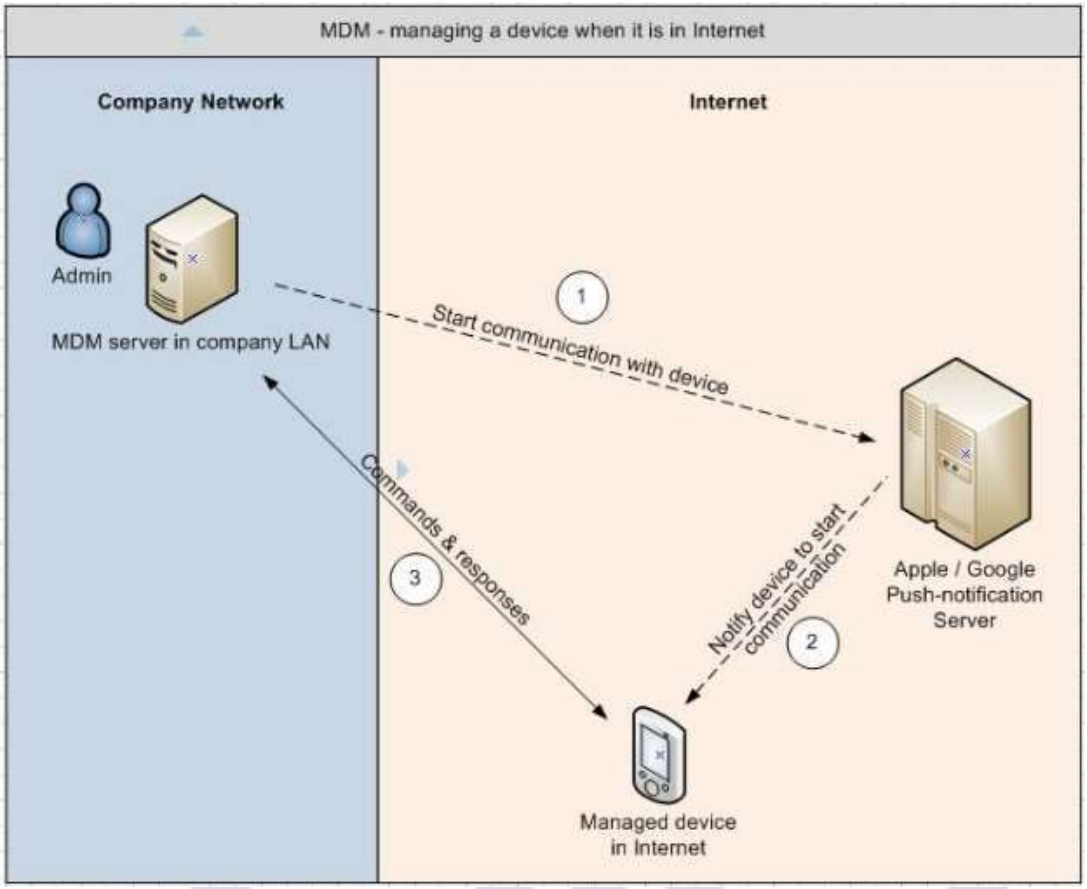

Fig. 5.5 Managing devices in Internet

Note that the push notification server is integral part of the MDM architecture en-visaged by Apple and Android. Without the push notification server, MDM solutions are not possible. Whenever a communication is required from server to client, a noti-fication is pushed to the device from server via the notification servers - shown as Fig.

5.5 and Fig. 5.6. The device wakes up and starts communicating with the server till the logical end of the particular communication session. The client devices will never initiate communication with server on its own accord.

The block diagram shown in Fig. 5.7 illustrates the MDM server application and the Mobile Vault application and their software components, each of which are described in the following sections.

5.5.3 MDM server application

The MDM server application runs on server at company premises. The application supports Linux, Windows and Mac server environments. The application will have a

ISSN: 2582-6433

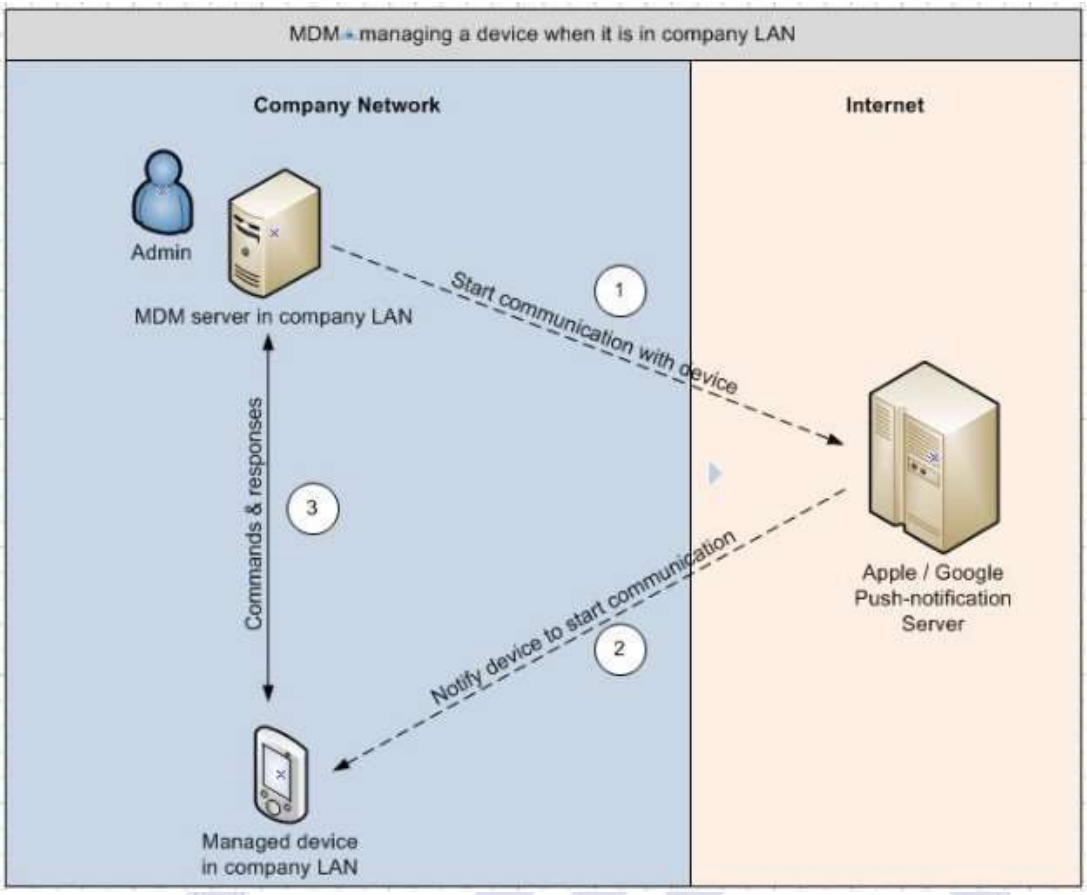

Fig. 5.6 Managing devices in local network

management console GUI that enables the Administrator to:

1. Enroll devices
2. View and manage enrolled devices

The MDM server application communicates with Apple/Google notification servers to initiate a management session with the device. The features provided by the MDM server application in a management session are described in detail below.

