C02047: Doctor of Philosophy
CRICOS Code: 00099F
Subject Code: 33875
December 2019

Machine Learning based Information Forensics from Smart Sources

Amber Umair

School of Electrical and Data Engineering
Faculty of Engg. & IT
University of Technology Sydney
NSW - 2007, Australia

Machine Learning based Information Forensics from Smart Sources

A thesis submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

in

Computer Systems

by

Amber Umair

to

School of Electrical and Data Engineering
Dr. Priyadarsi Nanda
University of Technology Sydney
NSW - 2007, Australia

December 2019

Abstract

We live in a world that connects, socializes and interacts using internet. Humans generate tons of information on daily basis, according to Forbes 2.5 quintillion bytes of data is created each day in year 2018. The data creation pace is continuously accelerating with the growth of the Internet of Things (IoT). Extensive social media usage fuels data creation which is primarily generated from mobile phones. In the present scenario, data is the asset and this asset is extremely vulnerable. In our research work we utilized these data sources to aid digital forensics investigation. Due to our technology engulfed lifestyle, we leave a lot of information about ourselves during our routine activities. These traces are used by the wrongdoers for their vicious objectives but also these traces can be used by investigators to understand any incident and to penalize the delinquents. Forensics investigators face challenges with a huge amount of data during investigations. Whether the data source is an online social network, a smart phone or an IOT based environment, huge amount of data adds complexity and delay to forensics investigation. To contribute to the forensics investigation we propose the use of machine learning for forensics data anaylsis. Forensics investigation is a three-phase process including data acquisition, data analysis and presentation. Our research focuses on the first two phases of the forensics investigation cycle i.e. data collection and data analysis. This thesis discusses following research achievements:

1. Data acquisition from smart sources for forensic information especially for IoT
2. Machine learning based data analysis to extract forensic artefacts
3. IoT forensics framework(acquisition and analysis phase) implementation

This thesis is segmented based on the three data sources for data analysis namely online social networks, smart phones and sensor-based networks (IoT). Using IoT based data this thesis proposes a scheme SACIFS(Smart aged care information forensics) for IoT forensic feature extraction and data analysis of elderly patients monitored in a nursing home environment. We developed our machine learning model based on Support Vector Machine to detect an incident and highlight relevant forensic artefacts. We used smart phone data in Digital Forensic Intelligence Analysis Cycle framework to identify strongly connected contacts during triage phase. We classified the contacts of a smart phone user with respect to their closeness, extracted from the data features from Facebook messenger. Moreover, utilizing publically available Online Social Network, we analysed multiple tools to collect, analyse and visualize data from Facebook pages and groups.

Author's declaration

I, *Amber Umair* declare that this thesis, submitted in partial fulfilment of the requirements for the award of Doctor of Philosophy, in the *School of Electrical and Data Engineering*, *Faculty of Engineering and Technology* at the University of Technology Sydney, Australia, is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis. This document has not been submitted for qualifications at any other academic institution. This research is supported by the Australian Government Research Training Program.

Production Note:

SIGNATURE: Signature removed prior to publication.

[Amber Umair]

DATE: 28th December, 2019

PLACE: Sydney, Australia

Dedication

To my beloved Parents, my loving Husband Umair and my kids Abdullah and Anabia
...

Acknowledgments

Foremost I would like to thank Allah, the sustainer, who kept me going through the highs and lows of this journey and made it achievable for me. He undoubtly is the source of light for me in every aspect of life.

I would like to express my deepest gratitude to my supervisor, Professor Priyadarsi Nanda for accepting me into the Phd. program and giving me the honor of being one of his research students. Prof. Nanda's guidance, patience, and continuous support were essential to the completion of this thesis and to my formation as a researcher. His unmatched knowledge and invaluable feedback immensely helped me go forward in my research. I am greatly indebted to him for helping me get through the difficult times I had during my research. I feel very lucky to have worked with Prof. Nanda without whom this thesis would have only been a dream. I would like to thank my Co-supervisor Professor Xiangjian He, who always provided his valueable and expert feedback on my work. His support, co-operation, and generosity thoughout the research tenure is truely undeniable.

I also wish to thank all of my colleagues and friends from the School of Electrical and Data Engineering at the University of Technology Sydney. Specifically, I would like to thank Upasana, Ashish, Annie, Amjad and Nisha for creating a friendly atmosphere in the group and assisting me in whatever manner possible. Many thanks to all the administrative staff at the School of Electrical and Data Engineering, especially Thomas, Eryani and Aprillia who helped me with administrative issues.I also acknowledge Chandranath Adak (UTS) for providing this thesis template to all HDR students and easing the thesis preparation procedure.

I am eternally grateful to my loving and supportive husband, lovely kids, beloved parents and parents in law for their sacrifices, prayers, encouragements, and endless love. Without their everyday support, I would have not been able to reach this stage. I sincerely dedicate this thesis to them. Words cannot express my gratitude and appreciation for their unwavering support and kindness throughout this journey.

List of Publications

Related to the Thesis :

1. Online Social Network Information Forensics Tools analysis and a survey of how cautious facbook users are.

   A. Umair, P. Nanda and X. He, "Online Social Network Information Forensics: A Survey on Use of Various Tools and Determining How Cautious Facebook Users are?," 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, 2017, pp. 1139-1144. doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.364

2. User Relationship Classication of Facebook Messenger Mobile Data using WEKA

   Umair A., Nanda P., He X., Choo KK.R. (2018) User Relationship Classification of Facebook Messenger Mobile Data using WEKA. In: Au M. et al. (eds) Network and System Security. NSS 2018. Lecture Notes in Computer Science, vol 11058. Springer, Cham

3. SACIFS: Smart Aged Care Information Forensics System using Machine-Learning (To be submitted to a suitable journal)

Table of Contents

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

1.1 Introduction

Technology take-up of humans in mobile usage, social media, smart care services and smart homes resulting in massive amount of data generated from these applications. This human generated data depicts many parts of their lives, events and personalities. When this data is analysed in an intelligent fashion, it reveals valuable information about not only the individuals but also about incidents that have happened around them. Our research is based on acquiring these different types of data from a number of sources and using intelligent algorithms to analyse this data to obtain more valuable information beyond the 1's and 0's. Therefore the core components of our research in this thesis are:

- Data from diverse sources [30, 118]
- Digital forensics [26, 114]
- Machine Learning [71]

Digital data forensics is the core of our research work. Data forensics, often used interchangeably with information forensics or computer forensics, is the study of digital data. How data is generated, collected and then used for the resolution of an investigation, is the question which we will be addressing. Information forensics is a branch of the bigger discipline of forensics, in which various types of evidence are examined to investigate an

alleged crime. Information forensics includes the data obtained not only from computers but also from mobile devices, social networks and now the prevailing internet of things (IoT) [95]. Data forensics process has three major phases including data acquisition, data analysis and data presentation. Our research focuses on the first two phases of the forensics investigation cycle, that is, data collection and data analysis. For data collection /extraction, we have used a variety of tools and techniques to obtain data from our data sources (OSN-199 instances, Mobile phones-instances and Sensors-52482 instenaces). We used these three data sources because the digital forensics research work in these dimensions is still scarce and needs prompt attention. For data analysis, we have utilized the strength of machine learning algorithms. Machine learning is a specific subset of AI (Artificial intelligence) [35] that trains a machine how to learn from data. It is a method for machines to learn from data. Machine learning models look for patterns in data and try to derive conclusions like human beings. Machine learning models need granular data, it thrives on huge data volumes and it needs very diverse sources of data to be able to find the pattern and learn for future usage. As of the writing of this thesis, we have used three diverse data sources and their data separately; each part covered in a separate chapter. However, in future data from multiple sources can be combined, analysed together to yield more accurate conclusions. The combination of digital forensics and machine learning have the potential to succeed which can benefit the humans of the information age. Machine learning has been used mostly in the image analysis based forensics. However, our proposed method of using machine learning for analysis of textual form of data to contribute towards the forensics artefacts collection is a novel approach. This thesis addresses the following research topics:

1. Acquisition of data from smart sources for information forensic as presently there is not any practical mechanism/framework available for IoT forensics

2. Analysis of acquired data using machine learning to obtain forensic artefacts

3. Practical implementation of IoT forensics framework(acquisition and analysis phase)

Our research work contributes by proposing and implementing a novel aspect of information forensics, which can benefit from the strength of machine learning. Our proposed application of a machine learning model by using the mobile and sensor based data shows promising results. In the proceeding sections, we will discuss the core components of our research in detail.

1.2 Research Core Components:

This sections details the primary parts of our research work and the overall system architecture. We will also explain how the apparently disjoint parts of our research work actually aim towards a common goal of obtaining forensics artefacts to aid in any investigation.

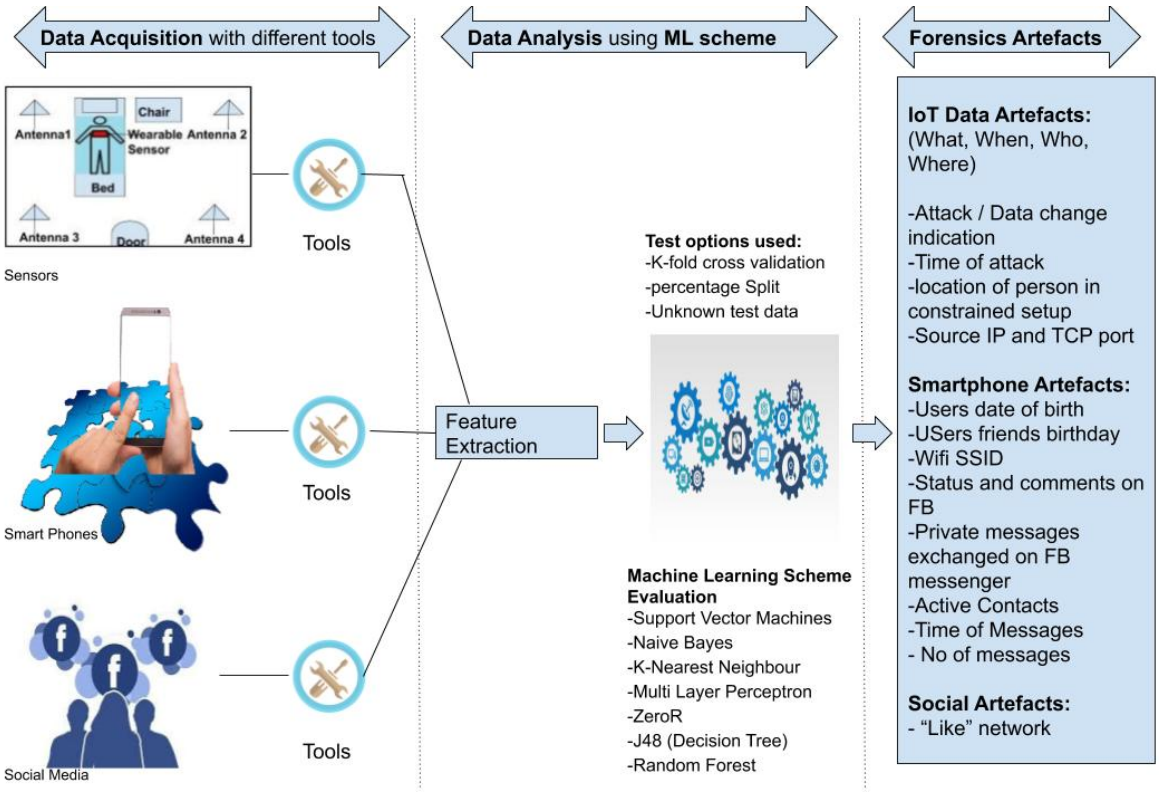

Figure 1.1: Research Core Components

We will explain the research core components in three main sections:

- Data Acquisition methods
- Data Analysis using machine learning schemes
- Forensics Artefacts

1.2.1 Data Acquisition methods

Internet of things (IoT) - Sensor data

Internet of things in a small low complexity sensor based system is defined by IEEE[51]

as: "An IoT is a network that connects uniquely identifiable "Things" to the Internet. The "Things" have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the "Thing" can be collected and the state of the "Thing" can be changed from anywhere, anytime, by anything. To perform forensic analysis on IoT sensor data, we obtained sensor based Smart Aged care Environment data set from UCI Machine Learning Repository[75]. In this work authors presented and evaluated this novel method for mitigating the high falls risk[108] associated with bed exits based on using an economical, privacy preserving and passive sensor enabled RFID[115] device. This dataset contains motion data of 14 healthy older aged participants between 66 and 86 years old, performing broadly scripted activities using a battery less, wearable sensor on top of their clothing at sternum level. The setting of S1 (Room1) uses four RFID reader antennas around the room (one on ceiling level, and 3 on wall level) for the collection of data. The participants are monitored for the routine activities like walking to the chair, sitting on the chair, getting off the chair, walking to the bed, lying on the bed, getting off the bed and walking to the door. Hence the possible class labels assigned for every sensor observation are

- Sitting on bed
- Sitting on chair
- Lying on bed
- Ambulating, where ambulating includes standing, walking around the room.