5.5.4 Android and iOS built-in MDM support

Android and iOS platform provide various MDM features which are built-in in the OS. The MDM server will make use of these features exclusively for device management. In general, iOS provides more extensive MDM features than Android. So, this will be a limiting factor in Android. In order to develop an Enterprise Mobile Device Man-agement software for Android, there are certain rules and regulations from Google to

ISSN: 2582-6433

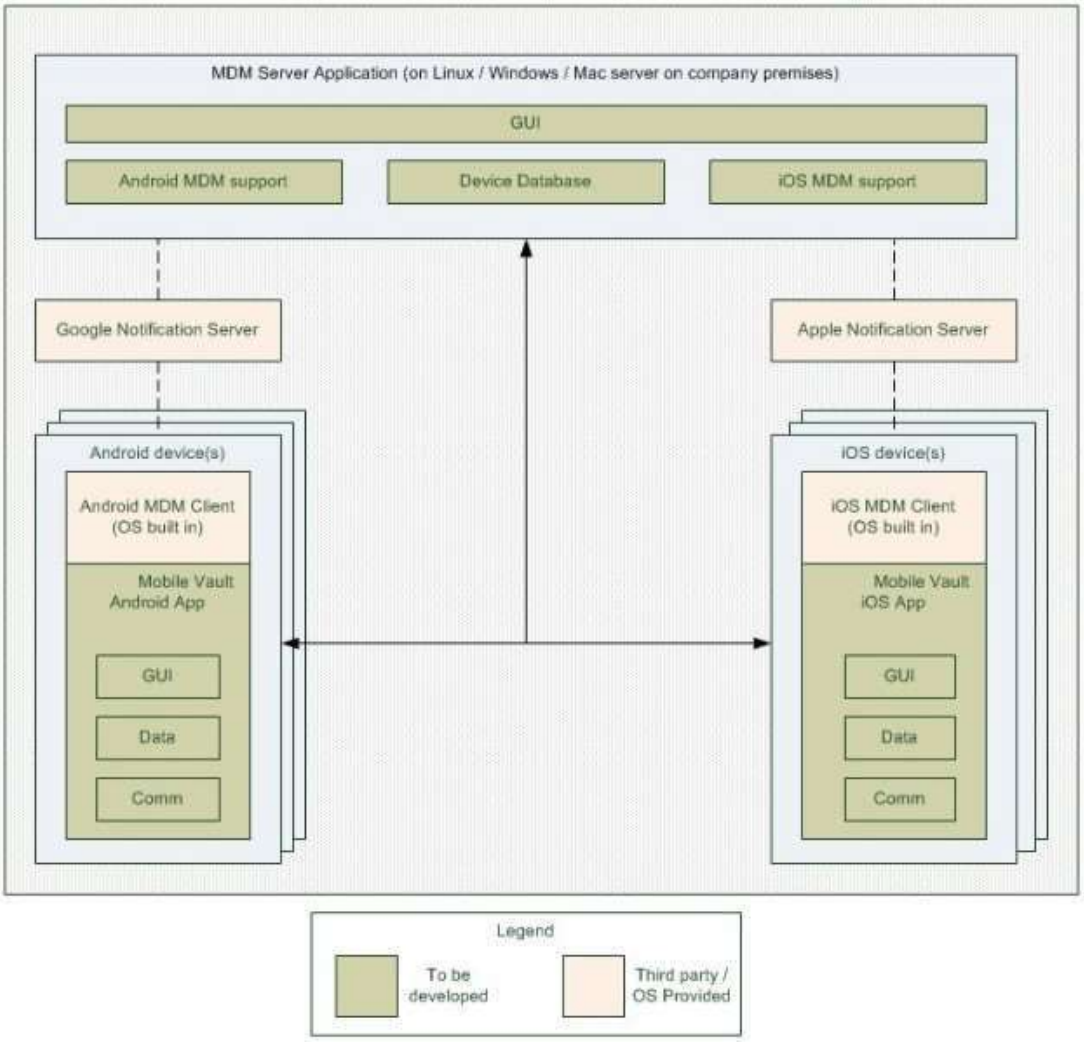

Fig. 5.7 DPS - High level software architecture

follow. The details of which can be found at Google developer web site. The develop-ment of DPS for Android will be according to these terms and conditions.

5.5.5 Mobile vault app

The Mobile Vault app is an integral component of the DPS. It essentially provides an encrypted storage for other managed apps (trusted applications). The app will also provide facilities to view the files stored in the vault and open it in other trusted apps. This essentially provides the app containment feature which is a core requirement for Mobile Application Management. The various features as well as mapping of these features with GDPR article, are explained in detail in the following sections.

5.6 Results and discussion

ISSN: 2582-6433

The MDM server was implemented in Ubuntu Linux and the client-side applications on Android and iOS. The features of MDM supported by Apple and Google are found to be elaborate and a solution for GDPR compliance in these devices is found to be fully feasible.

Figure 5.8 shows the web interface to be used by the administrator to control a mobile device remotely. There are quite a lot of functionality supported by MDM spec-ification – this implementation shows only 4 of them in Fig. 5.8.

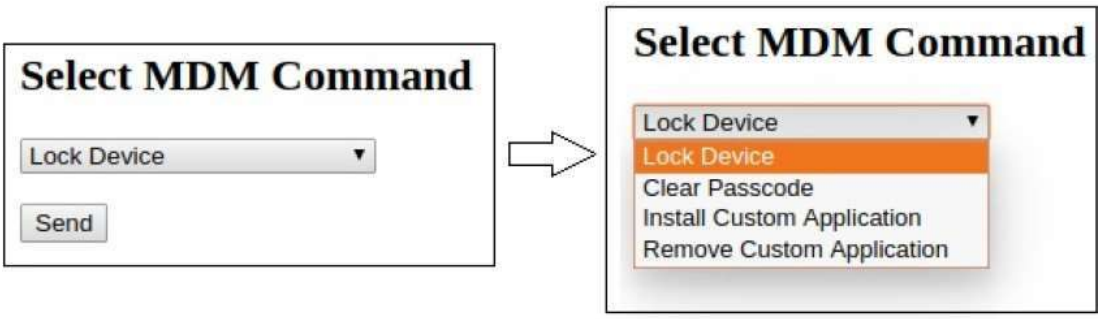

Fig. 5.8 MDM server web interface for device control

Figure 5.9 shows device management support provided by the MDM framework. As said earlier, only a subset of the elaborate specification is implemented here.

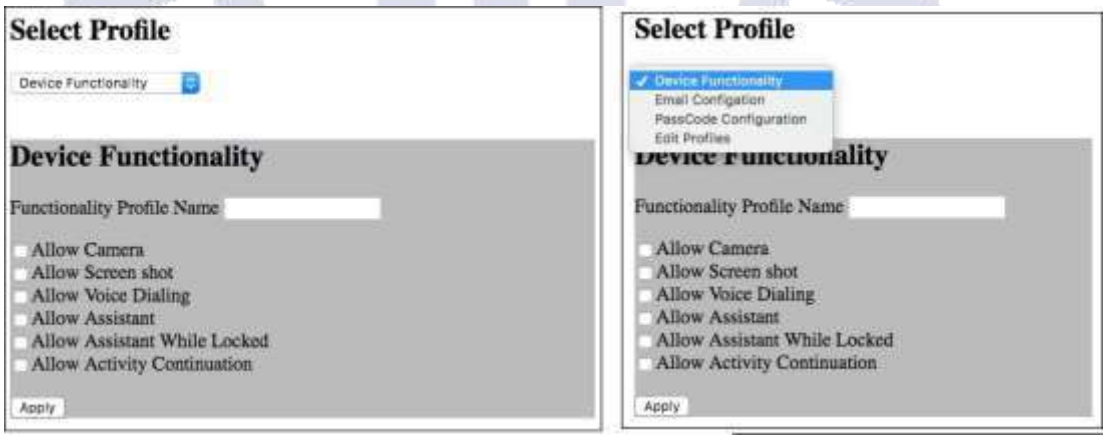

Fig. 5.9 MDM server web interface for device management

Figure 5.10 shows the client side of the MDM implementation. Here the "Profile and device management" section of iPhone settings shows the option to enroll this iPhone to the MDM system. It is mandatory for every phone owner to enrol their device to the MDM server.