Our research work contributes by utilizing this data, to make a smart care scenario suitable for forensics analysis. By mimicking a smart aged care environment, we want to work around the possibility of an attack or unauthorized change in the human activity data or smart health care data. Now from the forensics perspective we want to answer some questions that can be extracted from the data analysis. Therefore, we have added extended attributes to the existing data, to make the scenario suitable for forensics analysis and to be useful to serve for investigation aspects. The existing attributes in the data set are:

1. Time in seconds
2. Acceleration reading in G for frontal axis
3. Acceleration reading in G for vertical axis

4. Acceleration reading in G for lateral axis
5. Id of antenna reading sensor
6. Received signal strength indicator (RSSI)
7. Phase
8. Frequency
9. Label of activity(1: sit on bed, 2: sit on chair, 3: lying, 4: ambulating)

while the extended attributes for our research are:

1. Status (changed or unchanged or Malicious/Benign)
2. Source IP
3. Source Port
4. Destination IP
5. Destination Port
6. Sequence Number
7. Acknowledgement Number

This thesis contributes by using sensor data for validating the capability of support vector machine algorithm to predict data alteration, even with less number of features (attributes). Our proposed model gives forensics capability in IoT based environments, by highlighting suspicious instances and their relevant details. Moreover, our proposed SVM based model is favourable to resource-constrained systems (like IoT) as it performed well with less features. More details of this work are discussed in chapter 5, SACIFS: Smart Aged Care Information Forensics System using Machine Learning.

Smart Phone Data

Smart phone forensic analysis is carried out by creating two testbeds using android and iOS phones. Root access is obtained on the android phone to make physical copy of the phone's memory while for an IoS device (IPhone) data is obtained from the phone's backup image. Tools used to acquire data from smart phones for data analysis are as

follows:

Tools For Android Phone Data Acquisition:

- FTK access data FTK Imager 3.1.2.0
- Firefox SQLite manager
- One Root
- Root Checker
- ADB Android Debug Bridge Android Studio 2.3.2.

Tools For iOS Phone Data Acquisition::

- IPhone 6(iTunes version 12.0.1.26)
- IPhone Analyzer 2.1.70.

Our smart phone data based research highlights the importance of identifying strongly connected contacts of the device owner during a triage phase. This is because identification of the close contacts (leads) helps an investigation to rapidly progress in the right direction. We have classified the contacts of a smart phone user with respect to their relationship strength (closeness), which we extracted from the data features from Facebook messenger application in our case studies. In order to determine certain contact's relationship strength or contact's messaging frequency, we have given weight to the number and time of messages exchanged with that contact. This smart phone based case study contributed towards the forensic triage of mobile devices by classifying owner's contact into weak, medium and strong communication frequency. (i.e. determining their mutual relationship strength) using machine learning algorithms. More details of this part of our research is covered in chapter 4, Machine Learning Based Relationship Classification and Forensics Analysis .

Online Social Media Data

By using social media as a data source, we have evaluated various tools to collect, analyse and visualize data obtained from Facebook. The tools are selected based on retrieved data quality, data access feasibility and analysis. In this part of our preliminary work, we have reviewed the research work in the area of online social network information

forensics and its correlation with other types of data sources. We also conducted an online survey to understand and analyse the Facebook usage by people and their attentiveness towards the security challenges imposed on their privacy due to publicly sharing personal information. In this review study, we analysed the below mentioned tools:

- Social Snapshot
- Netvizz
- Nvivo Pro with Ncapture
- Gephi

We analysed these tools for their ability to gather social networks data to extract meaningful features. However, there are limitations attached with every tool in terms of varying format of results, inevitable changes in online social networks APIs (Facebook Graph API). Moreover, some tools actually need authorization information to work in the desired manner. We have discussed this preliminary part of our work in chapter 3.

Data Analysis Using Machine Learning Schemes

Application of machine learning algorithms to the giant pool of data gathered from the diverse data sources could accelerate the process of forensics artefacts discovery. Prevailing machine-learning methods offer novel ways to extract decisive forensic meaning from the raw chunks of data. In our thesis, we have evaluated many machine learning algorithms and techniques to find the best way to answer our forensics questions. We have applied automatic feature selection on our datasets by using different evaluators and search algorithms. Feature Selection aids in selecting only important features, which actually contribute most to the desired output. If feature selection phase is ignored, irrelevant features in the data can decrease the accuracy of the models and make the model learn based on irrelevant features. For our data analysis using different problem scenarios and datasets, we have analysed multiple machine learning schemes. Different schemes work better in a scenario and underperform in another scenario. Therefore, we evaluate the popular schemes to find out the one that best suits our data. The schemes used in our research work are as follows:

- Support Vector Machine
- Decision Tree (J48)

- Naive Bayes
- K-Nearest Neighbours (KNN)
- Random Forest
- ZeroR

Forensics Artefacts

This thesis discusses the variety of forensics artefacts obtained from different research scenarios and diverse data sources. The details are available in chapter 3, 4 and 5. By using the attributes of sensor-based data in a smart aged care environment, we extracted the following artefacts:

- Activity data deviation (What happened?)
- Time of incident (When the incident happened?)
- Source IP and TCP port (Who, which antenna was used in the incident?)
- Location of person in a constrained environment (Where was the victim when the incident happened?)

With the smartphone data in our android and iOS based case studies the artefacts obtained are:

- Users date of birth
- Users friends birthday
- Wifi SSID(Service Set Identifier)
- Status and comments on FB
- Private messages exchanged on FB messenger
- Active contacts
- Time of messages
- No of messages

While using our preliminary review research work and survey, our findings included the Like-network within the Facebook pages and groups. Moreover, the survey resulted in an insight about Facebook usage by people and their attentiveness towards the security challenges imposed on their privacy.

1.2.2 Research Work Scope:

Our research work is based on a variety of research sources and concepts. Due to this diversity and vastness of our research constituents, it is crucial to define the blurring boundaries of our work. We have detailed our "in-scope" research goals, and have mentioned the scope exclusions.

What is IN our research Scope?

- Information acquisition from unconventional sources.
- Information analysis with ML algorithms to obtain forensics artefacts
- Incident(attack / anomaly) indication
- Analysis and comparison of ML algorithms which perform better with our research data
- Feature extraction

What is OUT of our research Scope?

- Human activity detection
- Human activity recognition

1.2.3 Research Challenges and Contribution:

With the rise of big data resulting from technology exposure, the opportunities for enterprises are increasing, but data security breaches inevitably arise because of the ever-growing data volumes. For the same reason, information forensics face challenges in analysing huge data for investigation. Moreover, data breach incidents will become more damaging, especially when the targeted data is health related or compromises the

privacy of individuals.

Scalability Challenge: the ability to process large data content, for example, megabytes to terabytes, and to be deployed in distributed environments. Scalability is the key to efficiently processing massive amounts of data. By utilizing the power of machine learning algorithms, we have proposed a scalable solution, which can reduce the data processing delay and achieve quick data breach detection.

Accuracy challenge: achieving low false negative/positive rates for the detection is another challenge for IoT, mobile and social network forensics. Our proposed solution contributes by achieving promisingly accurate results in identifying a change in data (IoT data) and in identifying close contacts (Mobile data). Our thesis investigates on the following research questions:

- How human generated data on social networks, mobile phones and IoT can be used to extract forensics artefacts?
- How Facebook messenger data can help in an investigation by identifying the closeness of the phone owner to his /her contacts?
- Propose a machine learning based model to identify change in the smart care data and highlight the relevant artefacts.

1.2.4 Thesis Organisation:

This thesis is organised as follows:

Chapter 1 introduces our information forensics based research work. It highlights the challenges of digital data forensics and motivations for our work. It also details the overall architecture of our research concept. This chapter also provides an overview of the key components on which our research focuses. The data acquisition and analysis methodology is defined. Finally, the research challenges and our research contributions are presented.

Chapter 2 provides the literature review about digital forensics, the data acquisition techniques and associated challenges. This chapter also details the use of machine learning in the forensics field.

Chapter 3 details our preliminary research work for online social media. We have reviewed multiple social media applications for data acquisition and analysis. This chapter also details the results of a survey conducted to understand the awareness of Facebook users and their security sensitivity.

Chapter 4 explains the research work we have accomplished on mobile data. It discusses the two case studies based on android and iOS mobile phones. This chapter explains how we have used machine-learning analysis to simplify and speed-up the triage phase of information forensics.

Chapter 5 reports on our sensor based research work. It explains the smart aged care scenario and the security challenges to such IoT based environments. Evaluation of multiple machine learning algorithms is discussed. Moreover, our proposed model based on Support vector machine is explained.

Chapter 6 provides our preliminary data analysis with deep learning multi layer perceptron using the data set used in chapter 4 for classifying a users contact with respect to the frequency of conversations.

Chapter 7 concludes the thesis and also provides future directions.

CHAPTER 2

LITERATURE REVIEW

Digital forensics is a branch of the information security domain, which applies scientific investigatory procedures to digital misconduct and attacks. It encompasses many processes to uncover and then interpret data in electronic form. Mostly this term is applied to digital crimes only but technology and electronic devices are part of the daily routine. Digital forensics plays a vital role in incidents, which are not exactly technological. With the rise of technology, humans, their technological possessions like phones, smart watches, fitness devices and smart homes, produce a huge amount of data. This increasing volume of data has been highlighted as a challenge for digital forensics over many years [42, 90, 93]. Whilst this raises problems for government agencies and private sector organisations that have not met the demand for service there are positive aspects to the prevalent nature of technology. One affirmation is that with the increasing volume, variation, velocity, and accuracy of information available, this can enable investigators to have a better insight into the criminal environment, and support with informed verdicts[92]. Our research focus in this thesis is also on obtaining information intelligence from these diverse sources to contribute to information forensics. We foresee that by combining and correlating disparate artefacts, effective inferences are achievable.

The avenues of evidence collection for digital forensics involve social media, digital devices and now prevalent smart environments (Internet of things IoT), which are sensor based. In Internet of Things (IoT) pervasive, linked, and smart nodes cooperate autonomously to offer a number of services. Extensive dissemination, openness and relatively high processing power of IoT objects make them a perfect target for cyber-attacks.

Moreover, as IoT nodes collect and process private information, they serve as a goldmine of data for wrongdoers. Especially deployment of smart care environments that sense people's private information (such as health data or movement data) pose a new level of risk to privacy of individuals. Moreover, the sheer volume of data generated as a result of heterogeneous IoT environments, make it close to impossible to provide an end-to-end analysis of digital evidence[33, 118]. Therefore, security and specifically the ability to detect compromised nodes or data, together with collecting and preserving evidence of an attack emerge as a priority in successful deployment of IoT networks. However, attribution of malicious activities detected in an IoT environment is quite challenging in the absence of a reliable, forensics capable and secure architecture that assures a forensically sound logging, monitoring and analysing system.In this thesis, we have also analysed data from sensor based healthcare environment, to detect suspicious change of data and relevant artefacts by training our model on the normal values of human activity in a constrained environment. Authors in research[14, 15] highlight social media information forensics as a new frontier in digital forensics. Authors state that in 2018, 3.196 billion users were reported to be engaged in sharing their everyday activities on social media sites. Moreover, the information available on social media websites, about an individual, their actions, and contacts is used occasionally as a possible tool by investigators to backtrack a crime. The volatile progress of Online Social Networks (OSNs) usage in the last years has produced easy accessibility to personal data. This richness of information, combined with the capability to identify users' communication patterns, could be used in information forensics based on social network analysis to identify users' behaviour for a variety of tasks, such as general cybersecurity and incident response mechanisms.

Online social network data can give excellent support to investigators in the criminal investigation process if explored accurately. OSNs serve as a dynamic and new subset of data sources, created by people, like text posts, friend lists, images, geo-location data, videos, demographic information and so forth[15]. Moreover, the metadata (data about data) and associated network data hold sufficient potential to assist in criminal investigations.

Researchers[6] have used online social network data to understand new patterns of users' interaction, which gives a significant contribution to the recognition of malicious users in the context of OSNs. [28, 55] suggest a rapid preliminary investigative screening phase, namely Forensic Triage for digital forensics investigators when they encounter immense amount of data in any investigation. Digital forensic triage is "a process of

sorting enquiries into groups based on the need for or likely benefit from examination"[86]. In this approach greater use of limited resources is achieved [100]. Digital triage assists with the issue of voluminous data by identifying which items can potentially lead to an item of evidence. In the context of our research study, the purpose of the triage process is to quickly identify which elements from a group are likely to contain evidence, such as a rapid examination by an experienced practitioner to determine which item may contain evidence. In our research context, triage is not used for accepting or rejecting the artefact; instead, it is used for determining its importance relevant to the presented scenario[90]. We have used mobile phone Face book messenger based data and machine learning to assist in triaging and finding the important leads for a case.

Smart devices also provide a very large amount of information about their owners' interests and behaviours. Presently, it is a legal requirement in a considerable number of serious crime investigations to seize and inspect the digital devices of victims and suspects. This is because everyone uses a phone, iPad or tablet device for his or her day-to-day work or communication needs. The data on these portable devices is very helpful in finding traces of crime. Detailed timestamped trail or history of digital activities, performed by the user, can be obtained and analysed. The current digital examination procedures include the analysis of social media profiles of suspects and victims, due to the ease of access and richness of information available on them. However, the inclusion of social network sources as an artefact source in investigative analysis creates a very large load for digital forensics analysts. Their job becomes challenging owing to massive volumes of data created by the proliferation and wide-ranging participation of individuals in online communications[15].