ISSN: 2582-6433

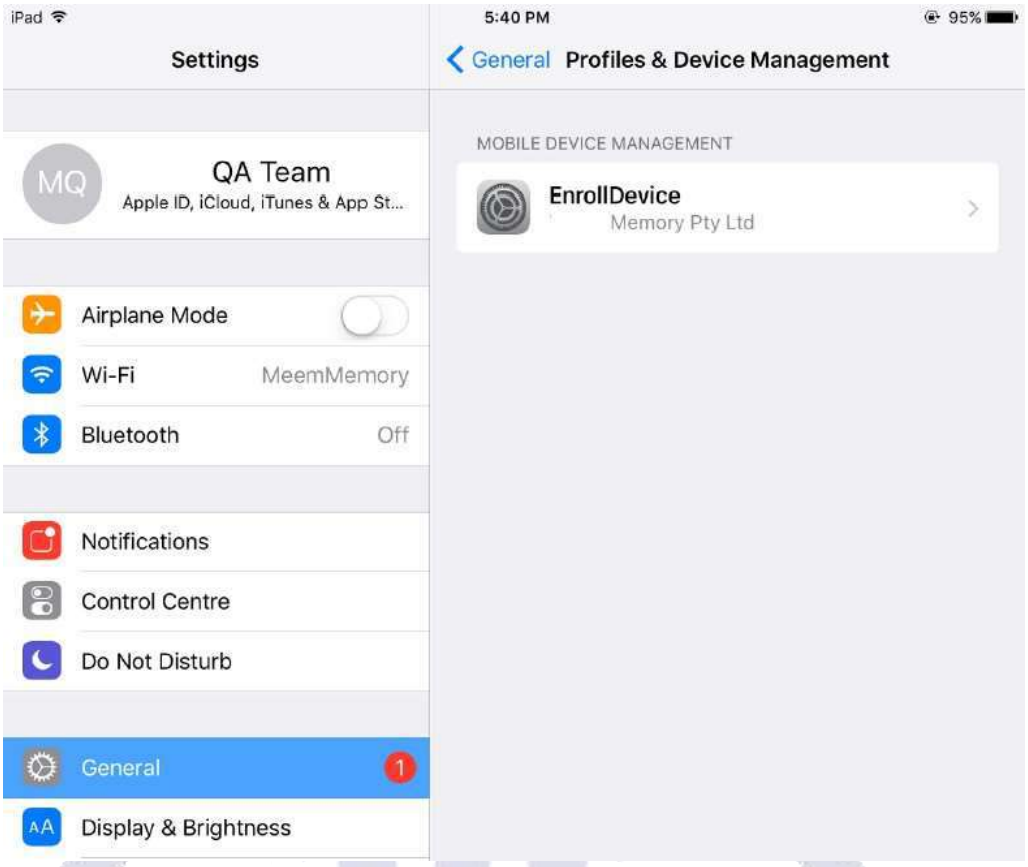

Fig. 5.10 MDM client installed on iPhone

The GDPR clauses and required features and how to implement them using MDM software is described in detail in the following sections.

5.6.1 Category - data management

In this section, we will describe the features related to searching, locating, classifying, minimizing and deletion of stored data. The term "Managed Device" refers to mobile device. The Managed device could be a company owned device or one operating under BYOD policy. The features listed below can be fully or partially implemented based on whether the device is company owned or BYOD. In BYOD, there needs to be a clear demarcation between the user's personally owned data and company owned data. GDPR mandates that the organization should not interfere in personal data. Since the proposed solution will not interfere in the user's personally owned data, there could be some limitations in the way the features are implemented in a BYOD device.

5.6.1.1 Locate device and data

Relevant GDPR Article – 30. One of the critical steps in GDPR compliance is to have a good

ISSN: 2582-6433

understanding of where the data is located or stored. The ability to locate the data will help to build a data map of where the information is stored and find other attributes of the data.

Purpose This feature will be available on the MDM server software. The MDM server will work in conjunction with the Vault App. The server software will be managed by the company appointed Administrator. The admin can use this feature to geographically locate the Managed device used by the employee. This is especially useful if the mobile device is stolen or if any kind of data breach has happened to the company's assets. When it comes to data location, the Vault App residing on the Managed device can help locate the data stored in the Managed device. The vault app can also provide information regarding the destination address of the file (like file/folder name), size, date/time of file creation and file ownership.

Technical brief On the MDM server, the admin will be able to view the list of all the devices used within the organization's predefined boundary. This boundary refers to the network boundary defined by the Organization. This could include some predefined Wi-Fi access points. The locate feature, provided in the software, will give the exact geographical location of the Mobile device.

5.6.1.2 Search data

Relevant GDPR Articles - 15, 16, 17, 18, 20. The GDPR states that the EU residents can request viewing of their data held by the organization, by submitting a Subject Access Request (SAR). The organization should be in a position to undertake and service these requests.

Purpose This feature will be available on the MDM server software. The MDM server will work in conjunction with the Vault App. This feature gives the server the ability to search the data in the Managed device held by the employee. The admin can also update the information in the Managed device based on SAR.

Technical brief The admin can use the MDM software to search for a requested data in the Managed device. The MDM software will only present data belonging to the organization. The request could be any one of the following actions such as Looking for a particular file in a Managed device, looking for a particular category of files in a Managed device, looking for a set of files across different Managed devices, Looking for particular attributes, like size, creation date and time etc., in a file, Sync relevant information between the server and the managed device and Edit or update files on the mobile device. The search capabilities can be customized to suit each organizational need.

5.6.1.3 Classify data

ISSN: 2582-6433

Relevant GDPR Articles - 15,16,17,18,20. The GDPR states that the EU residents can request viewing of particular set of data held by the organization, by submitting a Subject Access Request (SAR). The organization should be in a position to undertake and service these requests.

Purpose This feature will be available on the MDM server software. This feature gives the server the ability to classify the data based on certain criteria defined by the SAR. **Technical brief** By classifying the data, the admin can present the data based on the criteria set forth. This could be used to classify photos, calendars, contacts, documents etc. stored in the Mobile device. The admin can restrict processing certain data based on the classification criteria. Admin can also sync particular categories of data onto the server, based on SAR.

5.6.1.4 Data minimize

Relevant GDPR Articles - 5, 17, 32. Data minimization is one of the main tenets of the GDPR compliance. The primary goal of this feature is to make sure the organizations will keep the data only for the original intended purpose thereby reducing the overall amount of stored personal data in their premises.

Purpose This feature along with the classification, gives the server the ability to set validity period for each data residing in the Mobile device. The MDM server will have the necessary UI elements to help the admin to set the validity period for the data stored in Mobile device.

Technical brief By classifying the data, the admin will have the right to set the valid-ity period for particular sets of data. This gives admin the ability to fully control the organization's data stored in the Mobile device. The data can be made to automatically delete from the managed device, once the validity period has expired. The data can be reinserted into the managed device upon renewal or based on certain other conditions defined by the admin or the organization. These conditions can be customized for each organization based on their inputs.

5.6.1.5 Data deletion

Relevant GDPR Articles - 17, 19, 25. Right to erasure is part of the GDPR compliance. This also helps to protect data breaches, which is also an important tenet in GDPR. **Purpose** This feature will be available on the MDM server. The admin will be able to delete the data on the Managed device. The delete action could be performed based on a SAR or in case of a data breach. As an extreme step, the admin will be able to wipe out the entire Managed device's data contents, if need arises.

Technical brief The admin will have the ability to perform partial or complete deletion of data, based

ISSN: 2582-6433

on the SAR. Admin could also enable data erasure once the validity period for the particular set of data has expired. The MDM server will present the data based on the criteria set forth by the admin. The admin can perform this operation on all the connected devices.

5.6.1.6 Record processing activities

Relevant GDPR Articles - 5, 15, 16, 17, 18, 20, 24, 35, 42, 44, 45. Under GDPR, it is the duty of the organization to record all the transactions and report any data breaches to relevant authority.

Purpose The MDM server and the Vault App will record all the processing happening on the organization's data in the mobile device. This helps the organization in following ways such as Identifying risky files and take immediate action, and to identify the user behaviour and also to take remedial action and Delete the files in case of any data breach.

Technical brief Using MDM data protection suite of apps, the organization will be able to get the records of all the transactions that has happened on the managed device. The transaction records of all the actions triggered by the server will be securely stored in the server. In case of data breach or data lose, the records will be used for identifying the origins of the issue.

The records can be viewed based on different filter criteria set by the Admin. The organization will be able to monitor all the activities that have happened with respect to the organization owned apps.

The MDM server will also notify the admin in case of any unusual behaviour hap-pening in the managed device. The set of actions that would define an unusual behavior will be formulated based on each organizational need.

The apps owned by the organization will be pre-selected and entered into the MDM server.

5.6.1.7 View and share data

Relevant GDPR Articles - 15, 16, 17, 18, 20. Under GDPR, it is the duty for the organization to protect the data stored in the mobile device, by having control over the organization's data.

Purpose This feature gives the ability to view all the data stored in all the mobile de-vices. The employee can view the organization's data using the Vault App. The em-ployee can share the organization's data only using the Vault App. By this way, the organization will have control over the data stored in the managed device.

Technical brief On iOS platform, the Mobile Vault application will make use of iOS share extensions and 'Open-in' features to restrict the apps that can access the data saved in the vault for viewing and modification. On Android platform similar features will be provided using "Document provider" mechanism. Using MDM server, the Ad-ministrator can set a list of managed apps.

ISSN: 2582-6433

Using above described mechanisms, the viewing and sharing of data stored in the Mobile Vault is limited to those apps in the given list.

5.6.2 Category - data protection and monitoring

5.6.2.1 Data encryption

Relevant GDPR Articles - 5, 25, 32, 33, 34, 35. Under GDPR compliance, the organi-zations have the obligation to make sure all the data processing and collection activities are secure and protected from 3rd party attacks. In case of data theft or unauthorized access, the data cannot be consumed at any cost by any 3rd party organization or indi-vidual.

Purpose All the data belonging to the organization will be encrypted to prevent unau-thorized access. This includes all the data stored in the vault directory in the mobile device and all the records stored in the MDM server. The communication between the MDM server and the Mobile device will also be encrypted to prevent man in the middle attacks.

Technical brief The MDM solution encrypts the data in following scenarios: 1. The Mobile Vault app provides a secure storage in phone storage. All data stored in the Mobile Vault will be encrypted using AES 256-bit. 2. All the communication between the MDM server and the mobile device will be protected under Transport Layer Service (TLS) v2 (previously, Secure Socket Layer (SSL)) which is the existing standard in secure data transfer.

5.6.2.2 Data access violation and breach message

Relevant GDPR Articles - 5, 15, 16, 17, 18, 20, 24, 35, 42, 44, 45. Under GDPR, it is the duty of the organization to record all the transactions and report any data breaches to relevant authority. Also, it is the duty of the organization to report any data breach within 72 hours of the breach.

Purpose The GDPR solution will help organizations to identify data breaches and take immediate remedial action. The Mobile Vault app can record all access for data (read/ modify /delete) stored in it. Also, the MDM server can monitor the installation of unauthorized apps and warn and report to the user/administrator at predefined intervals. **Technical brief** The MDM server can be configured such that, it can detect any un-wanted mobile device software installs. It can blacklist applications and whitelist appli-cations. It can send a message to the employee to uninstall the blacklisted apps within stipulated time. Can inform the admin about the breach to take necessary action. Can record all the data breaches securely.

5.6.2.3 Monitoring apps for protection

ISSN: 2582-6433

Relevant GDPR Articles - 5, 15, 16, 17, 18, 20, 24, 35, 42, 44, 45.

Purpose The MDM server will help organizations monitor the apps installed on all the mobile devices. This includes blacklisting and whitelisting apps and also remote uninstall of apps, in case of data breach.

Technical brief The MDM server helps the organization to allow or restrict the follow-ing actions on the apps such as App installation from unknown sources, Installation of non-enterprise apps when connected to company's network, App deletion, In App pur-chase, iTunes store, App sharing and Transfer of data between managed and unmanaged apps.

5.6.3 Category - device control

Some of the key MDM features, relating to GDPR, are described below. Please refer to Annexure-1 to get a full list of MDM features which will be supported in MDM server software.

5.6.3.1 Enforcing password policy

Ability to change the password of the mobile device in case of breach and also the ability to set default password length.

5.6.3.2 Enforcing restrictions on device features

Ability to control the camera, screenshot recording, voice dialling, I Message, Siri re-motely in case of any breach of data, Ability to restrict data sharing between managed and unmanaged apps, Ability to wipe/erase all the data in the mobile device in case of data breach or theft, Ability to remotely lock device, Ability to filter URL in browser and the ability to change permissions for all the interfaces like Bluetooth, Wi-Fi and USB.

5.7 Summary

In this chapter, we addressed the problems in the field of mobile forensics. Most of these challenges arises because of the closed nature of mobile operating environments. Even though Android platform is open source, it is not easy to get access to the system software components in a commercially sold Android phone. Apple iOS is a tightly guarded closed environment. Since popular mobile platforms are not easy to be foren-sically analysed, we have adopted another method by which we can have significant control over mobile device operations - which is called Mobile Device Management (MDM) framework. MDM framework is supported by both Android and iOS and gives considerable control over device operation remotely. In order to prove the usefulness of

ISSN: 2582-6433

MDM framework in mobile operation security as well as collecting evidence infor-mation, we have designed and implemented a compliance solution for GDPR, which is a strict regulation of European Union that mandates very stringent requirements on of personal information protection by all organizations that handles personal information of EU citizens.

CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1 Conclusion

The massive amount of data to examine as well as byzantine data flow patterns in mod-ern software systems have made the digital forensics process, generally, the availability and acquistion of evidence data more challenging. A security enhanced operating sys-tem kernel can make the evidence acquisition more authentic and spatiotemporal com-pared to conventional methods of evidence acquisition which usually depends upon analysis of application and system logs.

In this research, we have proposed such a security solution (Crime Pattern Matching based on Process Execution Contexts - CPM-PEC) which includes a process monitor-ing mechanism that is implemented with OS kernel. The kernel mode process monitors latent security susceptible events to an application counterpart that examines the events to find matches with latent crime patterns –which are pre-defined sequences of secu-rity susceptible events. This combination of kernel mode and user mode components makes sure that every process in the system is monitored from its creation to termina-tion for various outcomes in its lifetime. For evaluation purposes, the proposed solution is implemented and integrated to Linux Security Module (LSM). It is observed that less than 2% overhead is incurred by the addition of this proposed solution in Linux kernel. Legacy methods of digital forensics tend to be lesser effective in a cloud environment. A proactive approach in which we observe and analyse the cloud system in real time using a distributed monitoring framework seems to be more practical. For investiga-tions relating to civil crimes and criminal cases, the digital data collected from mobile devices has become one of the primary sources of evidence.

In this thesis, the development and enforcement of policy for protecting the data in the systems using digital evidence acquisition techniques based on PEC analysis which uses the crime pattern matching algorithm and CPM daemon process are proposed and implemented.

We have developed Techniques for Policy Development/Enforcement for Protecting the Data in The Systems. The proposed Crime Pattern Matching - Process Execution Context Analysis Techniques can be used for stand-alone systems, which uses the Crime Pattern Matching Algorithm and Daemon Process. Our technique makes use of the Event History and Execution Context of the Processes.

ISSN: 2582-6433

Our work is trying to find the solutions to the problems such as:

1. Is it possible to completely/partly avoid the existing forensic tools by replacing it with security enhanced operating systems? If so, what are the possible exten-sions?
2. Will replacing the existing forensic tools with Security Enhanced OS, make the forensic process easier or difficult?