Forensic Analysis is a time intensive and multi-dimensional phase in the digital forensic process, which needs proficient automation techniques. To aid in automating the forensics process we have used machine learning in our research and we foresee that AI and machine learning have sound potential in this field. Forensics analysis involves the integration and correlation of extracted artefacts to get a comprehensive evidence. However, the unavailability of heuristic correlation among extracted data limits the ability to investigate other sources of publicly available information, such as close friends, spouse, co-workers, and relatives[15].

This intensive volume of data and extensive availability of data has led to many new domains which facilitate decision-making processes based on the rules learned from data. One of the flourishing domains with the propagation of big data is data science. [11] defines data science as "It is the science and art of using computational

methods to identify and discover influential patterns in data". The objective of Data Science is to achieve detailed insight from data and to enhance decisions to make them more dependable[7]. Data Science utilizes historic data and its trends on different times . However, the data used in Data Science can be collected over a period of a few years or just over a period of a few milliseconds.It can be an on-going process or just a one-off process. Consequently, Data Science computations can be performed on real-time or near real-time data collection. Data science is a superset for data mining and machine learning. Data mining is used to obtain rules from historic data, while machine learning teaches the computers to understand those rules driven from data mining techniques. Spafford (as cited in Palmer, 2001) mentioned data mining as a field of specialty which can contribute to digital forensic analysis. Beebe (2009) also mentioned that using data mining techniques can be another solution to the data volume challenge faced by investigators. Beebe also stated that data mining has the strength to locate trends and information from analysing data that may otherwise be hidden to human observation. Many researchers have explored machine learning capabilities for detection of intrusions or threats[49]. There is an increasing inclination of using data mining and machine learning detection methods, e.g. support vector machine (SVM), artificial neural network (ANN), and cluster analysis[57]. Abundant researches demonstrated that big data and machine learning can be used to improve the DDOS intrusion detection system [54, 82, 83, 102]. We have used machine learning to deduce forensic artefacts, which makes our research, novel and promising. In [70] proposed a triage approach that aims to automatically categorize digital media on the basis of possible connections between extracted traces from digital evidence and the criminal cases under investigation. The authors have discussed two case studies about copyright infringement and child pornography to verify that use of machine learning is practicable in digital forensics. They did a benchmark study using the most popular mining algorithms (i.e. Bayes Networks, Decision Trees, Locally Weighted Learning and Support Vector Machines) to discover the ones that best fit the problem under consideration. Promising results were obtained by triaging a data set of 13 digital media and 45 copyright infringement-related features. By using Bayes Networks or Support Vector Machines more than 93% correct classification was achieved. While in the child pornography exchange case, a dataset of 23 cell phones and 23 crime-related features, correct classification of 100% of the phones was achieved.

Machine learning use for digital forensics is promising to support traditional digital forensics techniques by speeding-up the identification of credible connections among

suspicious behaviours and electronic device usage method on a commonality basis that, if done manually, would be a laborious activity.

In [70] the authors discussed CBR (case based reasoning) as an artificial intelligence paradigm of problem solving and learning by experience. The authors proposed a system capable to extract features by using information extraction (IE) techniques from the existing autopsy reports. The system also analyses the case similarities by coupling the CBR technique with a Naive Bayes learner for feature-weights learning and finally it produces an outcome recommendation. Authors reveal that the CBR method with the implementation of a machine learner is indeed a viable alternative method to the forensic methods, with practical advantages. This machine learning based CBR system solves new problems by reclaiming solutions of old cases deposited in a case knowledgebase.

A number of researchers have used machine learning algorithms and tools for attack detection using the widely available datasets. One of the very famous datasets used for training and testing of the models is the intrusion dataset from On-Line System - Knowledge Discovery Data mining (NSL-KDD). [49] reflects on the performance of different learning models in detecting distributed denial of service (DDoS) attack. Authors have also explained how any change in the parameters results in the change of performance of the machine learning models. Algorithms were implemented using open source tools namely H20 and Weka (Waikato Environment for Knowledge Analysis) and a comparison of the accuracy of the algorithms in detecting DDoS attacks was carried out. Naive Bayes, Gradient Boosting Machine and Distributed Random Forest were concluded to be the most successful models for DDoS detection due to their high accuracy and short time taken for training. Authors further examined Gradient Boosting Machine and Distributed Random Forest parameters to improve accuracy. But they have not explored support vector machine (SVM) for the same purpose although SVM has been widely used for intrusion detection by research community. In [TLR 13] have discussed a botnet taxonomy and reviewed SVM and its variations as promising Botnet detection techniques.

With the prevailing use of IOT[68], now machine learning is widely used in various aspects to make the experience more user friendly and secure. However, IOT has numerous associated security challenges. Botnets are one of the major concerns associated with IOT. In [61] authors discuss the role of machine learning techniques for recognizing and examining botnets. Authors have examined four ML techniques of Decision Tree (DT), Artificial Neural Network (ANN), Naive Bayes (NB) on the USNW-NB15 data set. Their assessment of the accuracy and false alarm rate of the techniques revealed the

superiority of the decision tree in botnet detection.

Another serious security challenge on a global scale aggravated by IOT is Advanced Persistent Threats (APT) [74]. The accurate detection and prediction of APT is an ongoing concern[13]. In [43] authors proposes a novel machine learning-based system entitled MLAPT, which can detect and predict APT attacks in a methodical manner. Authors define MLAPT in three major stages: (1) Threat detection, in which different methods detect diverse practices used during the several APT phases. (2) Alert correlation, a correlation framework to link the output of the detection methods, to generate alert for an APT scenario; and (3) Attack prediction, which utilizes machine learning-based prediction to determine the probability of the early alerts to develop into a complete APT attack. MLAPT is able to predict APT in its early steps with a prediction accuracy of 84.8%.

Machine learning has the prospective to transform how digital forensic investigators and scientists evaluate electronic evidence and other forms of evidence. Number of researchers are using machine-learning methods in forensic applications with impressive results. The research community agrees that none of the algorithms can completely substitute for human intervention for the analysis and explanation of evidence. However, with the rise of big data and IoT, backed by voluminous data, augmented with extensive testing and validation, these algorithms can help in eliminating most of the subjectivity that pervades most forensic disciplines and can assist in approximation of the degree of indecision in forensic conclusions.

Our research work is motivated by the above mentioned promising performance of machine learning algorithms in various domains of information security. Also the abundance of data from diverse sources and its utilisation to get significant digital artefacts is also one of our objectives. Core combination of our research work areas, which include machine learning and unconventional data sources, makes our work interesting, unique and futuristic. Artificial intelligence is making its mark in many industries and we perceive a resilient and indisputable future for AI in the information forensics discipline.

CHAPTER 3

Digital social information dissemination and analysis

Online social networks have become utilities like electricity, water and gas. People extensively use / misuse them. Terabytes of unstructured data are generated daily by the users on social networks. This propagation of private information often leads to disastrous results. However, this information can also be used by Law enforcing agencies as an aid to reach, cease and prosecute criminals. Social network information analysis / forensics is proving its role in digital forensics but still a lot of milestones need to be achieved. This chapter discusses and compares the tools available for acquisition and analysis of social network data (Facebook) and combining the pieces of information to get an understanding of the big picture. Research on the tools to obtain and analyse Online Social Network (OSN) information is still at the infancy stage. The challenges include the ever-changing nature of social networks format (APIs). Moreover the data size makes feature extraction difficult. The data gathering process could not be fully automated and requires manual intervention to obtain relevant data. The contributions of this chapter include:

- Analysis of various tools to collect, analyse and visualize data obtained from Facebook. Tools are selected on the basis of retrieved data quality, data access feasibility and analysis.
- Study and discuss the research done in the area of online social network information forensics and its correlation with other types of data sources (e.g. Smart phone

sensor signals).

- Conduct an online survey to understand and analyse the Facebook usage by people and their attentiveness towards the security challenges imposed on their privacy.

The contribution of this chapter has been presented in [110]. The outline of this chapter is as follows:

Section 3.1 provides the background of using OSN information for forensics purpose.

Section 3.2 overviews and analyses the functionality of Facebook data tools.

Section 3.3 discusses the tools to obtain and compare OSN information as an artefact.

Section 3.4 discusses the findings of our online survey.

Section 3.5 concludes the chapter and discusses future scope.

3.1 Background

In recent years, use of technology for socializing has increased a lot. Relatives living across the globe, friends from the school, past and present office colleague are all just a click away. Moreover, now these clicks are generated from disparate sources / devices. A typical computer is no more the origin of this type of communication. Now the origin varies from a laptop, IPad, Tab, Mobile phone (iOS, Android), smart watch and health monitoring device (e.g. FITBIT). Although use of such varying devices to socialize has increased, usually users are unaware of the device configurations/ settings to avoid dissemination of unnecessary information about them. Even they do not realize the serious implications of such ignorant information propagation. Socializing over the web via online social networks, blogging, and emails can reveal a lot of information about an individual. Social information dissemination could help in understanding important information about an individual. Such information could be used by criminals to harm someone or to plan any harmful activity. Three information aspects about an individual which could be identified by social information are:

- Relationship Strength (Weak or Strong tie)
- Type of relationship

- Predicted behavior / characteristics of an individual

Nowadays, Facebook plays an important part in the lives of the majority of individuals. People post, like and share a great deal about themselves on Facebook. By observing the type of information shared by an individual, analyzing his / her joined groups, a lot of information could be inferred about them. For example, the strength of a relationship between two individuals user A and user B and their corresponding contacts can be estimated. The number of tags / picture sharing, similar subscribed groups and number of likes to one another's post can help in guessing the relationship strength[44, 116].This relationship strength can be demonstrated by the following equation:

$$RelationshipStrength = No.of likes from user A to B / Total no.of likes by A \quad (3.1)$$

User profiling on the basis of tags and joined groups support the theory of homophiles in social networks [8], which suggests that users with similar interest are more likely to form social connections[72]. However, in some cases users socially influence each other's behavior and they become similar over time [9]. From a forensics perspective, text mining on social networks data could also provide useful results, because topical similarity (words used by users in tags and statuses) can help in social link/relationship prediction [9]. Mining or searching for certain keywords used in the body of emails can help in extracting the type of relationship between the sender and recipient (e.g. manager and subordinate relationship). Two types of relationship ranking approaches could be used:

- Traffic Based Relationship Ranking: The sender and recipient details of captured emails can reveal the organizational structure [38]. From a forensics perspective, emails propagated from a certain email id (employee) to any non-relevant id (like not manager or peer) or external id could be marked as suspicious. Moreover, search pattern of an employee and social media usage could assist to detect a traitor for an inside attack detection[103].

- Content Based Relationship Ranking: By filtering the emails with certain keywords in the email content can also help in understanding the relationship between the sender and recipients.

Similarity of one individual with another or with a group of people can be predicted on the basis of browsed information, visited pages and joined groups. Email communication

can also help in identifying the similar characteristics and relationship strength between two or more users. For example, if a user A sends more emails to User B than User C, it is more likely that user A and user B have a stronger relationship than user A and user C [106] at a specific time; see Figure 3.1. This relationship strength could also be because of certain characteristics, shared interests, or similar age /demographics.

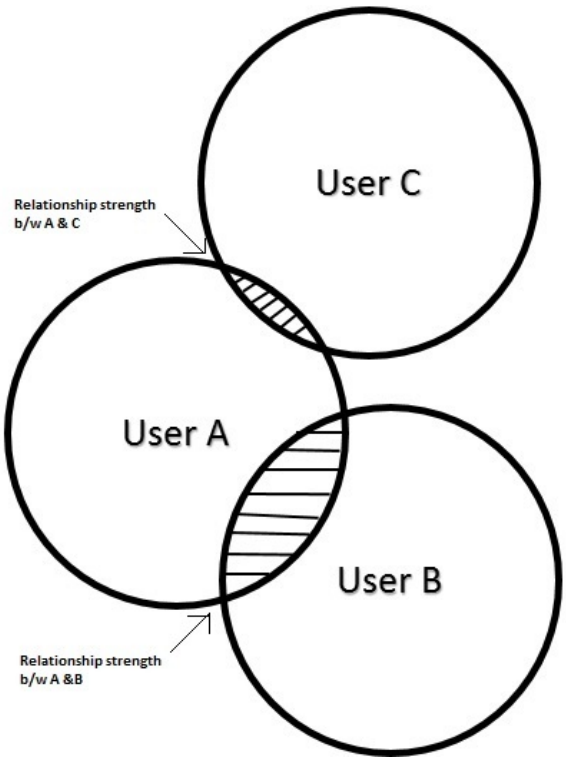

Figure 3.1: Relationship Strength Between Users On The Basis Of Emails Exchanged.

3.2 Online Social Network Tools Analysis

This section discusses and compares various tools to gather social networks data and analyse gathered data to provide some meaningful feature. There are constraints/limitations attached with every tool and every tool has varying format of results. Another challenge for the OSN information gathering tool is the inevitable changes in Facebook Graph API. These changes are made to secure the privacy of users but it often ends up either limiting functioning of the Apps / programs or makes them totally unusable. This section discusses the research done on social networks. It also compares the features and

functionality of the available tools which can be used to gain a variety of information from OSNs.

3.2.0.1 Social Snapshot Framework

Online Social Snapshot[50] is comprised of 3 parts.

1. Social Snap Shot Client.
2. Automated Browser to add the snapshot client to the target user's profile.
3. Third Party snapshot application.

Design: Due to the diversity of information available via OSNs, researchers in [50] propose a twofold approach: an automated web-browser in combination with a custom third-party application. The social snapshot application is initialized with a user's credentials or authentication cookie. In the following, a custom third-party application is temporarily added to the target account. This application fetches the user's data, pictures, friend list, communication, and more. Information that is unavailable through the third-party application is finally gathered using traditional web-crawling techniques[40]. By automating a standard web-browser and avoiding aggressive web-crawling, social snapshot simulates the behavior of a human OSN user, thus minimizing the risk of being blocked by the social networking site.

Depth of information collection:

Figure 3.2 shows an example of a social snapshot with depth = 2. For a given user, all of her friends are first fetched, followed by the friend's photos. The single path for photos of the friend's user illustrates the magnitude of available paths and thus data. Defining a specific social snapshot depth enables us to limit the amount of fetched data. The amount of data grows exponentially with social snapshot depth.

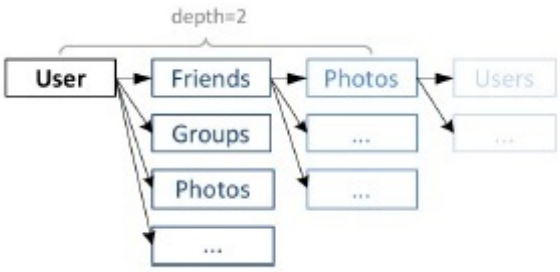

Figure 3.2: Example For Elements Fetched With Social Snapshot Of Depth=2. [50]

Social Snapshot introduced novel techniques to efficiently gather data from online social networks that may be used as criminal evidence. It gathered detailed data and made it feasible to link online evidence to traditional forensic artefacts. A prototype application for Facebook data collection was also developed and was shared as an open-source license for other researchers and helped significantly in Facebook data collection until the changes in Facebook API on April 2015.

3.2.0.2 Automated Identity Theft on OSN

Automated Identity theft on online social network is also possible with almost no manual / human intervention. This phenomenon has been explained by [19] in their prototype system which automates the identity theft process for four social network sites including Facebook and LinkedIn. There are two main concepts of this approach:

- Profile crawling: a target is selected and his/her profile is crawled on OSN1 (e.g. Facebook) to get maximum information about him/her and respective contacts.
- Profile Cloning: The existence of target ID is checked on other social networks OSN2 (e.g. LinkedIn). If the ID is not present on that OSN2 a clone ID is made containing same information which was obtained from the OSN. Request is sent to connect to the contacts of target ID, which is usually accepted by the contacts assuming that the same person is now on this new network and now wants to be connected.

There are five (5) components of this system:

- Profile Crawler: This component collects information of the individuals with public profiles.
- Identity Matcher: This component looks for the target individual's user id existence on other social networks. For example, If user A is present on Facebook, does A also has a profile on Linked In or Twitter?
- Profile Creator - This component creates a clone ID of the target Individual on the different network where he/ she was not present previously. It uses the same information (Profile picture, age, education etc.) for his/her profile obtained via the crawler module.
- Message Sender- this module sends the connection request to the contacts of target individual (which were obtained from the crawler module); usually people accept

the request without any suspicion as the similar picture and details of the requester are used.

- Captcha Analyser- is used to break the Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) of corresponding OSN site. Every site has a different captcha mechanism and requires different methods to break them. The crack of LinkedIn CAPTCHA [9] has not been achieved.

3.2.0.3 Netvizz V1.41

Netvizz is a research purpose tool that gets information from Facebook for in-depth analysis. However, its functionality is limited to Facebook pages and groups only. The limitations of this tool are that it is only a Facebook page and group specific and does not provide information about a user's profile[98]. Another limitation is that the target group should be an open group; closed group data could not be retrieved even if the logged in user is a member of the closed group. We have extracted the data for analysis from different open groups on Facebook. Most of these groups are used for buying and selling goods online. The following modules are currently available and are able to extract information:
Group data Module- creates networks and tabular files for user activity around posts on groups
Page data Module- creates networks and tabular files for user activity around posts on pages
Page like network Module- creates a network of pages connected through the "likes" between them
Page timeline images Module - creates a list of all images from the "Timeline Photos" album on pages
Search Module- interface to Facebook's search function
Link stats Module - provides statistics for links shared on Facebook

The data is extracted in gdf format (a simple text format that specifies a graph) as well as statistical files using a tab-separated format. That can easily be changed from TSV to CSV. These files can then be analyzed and visualized using graph visualization software such as gephi (https://gephi.org/). We have shown the page-like-network of an Open Facebook Page which sells baby products and connects with pages that are in a similar business. Data is gathered using Netvizz Page Module and visualization is

generated with the help of gephi, shown in Figure. 3.3:

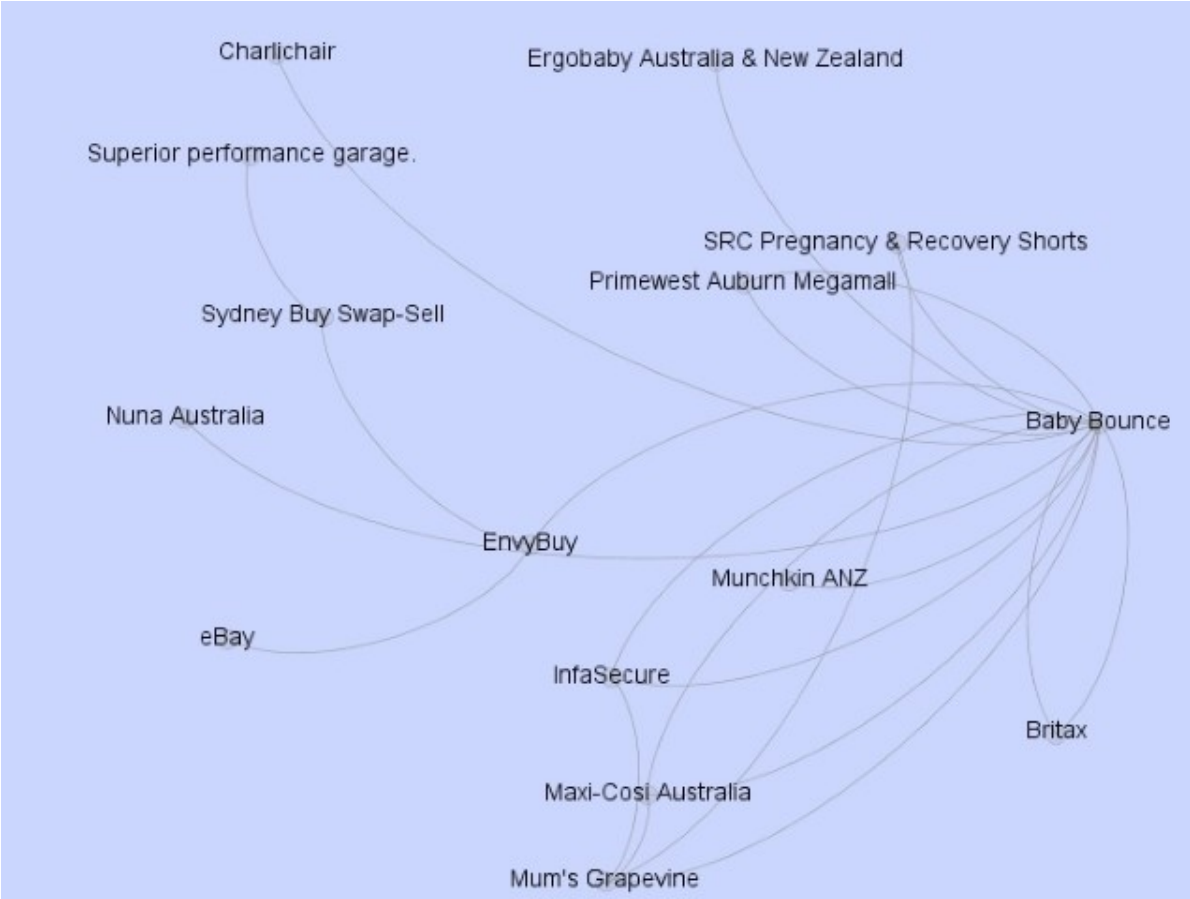

Figure 3.3: Page Like Network By Gephi.

3.2.0.4 NVivo 11 Pro with N capture addon for chrome

NVivo 11 Pro analyses and gives in-depth insight in qualitative and mixed method research[22]. This tool is an additional point for digital forensics because the digital evidence is scattered, unstructured and of various formats. Nvivo can gather and analyse data from popular social networks (Facebook, LinkedIn & Twitter); it also helps in discovering the hidden connections which are impossible to find manually [88].
NCapture is a web browser extension, to capture content like web pages, online PDFs and social media for analysis in NVivo 10 for Windows, NVivo 11 Pro for Windows and NVivo 11 Plus for Windows[89]. NCapture extension gathers web pages and online PDFs. It can gather the signed in user's Facebook wall posts and comments, it also gathers the wall posts and comments from people, organizations or groups. Then it imports them

into NVivo as a dataset source. Our experimentation with NVivo NCapture revealed that it is most appropriate and gives much deeper insight for twitter as compared to Facebook. Searches and data analysis and feature extraction in twitter could be based on a particular word, phrase or hashtag.
For Twitter content: Use NCapture to gather Tweets from Twitter for example, Tweets that include a particular word, phrase or hashtag, or Tweets by a particular user. Then import them into NVivo as a dataset source.
Linked-In group discussions: Use NCapture to gather LinkedIn group discussions that are relevant to your research. Then import them into NVivo as a dataset source.
Note: In May 2015 LinkedIn limited access to their web service (API). As a result, you can no longer capture a LinkedIn group discussion as a dataset using NCapture. You can still capture a group discussion, and any other page in LinkedIn, as a PDF.

3.2.0.5 Smartphone data to predict the spending profile

Extensive usage of smart phones has opened new avenues not only for consumers but also for the hackers and law-enforcers. Authors in [29] explain how the spending level of individuals can be determined by using only mobile sensors (Accelerometer, gyroscope). The study is performed in a non-intrusive manner; that is, the usage of sensitive smartphone sensors such as camera, microphone, contacts, calendar and call logs is avoided. The approach used to identify the spending level is by monitoring the user movement (getting of car, walking and loading of groceries) to tag the location and price level associated with that location (by using YELP). This type of profiling is actually long term and gathers data about the individual over a longer period of time as compared to the short term profiling which focuses only on user activity detection and short-term context.

Places visited+Frequency of visit+Price level of store(using Yelp) -> Spending level of consumer.
This approach also intentionally minimizes the use of GPS access to achieve battery efficiency[16]. It only starts logging the details of an individual when a getting-off-car action is detected. A getting off car action is triggered when a driving pattern is followed by a walking pattern(motion sensor-accelerometer).This observation is based on the fact that usually people drive for intended shopping (grocery) and after the drive, they walk to their preferred stores. At this point location mapping is performed by turning on the GPS, Latitude and Longitude (Li) is noted. Then GPS is turned off. Point of interest (POI) corresponding to the Li is checked, if it is not a business zone, it is not

included in the spending level profiling because the individual might be out to visit some friends or family. For example, shopping action of an individual is identified if after 15-120 mins of getting-off-car event, a loading event is observed by using smart phones motion sensor(Gyroscope). The loading event is a repetitive action that a user undergoes while lifting the items from the shopping cart and then placing them into the car trunk. The duration of 15-120 minutes is taken because the study considers only shopping for groceries/big purchases and relatively quick shopping or small purchases are excluded. Spending level (SL) of an individual is calculated by:

$$SL = (\Sigma(i)Ti.Pi)/\Sigma Ti \tag{3.2}$$

Where,
Ti -> Loading Time
Ri -> Location Response(As per the Longitude and Latitude)
If Ri = 1 POI (Point of interest) then Price level= Pi; It means that when the individual visits a single store(Single POI) then the price level of that store is taken from YELP. If Ri > 1 POI then Pi=Average price level of stores, it means that when the individual visits more than one single store or goes to a shopping mall, then the average price level of that mall(or number of grocery stores in that mall) is used because usually nearby situated stores have competitive price levels of products. Moreover if no loading-action is detected after a getting-off event then Ti=0. Here grocery buying behaviour of a user is used to determine his / her spending level. Similar approach could be used to analyse the spending behaviour of suspects after a crime.