The implementation of CPM-PEC technique is trying to bridge the gap between ex-isting security tools with proven cyber forensic models. At present, virtually no other framework exists that make use of operating system level monitoring that provides com-plete access to virtually all events in the system or anything which make use of the exe-cution contexts of the processes. This work aims on completed the following milestones during this research. Classification of threats and crimes that comes under the scope of this framework are identified first. Further, cyber forensic models and algorithms for mapping the models to the detected real-life events are identified. Then carrying out the detection of identified events using corresponding Linux kernel system entities that are related to LSM framework are studied in detail. The study of LSM framework also included a detailed analysis of SELinux which is one of the most popular LSM modules currently. As a future work, integration of other forensic tools (once evidence data is collected) is also planned.

Evidence acquisition in Advanced Resource Management System (ARMS) for Cloud which uses the distributed policy and rule engines are implemented which make use of the egalitarian stable matching algorithm and proved that the CPM-PEC technique can be applied/integrated with the cloud environment. Finally, in this work, we have done the study of mobile forensic approaches and proposed and implemented Mobile Device Management (MDM) based GDPR compliance for Android and iOS.

6.2 **Future work**

The focus of future research is on improving the whole cyber forensic investigation process by introducing log-based profiling, which involves research into more efficient evidence acquisition systems that should be ultimately built in as part of system soft-ware and in some cases, even partially or fully implemented in hardware.

We plan the future work to make use of Artificial Intelligence (AI) for security, since Cyber devices with AI, classify current activity by calculating how analogous such patterns are used to identify malicious software behaviour. Classification is inherently inclined to both false positives and false negatives, and a latent high degree of polishing on a company by company basis is required. Disguise as a different malware to confuse the AI which is called as Dolphin Attack are recent

ISSN: 2582-6433

activities by hacker and they will do this by exhibiting activity patterns not known to the AI or decelerating its reaction. Digital voice assistants like Siri, Google Assistant, Bixby, and Alexa can be used by hackers to control digital devices via what researchers are calling the Dolphin Attack. It basically takes advantage of device's microphone, which can pick up frequencies up to 20,000Hz and ultrasound frequencies. Hence, we propose to apply machine learning algorithms to detect and predict the crimes in the future.

The future work will focus on improving the digital forensic investigation process, which involves research into more efficient evidence acquisition techniques which uses crime-pattern matching algorithms and tools that should be ultimately built in as part of system or kernel and in some cases even partially or fully implemented in hardware, and to extend the solution to prevent the crime before it is or about to be committed. We foresee the probability of applying neural networks and genetic algorithms for crime pattern matching.

REFERENCES

Abdullah, Mohd. Taufik., Ramlan, Mahmod. and Ghani, Mohd. (2008), 'Advances in Computer Forensics', *International Journal of Computer Science and Network Security* **8**(2), 215-219.

Abdulghai., Ahmed, A. and Nurul, Amirah. Abdullah. (2016), Real Time Detection of Phishing attacks, *in* 'Proceedings of Information Technology, Electronics and Mobile Communication Conference', IEEE, pp. 1-6.

Adam, Jansen. (2010), Digital Records Forensics: Ensuring Authenticity and Trust-worthiness of Evidence over Time, *in* 'Proceedings of 5th International Workshop on Systematic Approaches to Digital Forensic Engineering', IEEE, pp. 84-88.

Alaa, Altorbaq., Fredrik, Blix. and Stina, Sörman. (2018), Data subject rights in the cloud: A grounded study on data protection assurance in the light of GDPR, *in* 'Pro-ceedings of 12th International Conference for Internet Technology and Secured Trans-actions', IEEE, pp. 305-310.

Android enterprise Feature List, Retrieved from https://developers.google. com/, 2018.

Antony, E., Trent, J. and Xiaolan, Z. (2002), Runtime verification of authorization hook placement for the Linux Security Modules frame work, *in* 'Proceedings of ACM Con-ference on computer and Communication Security', ACM, pp. 225-234.

Arati, B., I. Liviu, I. and Pandurang, K. (2007), Lurking in the shadow: Identifying sys-temic Threats to kernel Data,*in* 'Proccedings of Symposium on Security and Privacy', IEEE, pp. 246-251.

Baggili, Ibrahim. and Breitinger, Frank. (2015), Data Sources for advancing cyber forensics:

ISSN: 2582-6433

what the social world has to offer, *in* 'Proceedings of Sociotechnical Behavior Mining: From Data to Decisions? Spring Symposium', AAAI, pp. 6-9.

Baggili, Ibrahim., Breitinger, Frank. and Cinthya, Grajeda. (2017), 'Availability of datasets for digital forensics - and what is missing', *Digital Investigation* **22**(1), Science Direct, Elsevier, s94-s105.

Bates, A., Tian, D. and Butler, K. R. B. (2016), Trustworthy Whole-System Provenance for the Linux Kernel, *in* 'Proceedings of 24th USENIX Security Symposium', USENIX, pp. 319-334.

Bednarz, A. (2004), 'Profiling cybercriminals: A promising but immature science', networkworld.com/supp/2004/cybercrime/112904/profile.html

Belapure, Sunit. and Godbole, Nina. (2010), 'Cyber Security: Understanding Cy-ber Crimes, Computer Forensics and Legal Perspectives', Wiley India, ISBN: 978 812 6521791.

Bennett, David. W. (2011), 'The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations', *Information Security Journal A Global Perspective* **21**(3), 159-168.

Broadhurst, Roderic., Grobosky, Peter., Alazab, Mamoun. and Chon, steve. (2014), 'Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crimes', *International Journal of Cyber Criminology***8**(1), 1-20.

Broadhurst, Roderic., Brown, Paige., Maxim, Donald. and Trivedi, Harshit. (2019). 'Artificial Intelligence and Crime', *Technical Report*, Korean Institute of Criminology and Australian National University Cybercrime Observatory, Canberra, pp. 1-71.

Casey, Eoghan.(2011), *'Digital Evidence and Computer Crime'*, 3rd Edition, Elsevier Inc; ISBN:9780123742681.

Chen, L., Xu, L., Yuan, X. and Shashidhar, N. (2015), Digital Forensics in Social Net-works and the Cloud -Process, approaches, Methods, tools and challenges, *in* 'Proceed-ings of IEEE International conference (ICNC) on social Networks', CA, pp. 1132-1136.

Chen, D. and Chow, M. (2013), 'Information flow Control and Privacy', Introduction to Computer Security, *Science Direct*, COMP 116, Tufts University Department of Com-puter Science, Final Project Archive, pp. 1-10.

Chou, B., Tatara, K., Sakuraba, T., Hori, Y. and K. Sakurai, K. (2008), A Secure Virtual- ized logging scheme for digital Forensic in comparison with Kernel Module approach, *in* 'Proceedings of International conference on Information Security and Assurance', Busan, pp. 421-426.

Chung, Hyunji., Park, Jungheum. and Lee. Sangjin. (2017), 'Digitl Forensic Ap-proaches on amazon Alexa ecosystem', *Digital Investigation* **22**(1), 15-25.

ISSN: 2582-6433

Ciardhuain, S.O. (2009), 'An extended model of cybercrime', *International Journal of Digital Evidence* **3**(1) 1-22.

Clarke, Nathan., Richard, A. and Knake, Robert. (2012), *'Cyber war: The Next Threat to National Security and What to Do about It'*, Google Books, ISBN:978006192233.

Clarke, Nathan., Saad, Alqahtany., Furnel, steven. and Reich, Christoph. (2019), An Evaluation of a Cloud-based Forensic Acquisition and Analysis System (Cloud FAAS), *in* 'Proceedings of 18th annual Security conference', Las Vegas, USA, pp. 1-9.

Cohen, Charles. (2007),*The Growing Challenge of Computer Forensics*. The Police Chief Magazine, The Police chief Publications, USA.

Curran, K., Robinson, A., Peacocke, S. and Cassidy, S. (2010), 'Mobile Phone Foren-sics Analysis', *International Journal of Digital Crime and Forensics* **2**(2), 15-27.

Gale, D. and Shapley, L.S. (1962), 'College admissions and the stability of marriage', *American Mathematical Monthly* **69**(1), 9-15.