3.3 Tools Comparison

Table 3.1: Comparison of Tools for Online Social Network Information Analysis

Features	**Social Snapshot**	**NVivo**	**Netvizz**	**Gephi**
Programming Needed	No	No	No	No
Captures FB Group/Page Data	No	Yes	Yes	No
Captures User Data	Yes	Yes	No	No
Well suited for research purpose	Yes	Yes	Yes	Yes
Well suited for research purpose	Yes	Yes	Yes	Yes
Post Apr'15 FB API changes	Not functional	Functional	Functional	Functional

Table 3.2: Group / Page Data Analysis

Features	**Social Snapshot**	**NVivo**	**Netvizz**	**Gephi**
Gathers FB group data(Open/close)	Yes	Yes	No	No
Analysis of page data	Yes	Yes		No
Capture Images	Links Only	Yes	Yes	No
Visual Analysis	No	Yes	Yes(User specific)	Yes

Table 3.3: User Data Analysis

Features	**Social Snapshot**	**NVivo**	**Netvizz**	**Gephi**
User profile data collection	Not Now	No	Yes	No
Friends details capture	Not Now	No	Yes	No
User posts collection	Not Now	No	Yes	No

This section compares the tools on the basis of their usability, skills required to operate them, types of data they capture, analyse and visualize.Table 3.1 shows the comparision criteria and all four(4) tools results.

Table 3.2 details information about the Facebook group based data analysis provided by the discussed tools. Table 3.3 focuses on the user based data analysis and visualization.

3.4 Facebook Usage Survey

Facebook users behaviour and attentiveness regarding security can be gauged by using different interactive techniques such as focus groups, discussions, questionnaire based surveys and similar approaches[73]. We conducted an online survey to understand the Facebook usage behaviour of individuals and their perception about the security challenges with this social networking site, the applications, quizzes and games associated with it. Moreover the survey also inquired into the way people accept requests from other Facebook users and what information they seek prior to accepting any connection request[109]. The majority of respondents were aged between 20-40 years, were educated and employed individuals. The survey was completed by 60 individuals.

This survey aimed to analyse the following aspects of user's Facebook usage:

1. Facebook usage device (Phone, IPAD , Tablet, PC)

2. Do users provide location information via check-ins?

Table 3.4: Survey Respondents' Occupation Status

Occupation Status	Percentage of Respondents
Employed	58.3%
Self Employed	10%
Unemployed	11.7%
Student	18.3%

3. Understanding of privacy issues by users
4. User's awareness about the type and amount of information obtained by various Facebook applications, quizzes and games.

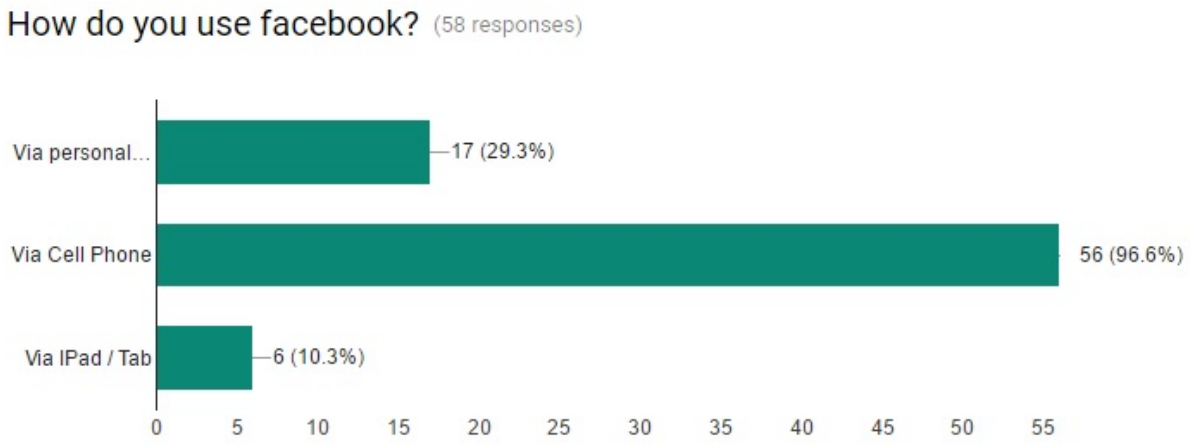

Figure 3.4: Facebook Usage Device

The responses collected from the survey suggest that the majority of the respondents use Facebook from their cell phones as in Fig. 3.4. With a variety of platforms available for cell phones, numerous security challenges arise. Cell phone related unaddressed risks combined with social media exposure magnifies the severity of data theft, identity theft and financial losses[52]. Most of the respondents showed that they care with whom they are being friends but results show that most of the people post or pre accepting a request do not check that when this profile was created as in Fig. 3.5. Anyone can make a fake ID by using the information available on another social network[19]. Afterwards social information can be an aid in a targeted social engineering attack[31].

As shown in Fig. 3.6. users use the check-in options but not very frequently. Check-in information can be used to understand the routine, and spending behaviour/level of a user.

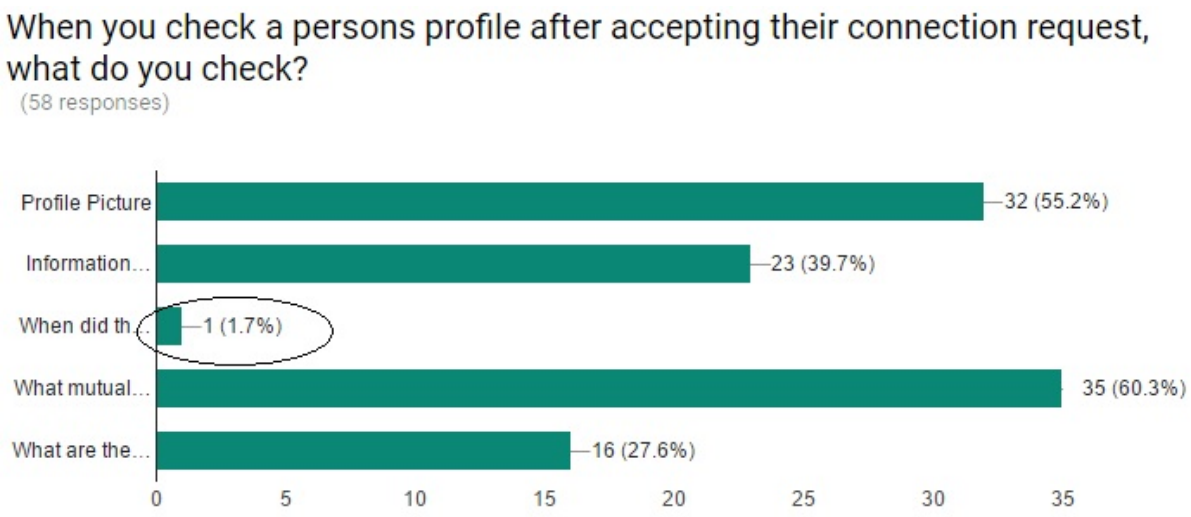

Figure 3.5: Actions Of Users After Adding A New Friend

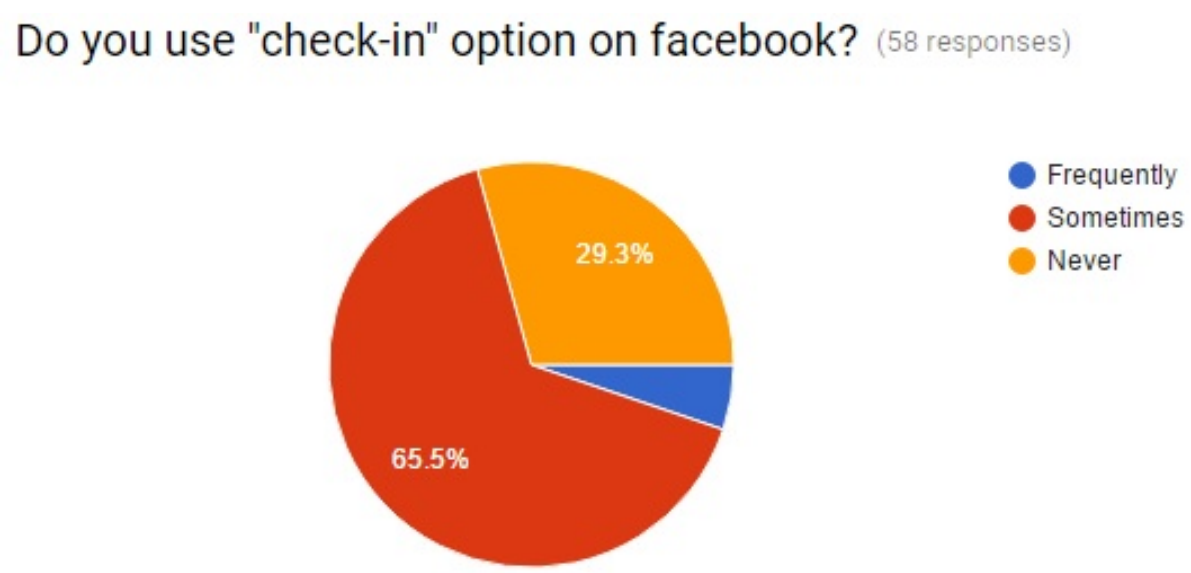

Figure 3.6: Check-In Option Usage

The information obtained by Facebook apps, quizzes and games is also a big challenge, although most of the respondents mentioned that they check what information is accessed by an app as in Fig. 3.7. However, malicious code could be easily attached with links to access these apps , quizzes /games and more information could be captured in the background[119].

Table 3.5 presents value for the survey responses categorized between types of users such as, Employed/self -employed, Unemployed and student. The data collected through

Figure 3.7: Awareness Of Users About Checking What Information Is Taken From Their Profile

Table 3.5: Survey Respondents' Cautiousness

Occupation	**Respondents%**	**Cautious Info. Discl.**	**Careful in friends request**
Empl/Self.Empl.	68.30%	Y=42%,N=17%,S=11%	81.2%
Unemployed	11.70%	Y=8.3%,N=1.6%,S=1.6%	12.5%
Student	18.30%	Y=13.3%,N=3.3%,S=1.6%	6.2%

the survey process represents that the employed and self-employed respondents have certain behavior regarding Facebook usage and their personal information disclosure on online media. The individuals with this behavior demonstrate informed decision making traits. They are careful in choosing the people they add in their circle of friends. Moreover they do not accept the second friend request of people already in their network until and unless they are sure about the authenticity of their friends new ID. This type of people are less vulnerable to identity theft attacks and if they become part of an investigation, it is difficult to get much information from their online social profiles. We also observed that 42% of employed/self-employed Facebook users mentioned that they check what information an application/ game/ quiz is accessing from their Facebook profile. In addition 81.2% of employed/self-employed mentioned that they did not accept a friend request if it is coming from a friend already present in their Facebook network as they see such action as a suspicious activity. The survey revealed less privacy cautious behavior towards Facebook usage by the unemployed and student respondents. Only

8.3% of unemployed individuals showed that they check what information is accessed by various applications on Facebook, while 13.3% of student respondents showed their cautiousness regarding personal information. On the other hand students showed a more casual approach regarding dual friend requests from their contacts. Only 6.2% of the student respondents mentioned that they would not accept a new friendship request from an existing friend on Facebook. The results suggest that academic organizations, student portals, supportive groups / organizations for unemployed people need more stringent security controls and need to spread awareness about the pitfalls of online social networks.

3.5 Conclusion and Future Work

Social networking information is being used and analyzed to understand consumer behavior and benefit online businesses. However, research in social network information to aid digital forensics is a new and challenging domain. With the excessive use of online social networks by individuals of every age, race and background, criminals are now able to get a lot of information about an individual or a group of individuals / organization. Information available via social networks serves as a good augment for social engineering attacks and targeted phishing attacks. This social network activity and resultant data could be used by Law enforcing agencies to get digital evidence against criminals/suspects. However, a lot of challenges are faced in terms of in-depth data extraction from Facebook. The tools with the ability to get in depth information usually require the authorization of targeted ID. For research purposes it is important to obtain consent from users whose accounts are used to extract information. Another challenge is Facebooks rapidly changing APIs and format. Many good research based applications have stopped working because of these rapid changes to protect privacy of Facebook users. Collaboration between the research community and online social networks to enhance the security mechanisms is one of the major steps to stand against the wrong doers. Social network data extraction, data reduction mechanisms and feature extraction algorithms need to be developed to obtain meaningful court admissible results. Combining information from social networks, mobile devices, wireless networks and global positioning systems can help in digging down to even finding a person in a building / room. However to achieve such granularity requires exceptional correlational mechanisms and accurate feature extraction.

CHAPTER 4

Machine Learning Based Relationship Classification and Forensics Analysis

In Chapter 3, we discussed Online social networks as a significant source of information to profile an individual or group. We also declared that the majority of social traffic is generated from mobile devices. By utilising the wealth of information about a mobile user, their digital and physical activities (e.g. online browsing and physical location) can be investigated. Therefore, in any crime investigation artifacts obtained from a mobile device can be extremely crucial. However, the variety of mobile platforms, applications (apps) and the significant size of data compound existing challenges in forensic investigations. In this chapter, we explore the potential of machine learning in mobile forensics, and specifically in the context of Facebook messenger artifact acquisition and analysis. Using Quick and Choo (2017)'s Digital Forensic Intelligence Analysis Cycle (DFIAC) as the guiding framework, we demonstrate how one can acquire Facebook messenger app artifacts from an Android device and an iOS device; the latter is using existing forensic tools. Based on the acquired evidence, we create 199 data-instances to train WEKA classifiers (i.e. ZeroR, J48 and Random tree) with the aim of classifying the device owner's contacts and determine their mutual relationship strength. The contribution of this chapter has been presented in International Conference on Network and System Security (NSS-2018). The outline of this chapter is as follows:

Section 4.1 discusses use of social mobile information for forensics analysis.