Gokila, D. and Baggili, Ibrahim. (2018), I Know What You Did Last Summer: Your Smart Home Internet of Things and Your iPhone Forensically Ratting You Out, *in* 'Pro-ceedings of ARES 13th International Conference on Availability, Reliability and Secu-rity', ACM, pp. 1-12.

Dominik, Schmelz., Gerald, Fischer., Philip, Niemeier., Zhu, L. and Grechenig, T. (2018), Towards Using Public Blockchain in Information-Centric Networks: Chal-lenges Imposed by the European Union's General Data Protection Regulation, in 'Pro-ceedings of International Conference on Hot Information-Centric Networking', IEEE, pp. 223-228.

Ducato, Rossano. (2018), Cloud computing for s-health and the data protection chal-lenge: Getting ready for the General Data Protection Regulation, *in* 'Proceedings of International Smart Cities Conference', IEEE, pp. 1-4.

Endicott, Barbara. E. (2006), Embedding Forensic Capabilities into Networks: Ad-dressing Inefficiencies in Digital Forensics Investigations. *in* 'Proceedings of Informa-tion Assurance Workshop', IEEE, pp. 133-139.

Endicott, B., Popovsky, B.E., Ryan, D. and Frincke, D. (2005), The New Zealand Hacker Case: A Post Mortem, *in* 'Proceedings of the Safety and Security in a Net-worked World: Balancing Cyber-Rights and Responsibilities Conference', Oxford, pp. 1-9.

Erbacher, Robert. F. (2010), Validation for Digital Forensics, *in* 'Proceedings of Sev-enth International Conference on Information Technology: New Generations', IEEE, pp. 756-761.

Fadelli,I. (2018), 'Using machine learning to detect software vulnerabilities', Tech Xplore. Retrieved from https://techxplore.com

ISSN: 2582-6433

Fahdi, M. Al., Clarke, Nathan. L. and Furnell. S.M. (2013), Challenges to Digital Forensics – A survey of Researchers and Practitioners Attitudes and opinions, *in* 'Pro-ceedings of Information Security for South Africa', IEEE, pp. 1-8.

Felson, M. (1994), 'Crime and everyday life:Insight and implications for society', *The British Journal of Criminology* **37**(1), 151-153.

Garfinkel, L. Simson. (2010), 'Digital Forensic Research; The Next 10 Years', *Digital Investigation* **7**(1), ScienceDirect, ELSEVIER, s64- s73.

Gianluca, I. (2002), 'Inside the Linux Packet Filter', *Linux Journal* **2002**(2), 1-12.

Greg, K. (2002), 'Using the Kernel Security Module Interface', *Linux Journal* **2002**(103), 1-7.

Gupta, Alka. and Sharma, L. Sen. (2018), 'A categorical survey of state of the art intrusion detection system- snort', *International journal of Information and computer security* **10**(4), 1-8.

Haiping, Wang., Chen, Danwei. and Guozi, Sun. (2006), 'Key Techniques Research to Effectiveness of Digital Forensics', *Information Network Security* **2006**(1), 1-8.

Hosmer, Chet. (2002), 'Proving the Integrity of Digital Evidence with Time', *Interna-tional Journal of Digital Evidence* **1**(1), 1-7.

Hosmer, C., Feldman, J. and Iordano, J. (1998), Advancing Crime Scene Computer Forensics Techniques. *in* 'Proceedings of SPIE 3576 International Symposium on En-abling Technologies for Law Enforcement and Security conference', pp. 1-10.

Hu, L., Zhang, X., Wang, F., Wang, Wenbo. and Zhao, Kuo. (2012), 'Research on the Architecture Model of Volatile Data Forensics', *SciVerse Science Direct Procedia Engineering*, **29**(2012), 4254-4258.

Irving, Robert. W., David, F. Manlove. and Sandy, Scott. (2008), 'The stable mar-riage problem with master preference lists', *Journal of Discrete Applied Mathematics*, Science Direct, **156**(15), 2959-2977.

Iulia, B., Frank, P. and Andrei, S. (2018), Prudent Design Principles for Information Flow Control. *in* 'Proceedings of 13th Workshop on Programming Languages and Analysis for Security Conference', ACM, 17-23.

Jafari, Fakeeha. and Rabail, Shafique. Satti. (2015), 'Comparative Analysis of Digital Forensic Models', *Journal of Advances in Computer Networks* **3**(1), 82-86.

Jingsha, He., Zhao, Bin., Wan, X., Liu, G. and Huang, N. (2013), On the applications of Digital forensic in different scenarios, *in* 'Proceedings of 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE)', pp. 1-5.

Johnson, Ann. (2017). AI (Artificial Intelligence) and Cybercrime: The good and bad

ISSN: 2582-6433

news.*Technical Report* Microsoft Philippines Communications Team,. Retrieved from https://news.microsoft.com

Joseph, Asha. (2012), Cloud Computing with Advanced Resource Management, *in* 'Proceedings of International Journal of Advanced Technology and Engineering Re- search', **2**(4), 70 - 70.

Joseph, Asha. (2017), 'Provenance of Digital Assets – Bitchains and Bitmarks', *IEEE ComSoc Newsletter*, **1**(1), 5-5.

Joseph, Asha. and Singh, K. John. (2018), 'GDPR and Enterprise Mobile Device Management', *IEEE ComSoc Newsletter: Communication Technology*, **4**(1), 5-5.

Jouvenal, J. (2016), 'Is crime prediction software the way forward for modern polic-ing? Or biased against minorities?', *The Independent*. Retrieved from http://www. independent.co.uk

Juanita, Blue. and Eoghan, Furey. (2018), A Novel Approach for Protecting Legacy Authentication Databases in Consideration of GDPR, *in* 'Proceedings of International Symposium on Networks, Computers and Communications', IEEE, pp. 1-6.

Jun, chen. and Chuanxiong, guo. (2006), Online detection and prevention of phish-ing attacks, *in* 'Proceedings of First International Conference on Communications and Networking in China', IEEE, pp. 1-7.

Junaid, Akram., Majid, Mumtaz., Gul, Jabeen. and Ping, Luo. (2019), 'DroidMD: An Efficient and Scalable Android Malware Detection Approach at Source Code Level', *International journal of Information and computer security* **11**(1),1-8.

Kao,Da-Yu. and Tso,Raylin.(2018), 'Intelligence-Led Response: Turning Theory into Law Enforcement Practice in Cyber Security Incidents', *International journal of Infor-mation and computer security* **11**(4), 9-14.

Kazuo, Iwama. and Shuichi, Miyazaki. (2008), A Survey of the Stable Marriage Prob-lem and Its Variants, *in* 'Proceedings of International Conference on Informatics Edu-cation and Research for Knowledge-Circulating Society', Kyoto, pp. 131-136.

Kerr, Orin.(2005), 'Digital Evidence and the New Criminal Procedure', 105 Columbia Law Review 279, Research Paper **108**(1), 1-40.

Kim, Do. Hoon. and Peter, Hoh. In. (2008), Cybercriminal Activity Analysis Models using markov chain for digital Forensics. *in* 'Proceedings of International Conference on Information Security and Assurance', IEEE, pp. 193-198.

King, T. C., Aggarwal, N., Taddeo, M. and Floridi, L. (2019), 'Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions', Science and Engineering

ISSN: 2582-6433

Ethics. Retrieved from https://doi.org/10.1007

Kwan, L., Ray, P. and Stephens, G. (2008), Towards a Methodology for Profiling Cyber Criminals, *in* 'Proceedings of 41st Hawaii International Conference on System Sci-ences', IEEE, pp. 264-284.

Kyei, Kwaku., Zavarsky, Pavol., Lingskog, Dale. and Ruhl, Ron. (2013), A Review and comparative study of digital forensic investigation models, *in* 'Proceedings of Interna-tional conference on Digital forensic and cyber crime', Springer, pp. 314-327.

Liapakis, X. (2018), 'A GDPR Implementation Guide for the Insurance Industry', *In-ternational Journal of Reliable and Quality E-Healthcare* **7**(4), 3-8.