Section 4.2 details our case study and our experimental setup.

Section 4.3 explains use of machine learning for relationship strength classification.

Section 4.4 concludes the chapter and discusses future work.

4.1 Background

Online social networks are a source of information, for example to profile an individual or group, to understand consumer sentiments on a particular topic, to detect an ongoing event (e.g. earthquake), to stay in touch (e.g. Facebook's Safety Check feature) [111]. Moreover the mobile phones can even help in outdoor and indoor localization using the size of the room, the number of available beacons, and the strength of RSSI signal[84][48]. In other words, such information can also be useful in a forensic investigation for both criminal cases and civil litigation. However, mobile device and app forensics is constantly playing catch-up due to rapid changes in mobile device technologies [17, 37]. Compounding the challenge is the different formats used to store data on different devices [12, 69]. Unsurprisingly, mobile device and app forensics is an active research area. For example, the authors in [113] forensically examined 20 popular Android instant messaging apps and demonstrated how one can reconstruct message content, to different extent, from 16 of these 20 apps. Other researchers have also shown that a range of artifacts relating to user activities (e.g. login, uploading, downloading, deletion, and the sharing of files) can be recovered from a mobile forensic investigation [25, 36, 117].

Facebook messenger is another popular application (app) where a Facebook user can have text, voice or video conversations with one or more other Facebook users (e.g. one-to-one or one-to-many conversations); thus, this application is the focus of this chapter.

Contribution 1: Specifically, we seek to demonstrate the artifacts that can be obtained from such an app when installed on an Android device and an iOS device. We use the Digital Forensic Intelligence Analysis Cycle (DFIAC) [91] to guide the forensic investigation and use existing commercial forensic tools (i.e. FTK access data, SQLite, IPhone Analyzer) to acquire the forensic artifacts from both devices. The original DFIAC model comprises the following steps:

1. Commence(Scope/Tasking)

2. Prepare

3. Evaluate and Identify

4. Collect/Preserve/Collate

5. Analyze

6. Inference Development

7. Present, Complete / Further Tasks identified

In [91], the authors exported the metadata reports from mobile devices, and the CSV, XLS and SLSX reports were collated and manually combined into a spreadsheet. Then, the spreadsheet was converted in Pajek format for analysis. To highlight the interconnections from the acquired data, a graph (e.g. Fruchterman reingold 2D link chart) can then be created and the information analyzed, for example to identify links between individuals in seemingly disparate cases. In this chapter we limit our investigation scope to messages from only the Facebook messenger app. For example in our iOS case study, the data was acquired from a real-world suicide incident, and we were able to determine the victim's relationship strength with other contacts based on factors such as number of messages exchanged in a day or week, and time and day of the messages.

Contribution 2: We also seek to demonstrate the utility of using machine learning to classify the device owner's contacts with respect to relationship strength, from the obtained forensic artifacts. Thus, in step 6 of DFIAC (i.e. Inference Development), we train three WEKA Classifiers (i.e. ZeroR, J48 and Random tree) to efficiently classify the messenger contacts of the phone owner and determine their mutual relationship strength.

4.2 Case Studies

In this section, we will describe our two case studies, namely, an Android device (see Section 4.2.1) and an iOS device (see Section 4.2.2). We also remark that our case study Section 4.2.2 used the backup image from the iPhone of a real-world victim. The overview of our case study test bed is shown in the fig[4.1].

4.2.1 Android Device Case Study

Table 4.1 summarizes the equipment used in this case study. Figure 4.1 depicts the case study test bed setup.

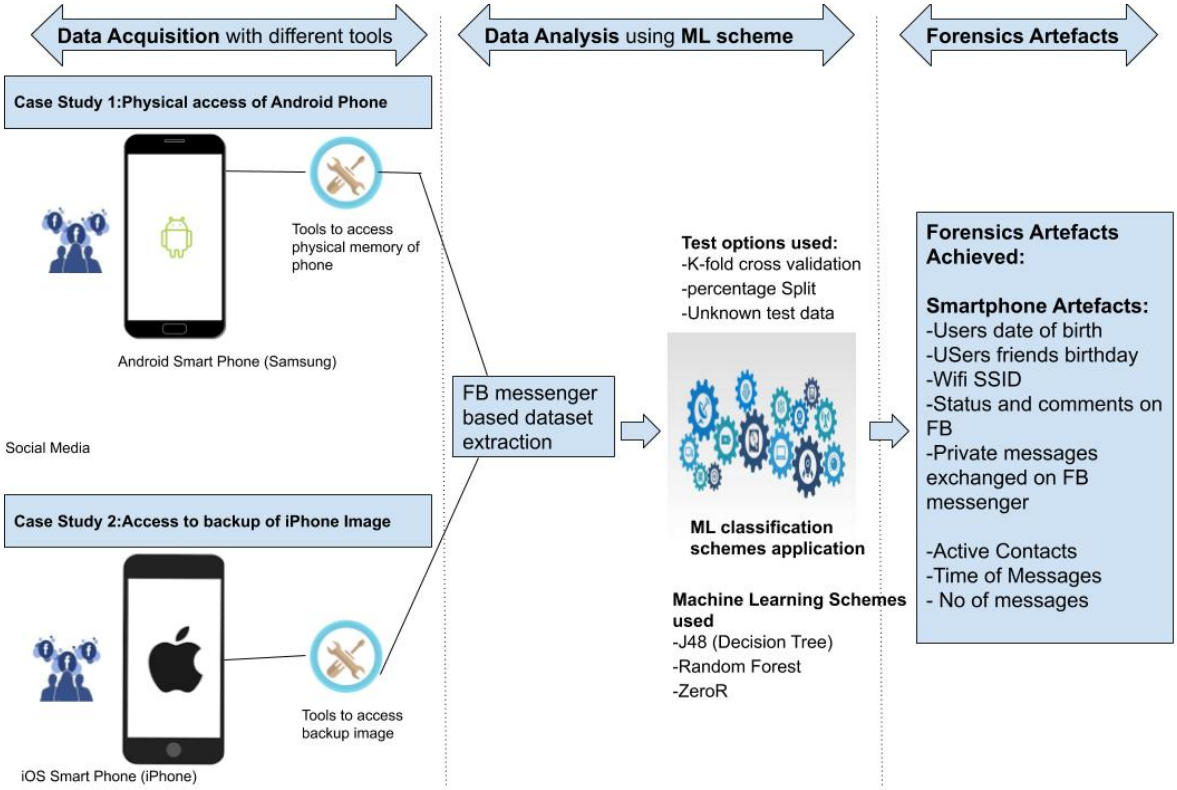

Figure 4.1: Case Study Test Bed Setup

Table 4.1: Experimental Setup

Equipment	Version	Purpose
Samsung Galaxy S3	Android Version 4.3	Test device
ADB Android Debug Bridge	Android Studio 2.3.2.	Android IDE
One Root	Version 1.0	Gain super user access
Root Checker	Version 6.1.7	Verify root access
Forensic Toolkit (FTK)	FTK Imager 3.1.2.0	Disk imaging program
Dell Laptop	Intel Core i7 Windows 10 Ent	Phone images Analysis

4.2.1.1 Device Preparation:

To facilitate the creation of a physical image of the Samsung Galaxy S3 device, we root the device to gain super user privileges and verify root access using the freely available One Root and Root Checker software. Android Debug Bridge (ADB) is installed on the laptop so that we can issue shell commands to the device by connecting it using a data cable.

4.2.1.2 Test Data Creation:

We then create the test data by installing Facebook app on the device. We also proceed to create a test Facebook user ID and undertake the following user activities on the device:

- Sign In. (Login Id and password entered via Facebook application)
- Remove phone number
- Add Friend (Henry gray)
- Upload post (Time is flying)
- Message sent to Henry via messenger app (Hi Henry, Any Plans for the weekend.)
- Comment on own post (And I can't do anything about it.)

4.2.1.3 Imaging of phone memory:

To examine the device's image, we acquire the physical (i.e. bit-for-bit) image of the device's storage, and we know that the device's memory partitions contain user specific data and are of potential forensic interest as shown in Figure 4.2.

- */system - mmcblk0p9* is where read-only memory (ROM) is installed. Within the '/system' are a number of important folders that a user cannot normally access. For example, Location /system/app all where key ROM applications are located. Things like the device app and the messaging app /system/bin are where important binaries, which allow Android to execute the required commands.
- */data - mmcblk0p12* contains information about the installed app, such as SMS and emails. Key directories here are /data/app and /data/data, which are generally wiped when a device is set to the factory default.

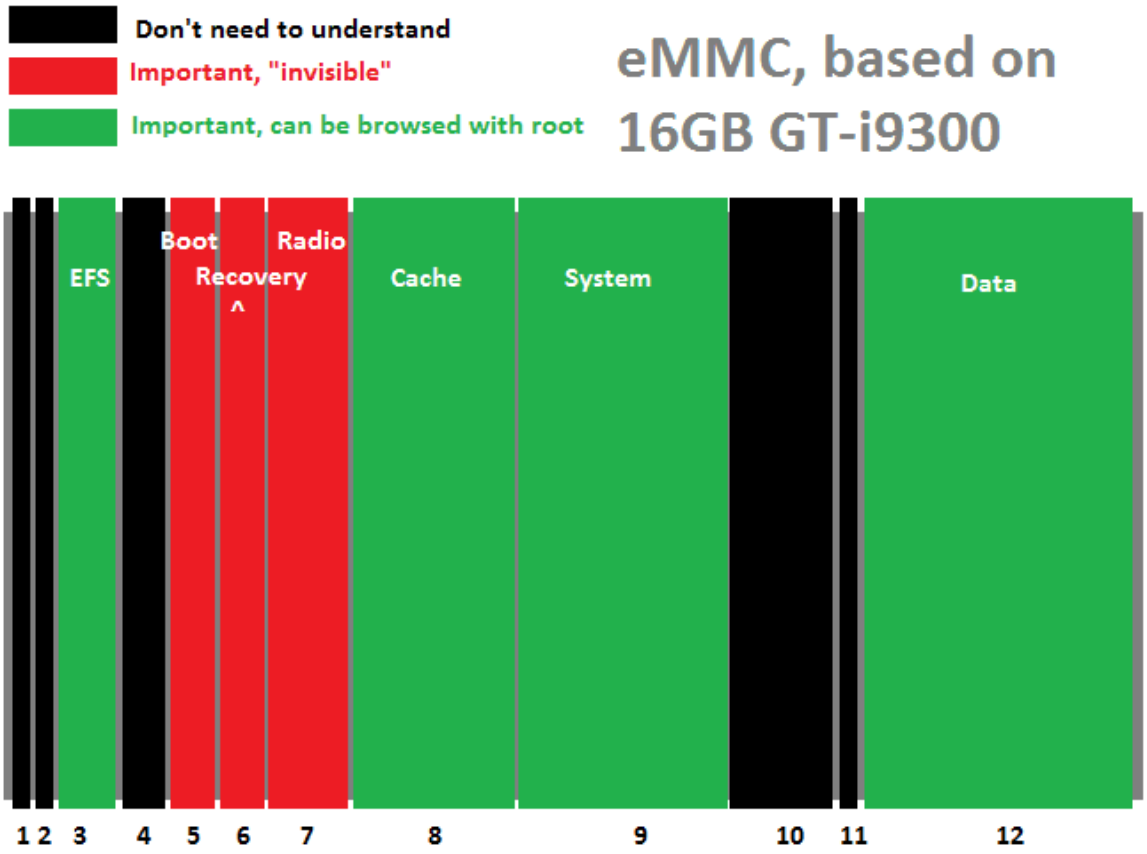

Figure 4.2: GT-i9300 Memory Partitions

- */cache - mmcblk0p8* stores the temporary system data for everyday tasks, designed to expedite the system's access to apps.

Example artifacts of what we obtain from using FTK are depicted in Figures 4.3 to 4.7.