Losavio, Michael. (2005), Non-Technical Manipulation of Digital Data: Legal, Ethical and Social Issues for Computing, Judicial Process and Digital Forensics. Research Advances in Digital Forensics, *in* 'Proceedings of International Conference on Digital Forensics', Springer, pp. 51-63.

Losavio, Micheal., Deborah, W. K., Adel, S. E. and Shutt, John. (2008), Implications of Attorney experiences with digital Forensics and Electronic evidence in the United States. *in* 'Proceedings of 3rd international workshop on Systematic approaches to Digital Forensic Engineering', IEEE, pp. 79-90.

Loscocco, P.A. and Smalley, S., Patrick, A. M. and Ruth, C. T. (1998), The inevitability of failure: The flawed assumption of security in modern computing environments. *in* 'Proceedings of the NISSC 10', pp. 1-12.

Loscocco, P.A.and Smalley, S. (2001), Meeting critical security objectives with security-enhanced Linux, *in* 'Proceedings of Ottawa Linux symposium', pp. 115-134.

Mahmoud, Elbasir. and Mohamed, S. (2015), 'Mobile Application Information Flow Control',*Almadar Journal for Communications, Information Technology and applica-tions* **2**(1), 2-11.

Marcella, Albert. and Menendez, Doug. Jr. (2014), 'Cyber Forensics: A Field Man-ual for Collecting, Examining, and Preserving Evidence of Computer Crimes', Second Edition,CRCpress, ISBN:978-084-938 3281.

Miroslaw, Z. and Ibrahim, H. (2002), 'Linux Distributed Security Module', *Linux Jour-nal* **1**(1), 1-11.

Mislan, Richard. P, Baggili, Ibrahim. and Rogers, M. (2007), 'Mobile Phone Forecnsic tool Testing', *International Journal of Digital Evidence* **6**(2), 168 -178.

Mobile device Management Protocol Reference. (2018), Apple Developers Forum , pp. 1-227.

Murmann, Patrick., Fischer. and Simone, H. (2018), 'Tools for Achieving Usable Ex Post

ISSN: 2582-6433

Transparency: A Survey', *IEEE Access* **5**(1), 22965-22991.

Murray, T., Andrei, S. and Lujo, B. (2017), 'Special Issue on verified Information Flow Security', *Journal of Computer Security* **25**(1), 319-321.

Nance, Kara., Brian, Hay. and Bishop, Matt. (2009), Digital Forensics: defining a Research Agenda. *in* 'Proceedings of 42nd Hawaii international conference', IEEE, pp. 1-6.

Nasr, Al-Zaben., Nam-Yong, Lee., Yang, J. and Kim, C. (2018), General Data Pro-tection Regulation Complied Blockchain Architecture for Personally Identifiable In-formation Management, *in* 'Proceedings of International Conference on Computing, Electronics and Communications Engineering', IEEE, pp. 77-82.

Nykodym, N., Ariss, S. and Kurtz, K. (2008), 'Computer addiction and cyber-crime', *Journal of Leadership, Accountability and Ethics*, North American Business Press, **35**(1),55-59.

Ø'Connor, T. J. (2012), *'Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers',* Syngress Publishing.

Okechukwu, wori. (2014), 'Computer Crimes:Factors of Cybercriminal Activities', *International journal of Advanced Computer science and Information Technology,* **3**(1), 51-67.

Pandi, H. J., Debruyne. C., O'Sullivan and Declan, Lewis. Dave. (2018), 'An Ex-ploration of Data Interoperability for GDPR', *International Journal of Standardization Research* **16**(1), 1-21.

Park, J., Nguyen, D. and Sandhu, R. (2012), A Provenance-Based Access Control Model, *in* 'Proceedings of 10th Annual International Conference on Privacy, Security and Trust', pp. 137-144.

Pasquier, T. F. J. M. (2016), 'Towards practical information flow control and audit', *Technical Report*, University of Cambridge, UK, UCAM-CL-TR-893(1476-2986), pp. 1-153.

Polkowski, Zdzislaw. (2018), The Method of Implementing the General Data Protec-tion Regulation in Business and Administration, *in* 'Proceedings of 10th International Conference on Electronics, Computers and Artificial Intelligence', IEEE, pp. 1-6.

Pohly, D., McLaughlin, S., McDaniel, P. and Butler. K. (2012), Hi-Fi: Collecting High-Fidelity Whole-System Provenance, *in* 'Proc. of Annual Computer Security Ap-plications Conference', Orlando, FL, USA, pp. 259-268.

Poulsen, Kevin. (2011), Kingpin: How One Hacker Took over the Billion-Dollar Cy-bercrime underground. *Crown Publishers*, ISBN:978-0-307-588685.

Radi, Romansky. and Kiril, Kirilov. (2018), Model Investigation and Realization of Web-based Application about GDPR, *in* 'Proceedings of IX National Conference with International Participation', Sofia, IEEE, pp. 1-4.

ISSN: 2582-6433

Rathi, K., Aderibigbe, T., Karabiyik, U. and Chi, H. (2018), Forensic Analysis of En-crypted Instant messaging Applications on Android, *in* 'Proceedings of 6th Interna-tional Symposium on Digital Forensic and Security', Antalya, IEEE, pp. 1-6.

Regulation (eu) 2016/679of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46 (General Data Protection Regulation). *Official Journal of the European Union L119*, **L** (119), 1-88.

Reza, Montasari. and Hill, R. (2019), Next-Generation Digital Forensics: Challenges and Future Paradigms, *in* 'Proceedings of IEEE 12th International Conference on Global Security, Safety and Sustainability', UK, pp. 205-212.

Reith, M., Carr, C. and Gunsch, G. (2009), 'An examination of digital forensic models', *International Journal of Digital Evidence* **1**(3), 1-12.

Rita, Heims.(2016), 'Global InfoSec and Breach Standards', *IEEE Security and Privacy* **14**(5), 68-72.

Rowlinson, R. (2004), 'Ten Steps to Forensic Readiness', *International Journal of Dig-ital Evidence* **2**(3), 1-28.

Ryan, J. Phil. (2018), Privacy and Inclusivity, *in* 'Proceedings of IEEE Games, Enter-tainment, Media Conference (GEM)', IEEE, pp. 1-9.

Sammons, John. (2010), *'The Basics of Digital Forensics - The Primer for Getting Started in Digital Forensics'*, 2nd Edition, Syngress Publications.

Santanam, Raghu., Sethumadhavan, M. and Virendra, Mohit. (2011), *'Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives'*, IGI Global, ISBN: 978-1609601232.

Shinder, Deb. (2010), 'Profiling and Categorizing Cyber Criminals'. http://www. TechRepublic.com/blog/it-security

Shirley, Crompton. and Jens, Jensen. (2018), Towards a Secure and GDPR-Compliant Fog-to-Cloud Platform, *in* 'Proceedings of IEEE/ACM International Conference on Utility and Cloud Computing Companion', Zurich, IEEE/ACM, pp. 296-301.

Shrivastava, G., Sharma, K., Khari, M. and Zohora, S. E. (2018), *Role of Cyber Security and Cyber Forensics in India. In Handbook of Research on Network Forensics and Analysis Techniques*, IGI Global, pp. 143-161.

Sikorski, Michael. (2012). *'Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software'*, Wiley Publications, ISBN: 9781593274313.

ISSN: 2582-6433

Smalley, S. (2001), Which operating system access control technique will provide the greatest over all benefit to users? *in* 'Proceedings of 6th ACM symposium on Access control models and Technologies', ACM, pp. 147-154.

Smalley, S., Fraser, T. and Vance, C. (2001), Linux Security Modules: General Secu-rity Hooks for Linux,*in* 'Proceedings of the 11th USENIX Security Symposium', San Francisco, California, pp. 1-3.

Smalley, S. and Loscocco, P. (2001), Integrating flexible support for security policies into the Linux operating system, *in* 'Proceedings of USENIX Annual Technical Con-ference'. USENIX, pp. 2-62.