4.2.2 iOS Device Case Study

The device of a teenager who had committed suicide was made available to the researchers for this research, in order to facilitate the determination of the motive and other factors relevant to the investigation. One of the evidence sources is the victim's iPhone backup files obtained from the victim's laptop. Therefore, artifacts were collected from the victim's iPhone 6 (iTunes version 12.0.1.26) backup. As the data is from an ongoing investigation, we anonymize the information to prevent the identification of the case or the individual(s) involved.

```
10fd91790 34 0A 00 00 C0 0A 00 00-C4 0A 00 00 C8 0A 00 00 4···À···Ä···È···
10fd917a0 98 0E 00 00 B0 0E 00 00-BC 0E 00 00 E0 0E 00 00 ····°···¼···à···
10fd917b0 5A D5 FF FF 04 00 00 00-16 00 00 00 42 6F 72 6E ZÕÿÿ·····Born
10fd917c0 20 6F 6E 20 41 70 72 69-6C 20 32 35 2C 20 31 39  on April 25, 19
10fd917d0 38 35 00 00 3D 00 00 00-68 74 74 70 73 3A 2F 2F 85··=···https://
10fd917e0 6D 2E 66 61 63 65 62 6F-6F 6B 2E 63 6F 6D 2F 31 m.facebook.com/1
10fd917f0 30 30 30 31 37 33 36 30-35 33 33 30 36 33 2F 70 00017360533063/p
10fd91800 6F 73 74 73 2F 31 30 36-34 31 31 38 38 36 36 31 osts/10641188661
10fd91810 34 31 36 32 2F 00 00 00-16 00 00 00 42 6F 72 6E 4162/·····Born
10fd91820 20 6F 6E 20 41 70 72 69-6C 20 32 35 2C 20 31 39  on April 25, 19
10fd91830 38 35 00 00 00 00 8E 09-10 00 0C 00 00 00 00 00 85······
10fd91840 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····
10fd91850 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····
```

Figure 4.3: User's Birthday

```
04849ddc0 5F 66 69 65 6C 64 22 3A-7B 22 5F 5F 74 79 70 65 _field":{"__type
04849ddd0 5F 5F 22 3A 7B 22 6E 61-6D 65 22 3A 22 4D 65 73 __":{"name":"Mes
04849dde0 73 65 6E 67 65 72 43 6F-6E 74 61 63 74 4E 61 6D sengerContactNam
04849ddf0 65 22 7D 2C 22 5F 5F 74-79 70 65 6E 61 6D 65 22 e"},"__typename"
04849de00 3A 22 4D 65 73 73 65 6E-67 65 72 43 6F 6E 74 61 :"MessengerConta
04849de10 63 74 4E 61 6D 65 22 2C-22 76 61 6C 75 65 22 3A ctName","value":
04849de20 7B 22 74 65 78 74 22 3A-22 48 65 6E 72 79 20 47 {"text":"Henry G
04849de30 72 61 79 22 7D 7D 7D 5D-2C 22 62 69 72 74 68 64 ray"}}}],"birthd
04849de40 61 79 44 61 79 22 3A 32-30 2C 22 62 69 72 74 68 ayDay":20,"birth
04849de50 64 61 79 4D 6F 6E 74 68-22 3A 31 32 2C 22 69 73 dayMonth":12,"is
04849de60 50 61 72 74 69 61 6C 22-3A 66 61 6C 73 65 2C 22 Partial":false,"
04849de70 6C 61 73 74 46 65 74 63-68 54 69 6D 65 22 3A 31 lastFetchTime":1
04849de80 35 30 35 31 39 32 36 37-37 36 31 33 2C 22 6D 6F 505192677613,"mo
04849de90 6E 74 61 67 65 54 68 72-65 61 64 46 42 49 44 22 ntageThreadFBID"
```

Figure 4.4: User Contact's Birthday

```
0bd593e30 4F 4E 45 5F 54 4F 5F 4F-4E 45 3A 31 30 30 30 32 ONE_TO_ONE:10002
0bd593e40 32 30 38 31 38 30 31 37-35 31 3A 31 30 30 30 31 2081801751:10001
0bd593e50 37 33 36 30 35 33 33 30-36 33 06 5B 7B 22 65 6D 7360533063·[{"em
0bd593e60 61 69 6C 22 3A 6E 75 6C-6C 2C 22 75 73 65 72 5F ail":null,"user_
0bd593e70 6B 65 79 22 3A 22 46 41-43 45 42 4F 4F 4B 3A 31 key":"FACEBOOK:1
0bd593e80 30 30 30 31 37 33 36 30-35 33 33 30 36 33 22 2C 00017360533063",
0bd593e90 22 6E 61 6D 65 22 3A 22-4A 61 6D 65 73 20 57 68 "name":"James Wh
0bd593ea0 69 74 65 22 7D 2C 7B 22-65 6D 61 69 6C 22 3A 6E ite"},{"email":n
0bd593eb0 75 6C 6C 2C 22 75 73 65-72 5F 6B 65 79 22 3A 22 ull,"user_key":"
0bd593ec0 46 41 43 45 42 4F 4F 4B-3A 31 30 30 30 32 32 30 FACEBOOK:1000220
0bd593ed0 38 31 38 30 31 37 35 31-22 2C 22 6E 61 6D 65 22 81801751","name"
0bd593ee0 3A 22 48 65 6E 72 79 20-47 72 61 79 22 7D 5D 48 :"Henry Gray"}]H
0bd593ef0 69 20 68 65 6E 72 79 2C-20 41 6E 79 20 70 6C 61 i henry, Any pla
0bd593f00 6E 73 20 66 6F 72 20 74-68 65 20 77 65 65 6B 65 ns for the weeke
0bd593f10 6E 64 2E 7B 22 65 6D 61-69 6C 22 3A 6E 75 6C 6C nd.{"email":null
0bd593f20 2C 22 75 73 65 72 5F 6B-65 79 22 3A 22 46 41 43 ,"user_key":"FAC
0bd593f30 45 42 4F 4F 4B 3A 31 30-30 30 31 37 33 36 30 35 EBOOK:1000173605
0bd593f40 33 33 30 36 33 22 2C 22-6E 61 6D 65 22 3A 22 4A 33063","name":"J
0bd593f50 61 6D 65 73 20 57 68 69-74 65 22 7D 01 5E 74 94 ames White"}·^t·
```

Figure 4.5: Private Facebook Messages

```
14c7cf3d0 | 33 22 2C 22 74 61 67 67-65 64 5F 69 64 73 22 3A | 3","tagged_ids":
14c7cf3e0 | 5B 5D 2C 22 73 6F 75 72-63 65 5F 74 79 70 65 22 | [],"source_type"
14c7cf3f0 | 3A 22 6E 61 74 69 76 65-5F 74 69 6D 65 6C 69 6E | :"native_timelin
14c7cf400 | 65 22 2C 22 72 61 77 5F-6D 65 73 73 61 67 65 22 | e","raw_message"
14c7cf410 | 3A 22 54 69 6D 65 20 69-73 20 66 6C 79 69 6E 67 | :"Time is flying
14c7cf420 | 2E 22 2C 22 70 75 62 6C-69 73 68 5F 6D 6F 64 65 | ","publish_mode
14c7cf430 | 22 3A 22 4E 4F 52 4D 41-4C 22 2C 22 6C 61 73 74 | ":"NORMAL","last
14c7cf440 | 5F 65 72 72 6F 72 5F 64-65 74 61 69 6C 73 22 3A | _error_details":
14c7cf450 | 7B 22 6D 65 73 73 61 67-65 22 3A 22 22 2C 22 6C | {"message":"","l
14c7cf460 | 6F 67 5F 6D 65 73 73 61-67 65 22 3A 22 22 2C 22 | og_message":"","
```

Figure 4.6: Facebook Status Update And Comments

```
110 | 0A 70 32 70 5F 6F 70 65-72 5F 72 65 67 5F 63 6C | ·p2p_oper_reg_cl
120 | 61 73 73 3D 31 32 34 0A-70 32 70 5F 6F 70 65 72 | ass=124·p2p_oper
130 | 5F 63 68 61 6E 6E 65 6C-3D 31 34 39 0A 6F 6B 63 | _channel=149·okc
140 | 3D 31 0A 61 75 74 6F 73-63 61 6E 3D 65 78 70 6F | =1·autoscan=expo
150 | 6E 65 6E 74 69 61 6C 3A-38 3A 31 32 38 0A 0A 63 | nential:8:128··c
160 | 72 65 64 3D 7B 0A 09 69-6D 73 69 3D 22 35 30 35 | red={··imsi="505
170 | 30 32 2D 22 0A 7D 0A 0A-6E 65 74 77 6F 72 6B 3D | 02-"·}··network=
180 | 7B 0A 09 73 73 69 64 3D-22 54 65 6C 73 74 72 61 | {··ssid="Telstra
190 | 44 43 42 34 22 0A 09 70-73 6B 3D 22 34 36 30 33 | DCB4"···psk="[redacted]
1a0 | 34 33 31 30 38 36 22 0A-09 6B 65 79 5F 6D 67 6D | [redacted]···key_mgm
1b0 | 74 3D 57 50 41 2D 50 53-4B 0A 09 70 72 69 6F 72 | t=WPA-PSK··prior
1c0 | 69 74 79 3D 31 0A 09 66-72 65 71 75 65 6E 63 79 | ity=1···frequency
1d0 | 3D 32 34 31 32 0A 09 61-75 74 6F 6A 6F 69 6E 3D | =2412···autojoin=
1e0 | 31 0A 7D 0A 0A 6E 65 74-77 6F 72 6B 3D 7B 0A 09 | 1·}··network={··
1f0 | 73 73 69 64 3D 22 43 6F-6E 6E 65 63 74 69 66 79 | ssid="Connectify
200 | 2D 6D 65 22 0A 09 70 73-6B 3D 22 61 6D 62 65 72 | -me"···psk="[redacted]
210 | 31 32 33 34 35 22 0A 09-6B 65 79 5F 6D 67 6D 74 | [redacted]···key_mgmt
220 | 3D 57 50 41 2D 50 53 4B-0A 09 70 72 69 6F 72 69 | =WPA-PSK··priori
230 | 74 79 3D 32 0A 09 61 75-74 6F 6A 6F 69 6E 3D 31 | ty=2···autojoin=1
240 | 0A 7D 0A 00 00 00 00 00-00 00 00 00 00 00 00 00 | ·}··· ··· ··· ···
250 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ··· ··· ··· ··· ···
```

Concealed

Figure 4.7: WIFI And Connectify Details

Tools used to obtain the artifacts from the iPhone are FTK Access Data, SQLite Forensic Explorer, Firefox SQLite manager and IPhone Analyzer 2.1.70. Password was not required to extract the personal data from the backup, which included contact numbers, call logs, phone messages, Facebook messenger data/ chats, notes, phone reminders /alarms, pictures, videos and audios. The iPhone Analyzer was able to pull out all details from the backup data, without requiring any passcode. Moreover, it was also able to export all data in the way it was organized on the victim's phone. Figures 4.8 and 4.9 are a snapshot of what could be obtained from the phone's backup. For example, call logs and messages could be easily seen, browsed and exported. We concealed the phone numbers to protect the identity of phone owner. For the same reason, snapshots from other messages artifacts are not shown.

Call logs and messages can be easily seen, browsed and exported. The phone numbers are concealed to protect the identity of phone owner. Similarly messages artefacts snapshot is not shown.

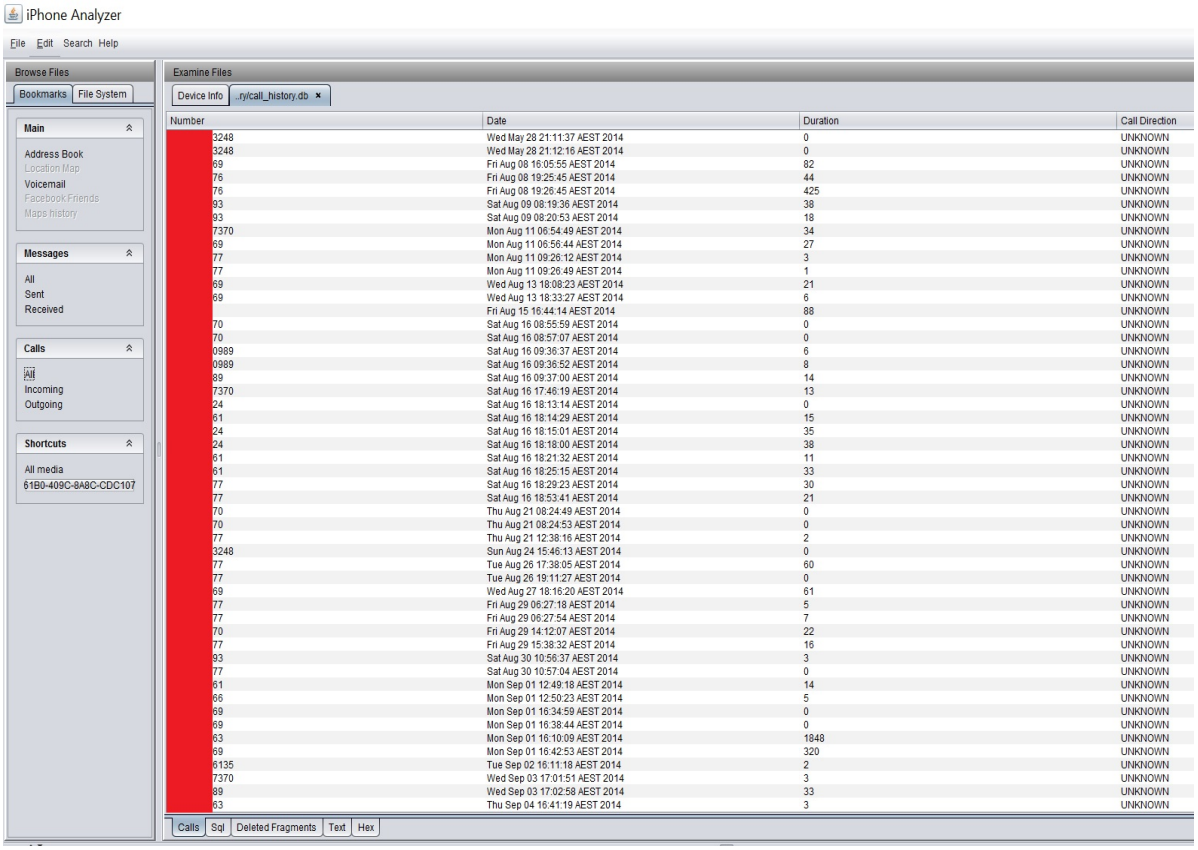

Figure 4.8: iPhone Analyzer

4.3 Machine Learning based Data Analysis With Weka

In our case studies presented in the preceding section, one challenge we face is the difficulty in quickly pinpointing the more important evidence due to the different data formats, number of social apps on a device, etc. In addition, a real-world user will have possibly a number of identities for different social network accounts, a significantly larger number of contacts, etc. Thus, an investigation triage phase needs to be sufficiently robust.