Smalley, S. and Craig, R. (2013), Security Enhanced (SE) Android: Bringing Flexible MAC to Android, *in* 'Proceedings of NDSS Symposium 310', pp 20-38.

Smalley, S., Vance, C. and Salamon, W. (2001), 'Implementing SELinux as a Linux security module', *NAI Labs Report*, **1**(43), 5-58.

Smalley, S., and Fraser, T. (2001), 'A Security Policy Configuration for the Security-Enhanced Linux', *NAI Labs Technical Report*, pp. 3-20.

Stefan, D., Russo, A. J. and John, C. M. (2018), 'Flexible Dynamic Information Flow Control', *Journal of functional Programming* **46**(12), 1-12.

Stoll, Clifford. (2005), 'A Spy Through the Maze of Computer Espionage', *Gallery Books*,ISBN: 9781416507789.

Skendžić, A., Kovačić, B., and Tijan, E. (2018), General data protection regulation - Protection of personal data in an organization, *in* 'Proceedings of 41st International Convention on Information and Communication Technology, Electronics and Micro-electronics', IEEE, pp. 1370- 1375.

Szilvia, Varadi. (2016), 'Regulating European Clouds: The New European Data Protec-tion Framework', ch 2, *In handbook of Developing Interoperable and Federated Cloud Architecture*, IGI Global Publications, pp. 42-60.

Tennakoon, Hemamali. (2016), 'The need for a comprehensive methodology for profil-ing cyber-criminals', http://www.newsecuritylearning.com

Thomas, B. and H. Dieter. (2014). 'Information Flow control for workflow manage-ment system', *Journal of Information Technology* **56**(6), 294–299.

Tomoya, E. and Makoto, T. (2011), 'Purpose-Based Information Flow Control for Cy-ber Engineering', *IEEE Transactions on Industrial Electronics* **58**(6), 2216- 2225.

Tzanko, Tzolov. (2018), One Model for Implementation GDPR Based On ISO Stan-dards, *in*

ISSN: 2582-6433

'Proceedings of International Conference on Information Technologies', Varna, IEEE, pp. 1-3.

Vasiliki, Diamantopoulou., Aggeliki, Androutsopoulou., Gritzalis, S. and Charalabidis, Y. (2018), An assessment of privacy preservation in crowdsourcing approaches: To-wards GDPR compliance, *in* 'Proceedings of 12th International Conference on Re-search Challenges in Information Science', IEEE, pp. 1-9.

Victor, Castro. (2013), 'Roll your own Firewall with Netfilter', *Linux Journal* **2003**(10), 1-9.

Wang, Chundong., Lei, Yang., Guo, Hao. and Wan, Fujin. (2018), 'Data Protection and Provenance in Cloud of Things Environment: Research Challenges,' *International Journal of Information and Computer Security* **11**(4), 1-8.

Wang, Xiaolei. and Yang, Yuexiang. (2018), 'PrivacyContext: Identifying Malicious Mobile Privacy Leak Using Program Context,' *International Journal of Information and Computer Security* **10**(4), 562-584.

Walker, Cornell. (2009), 'Computer Forensics: Bringing the Evidence to court,' http: //www.infosecwriters.com, pp. 1-6.

Watson, R. N. M. (2007), 'Exploiting Concurrency Vulnerabilities in System Call Wrap-pers', USENIX, pp. 1-8.

Watson, R. N. M. (2010), 'ExtremeXOS Operating System', Datasheet. Oxford Uni-versity Press, pp. 1-21.

Wright, A., Cowan, C. and Morris, J., Greg, K. (2002), Linux security module frame-work, *in* 'Proceedings Of Ottawa Linux Symposium 8032', pp. 6-16.

Wright, A., Cowan, C., Smalley, S., Morris, James. and Greg, K. (2003), 'Linux Secu-rity Modules: General Security Support for the Linux Kernel', *Foundations of Intrusion Tolerant Systems* **2003**(8), 213-226.

Yang, Zhang. and Gao, Yang. (2010), The Realization of Digital Forensics Identifica-tion Workflow Audit and CustodySystem, *in* 'Proceedings of International Conference on Apperceiving Computing and Intelligence Analysis', IEEE, pp. 384-387.

Yanhui, Du. and Fu, Xue.(2014), Research of anti-phishing technology based on email extraction and analysis, *in* 'Proceedings of International Conference on Information Science and Cloud Computing Companion', IEEE, pp. 1-6.

Youssef, B., Charhi, Nada. Mannane. and Boubker, Regragui. (2019), 'Behavioral analysis approach for IDS based on attack pattern and risk assessment in cloud comput-ing', *International journal of Information and computer security* **11**(4/5), 315-331.

Yusoff, Yunus., Roslan, Ismail. and Zainuddin, Hassan. (2011), 'Common Phases of Computer

ISSN: 2582-6433

Forensics Investigation Models', *International Journal of Computer Science and Information Technology* **3**(3), 17-31.

Zhang, S., Meng,X. and Wang, L. (2016), 'An Adaptive Approach for Linux Mem-ory Analysis based on Kernel Code Reconstruction', *Eurasip Journal on Information Security* **2016**(14), 1-13.

LIST OF PUBLICATIONS

Asha, Joseph. and K. John, Singh. (2019), 'Crime Pattern Matching based on Process Execution Context – An Evidence Acquisition Technique', *Journal of Advanced Research in Dynamical and Control Systems* **11**(4), 202–211.

Asha, Joseph. and K. John, Singh. (2018), 'Real Time Detection of Phishing Attacks Using a Variant of Link Guard Algorithm', *Journal of Computational and Theoretical Nanoscience* **15**(11/12), 3303–3307.

Asha, Joseph. and K. John, Singh. (2020), 'Survey on IOT Security and Chal-leges of IoT Forensics', *Journal of Test Engineering and Management* **82**(1), 168–173.

Asha, Joseph. and K. John, Singh. (2018), 'Digital Forensics in Distributed Environment', *Handbook of Research on Network Forensics and Analysis Tech-niques', IGI Global Publications* **1**, 246–265.

Asha, Joseph. and K. John, Singh. (2019), 'Relation between cybercrime, cyber behavior, crime and Personality Disorders - A Perspective Review', *International Journal of Cyber Behavior, Psychology and Learning, IGI Global* (Under Re-view).

Asha, Joseph. and K. John, Singh. (2019), 'A GDPR Compliant Proposal to Provide Security in Android and iOS Devices', *in* 'Proceedings of International Conference on Emerging Trends in Information Technology and Engineering', *IEEE Xplore*, 978-1-7281-4141-1, 1–8.

Asha, Joseph. and K. John, Singh. (2016), 'Review of Digital Forensic Mod-els and A Proposal For Operating System Level Enhancements', *International Journal of Computer Science and Information Security* **14**(11), 797–806.

Asha, Joseph. and K. John, Singh. (2019), 'Egalitarian Stable Matching Al-gorithm for Resource Management in Cloud Computing systems', *International Journal of Information and Computer Security, Inderscience* (Accepted).

Asha, Joseph. and K. John, Singh. (2016), 'A Survey on Latest Trends and Challenges in Cyber Forensics', *International Journal of Advances in Electronics and Computer Science*, **Special Issue**(September), 75–78.

ISSN: 2582-6433

Asha, Joseph. and K. John, Singh. (2017), 'A Study on Digital Forensics in Mobile Devices', *International Journal of Electrical, Electronics and Data Com-munication* **5**(12), 13–16.

Asha, Joseph. and K. John, Singh. (2018), 'GDPR and Enterprise Mobile Device Management', *IEEE ComSoc Newsletter: Communication Technology* **1**(4), 5–5.

Asha, Joseph. and K. John, Singh. (2017), 'Provenance Based Digital Evidence Collection – Execution Context Approach over Information Flow Control', *In-ternational Journal of Advanced Studies in Computer Science and Engineering* **6**(9), 2–2.