We posit the importance of identifying strongly connected contacts of the device owner during a triage phase, for example by analyzing the social networking messaging app and its content. Therefore, to classify the contacts with respect to their relationship strength, we extract the data features from Facebook messenger app in our case studies. The focus is on the number of messages exchanged with a certain contact. Moreover,

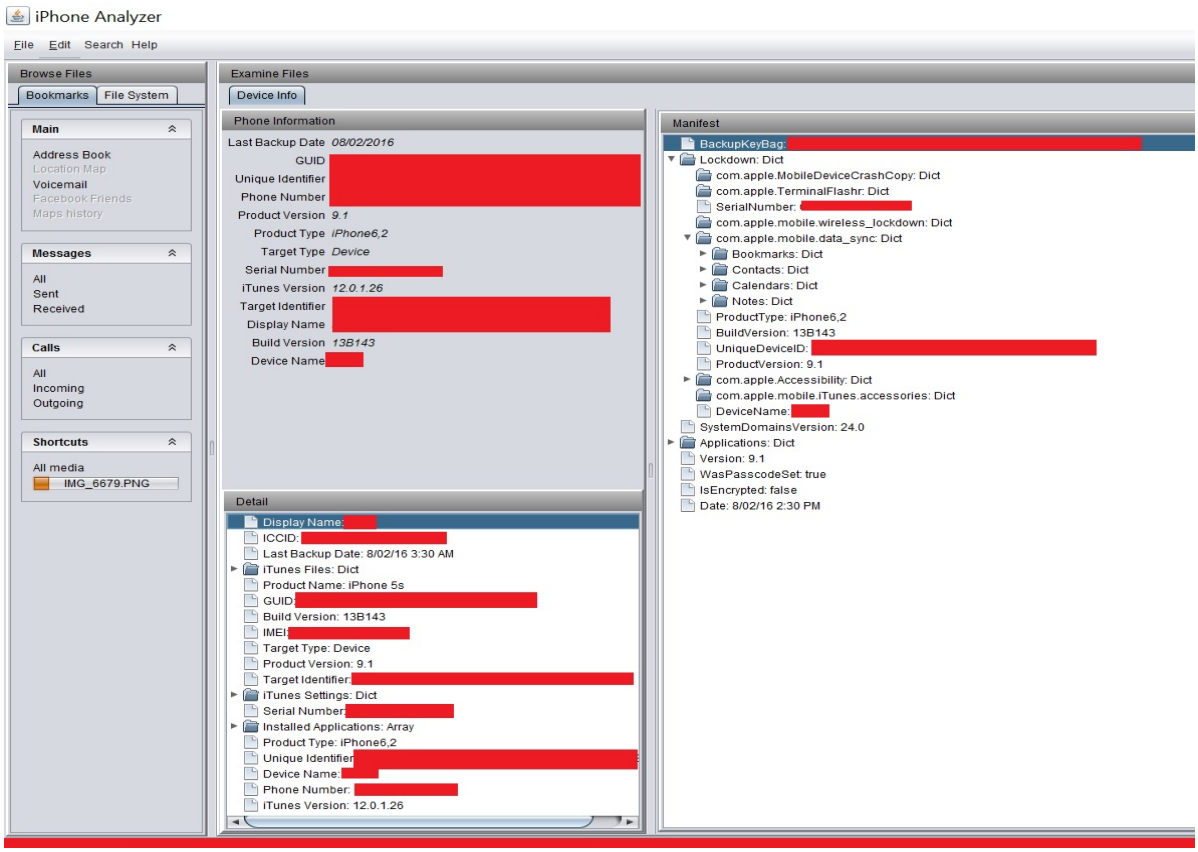

Figure 4.9: iPhone Analyzer Call Details

message exchange during certain times of the day / week (e.g. weekend) may be given a higher weight in determining relationship strength, depending on the context. In order to test the effectiveness of our approach, we analyze the message dataset of 199 instances which represent the message communication pattern of a user with his/her contacts.

Weka (Waikato Environment for Knowledge Analysis) [16] is used to determine the best performing classifiers among ZeroR [65], J48 Decision Tree [87] and Random Tree algorithms [21]. Specifically, we evaluate their performance on our dataset, based on the following key performance indicators: number of correctly identified instances, False Positive Rate(FP), Recall and F-measure.

- The correctly identified instances are the accurately classified instances, which indicate the precision of a classifier.

- FP measure denotes the number of examples predicted positive that are actually negative.

Table 4.2: Attribute Details

Attribute	Description
User	Phone owners Facebook contact/ friend id.A,B,C,D,E
Wavg	Weekly messages exchanged. Can be less than or greater than 320. (64 msgs/day X 5 days= 320)
Weekend	Messages exchange on weekends 0-No messaging 1-Messaging on Saturday or Sunday 2-Messaging on both Saturday and Sunday
Relationship	Relationship type with phone owner W-Weak M-Medium S-Strong

- Recall / sensitivity is the fraction of relevant instances that have been retrieved over the total amount of relevant instances.

$$Recall = TruePositive / (TruePositive + FalseNegative) \tag{4.1}$$

- F-measure is a measure of a test's accuracy. It is the harmonic mean of recall and precision.

$$F - measure = 2 * Recall * Precision / (Recall + Precision) \tag{4.2}$$

The features / attributes of our dataset are presented in Table 4.2. The J48 decision tree is the Weka implementation of the standard C4.5 algorithm. It starts from the training data, builds a predictive model in a tree structure. Its goal is to achieve optimal classification with a minimal number of decisions. The end nodes are the targets/classes.

Random Tree Classifier is a supervised machine-learning classifier based on constructing a multitude of decision trees, choosing random subsets of variables for each tree, and using the most frequent tree output as the overall classification. We use this classifier, as it is known to correct for the J48 decision tree classifier over-fitting issue. In this method, a number of trees are grown (i.e. a forest). Variation among the trees is introduced by projecting the training data into a randomly chosen subspace before fitting each tree. Testing this algorithm on test data resulted in reduced correctly classified instances but the tree structure revealed more detailed decisions on the data attributes as shown in Figure 4.10.

To evaluate performance of J48 decision tree classifier and random tree classifier, we compare their outputs to that of the ZeroR Classifier. ZeroR is the simplest classification algorithm and is based on a frequency table. This classifier relies on the target/class

```
wavg < 319.5 : W (92/0)
wavg >= 319.5
|   weekend < 1.5
|   |   weekend < 0.5 : W (42/0)
|   |   weekend >= 0.5
|   |   |   user = A
|   |   |   |   wavg < 320.5 : W (1/0)
|   |   |   |   wavg >= 320.5 : M (12/0)
|   |   |   user = B : M (7/0)
|   |   |   user = C : M (1/0)
|   |   |   user = D
|   |   |   |   wavg < 321 : W (3/0)
|   |   |   |   wavg >= 321 : M (4/0)
|   |   |   user = E : W (0/0)
|   weekend >= 1.5 : S (37/0)

Size of the tree : 16
```

Random Tree

```
weekend <= 1
|   wavg <= 320: W (78.0)
|   wavg > 320
|   |   weekend <= 0: W (35.0)
|   |   weekend > 0: M (24.0)
weekend > 1
|   wavg <= 319: W (25.0)
|   wavg > 319: S (37.0)

Size of the tree :        9
```

J48 Tree

Figure 4.10: Random Tree And J48 Tree

only and ignores the features. It is useful for determining the baseline of a model. We analyze the data by using the following three test options using ZeroR, Decision Tree and Random Tree.

- Option 1: With K- fold cross validation(K=199)
- Option 2: With 66% Split data
- Option 3: With test data

4.3.1 Option 1: Classifiers with K- fold cross validation(K=100, 150, 199):

For K-fold, data is decomposed into K-blocks. Then, for K = 1 to X, the Kth block is made the test block and the rest of the data become the training data. Classifier is trained, tested, and then K is updated. Theoretically, the higher the number of folds, less biased results are achieved [96]. It is important that K<=X, where X=no. of instances. In our dataset analysis, we use three different values of K=X=100, 150 and 199 to achieve unbiased results. ZeroR provides the baseline 69.3% accuracy for the model when used with K-fold cross validation for all three values of K (100, 150, 199). J48 classifier outperforms with perfect correctly identified instances. Moreover, J48 classifier results remain consistent for all three values of K. The results with J48 also appears optimistic, therefore the same data are used with the random tree classifier, which results in 98.9% correctly identified instances with K=199. Similarly, other performance indicators like

Table 4.3: Test Option 1: With K- fold Cross Validation(K=100, 150, 199)

Classifier	K	Correctly classified	FP	Recall	F-measure
ZeroR	100	69.30%	0.693	0.693	0.568
	150	69.30%	0.693	0.693	0.568
	199	69.30%	0.693	0.693	0.568
J48	100	100%	0	1	1
	150	100%	0	1	1
	199	100%	0	1	1
Random Tree	100	98.40%	0.024	0.985	0.984
	150	99.40%	0.011	0.995	0.995
	199	98.90%	0.023	0.99	0.99

FP, Recall and F-measure are more realistic when using Random Tree. The changes in K value vary between the results of Random Tree classifier from 0.5% to 1%.

Table 4.3 summarizes the results with K-fold cross validation for all three classifiers.

4.3.2 Option 2: Classifiers With Split Data (50%, 66%, 80%)

Initially, we tested the classifiers on Weka default split value of 66%. By splitting the data of 199 instances in 66% means that 66% of data (131 instances) were used as training and 34% (68 instances) as test.

In this test option, our classifiers show a significant decrease in precision as compared to the K-fold cross validation, but J48 and Random tree still perform with an above 90% accuracy rate. We also analyze the behavior of all three classifiers by splitting the data in 50% and 80%. J48 and Random tree achieve accuracy rates of 100% and 97.50% respectively, at 80% of data splitting. However, ZeroR achieves the highest accuracy (69.30%) at 66% data split and lowest accuracy (62.50%) at 80% data split. Table 4.4 summarizes the results of all three classifiers with 50%, 66% and 80% split data.

4.3.3 Option 3: Classifiers With Test Data

In the third test option, we provide a separate test data to Weka, to check the performance of our dataset. In this test option, Random tree classifier results improve by 0.5% as compared to option 1 (K-folds) and 6.8% as compared to option 2 (split data). Therefore, on an average the performance of the Random Tree classifier improves by 3.65% when

Table 4.4: Test Option 2: With Split Data (50%, 66%, 80%)

Classifier	% split	Correctly classified	FP	Recall	F-measure
ZeroR	50%	67.70%	0.677	0.677	0.546
	66%	69.30%	0.693	0.647	0.49
	80%	62.50%	0.625	0.625	0.481
J48	50%	95.95%	0.085	0.96	0.957
	66%	94.12%	0.101	0.941	0.937
	80%	100%	0	1	1
Random Tree	50%	95.95%	0.085	0.96	0.957
	66%	92.60%	0.105	0.926	0.922
	80%	97.50%	0.042	0.975	0.974

Table 4.5: Test Option 3: With Test Data

Classifier	Correctly classified	FP	Recall	F-measure
ZeroR	69.3%	0.693	0.693	0.568
J48	100%	0	1	1
Random Tree	99.4%	0.001	0.995	0.995

a new/unknown test data is introduced. The performance of ZeroR and J48 is almost identical to the first test (K-folds) – see Table 4.5.

4.4 Conclusion and Future Work

In this chapter, we studied the potential of using machine learning classifiers to facilitate mobile forensics, specifically in terms of Facebook messenger artifact triaging. Specifically, after acquiring forensic artifacts from an Android device and an iOS device, we created 199 data-instances and trained three WEKA Classifiers (i.e. ZeroR, J48 and Random tree). This was done so that we were able to classify the device owner's contact classification into weak, medium and strong (i.e. determine their mutual relationship strength). Our analysis with the three test options and three different classifiers revealed that J48 appeared to be highly biased or overfitted to the provided dataset, and Random tree achieved optimal performance in all three test options with increased accuracy when tested with a different test dataset.

Future work includes extending this work to deep learning algorithms and also using a broader range of bigger datasets.

CHAPTER 5

SACIFS: Smart Aged Care Information Forensics System using Machine-Learning

In chapter 4, our research work focused on the mobile phones based data analysis. However, with the rise of internet of things (IoT), sensor based attacks have gained global concern. In chapter 5, we have discussed the use of machine learning algorithms on sensor based data for forensics insights. The outline of this chapter is as follows:

Section 5.1 gives overview of the prevailing use of sensor based smart environments and the associated challenges.

Section 5.2 discusses the related work in secure smart environments .

Section 5.3 explains the research problem and data collection methodology.

Section 5.4 explains proposed model and research methodology.

Section 5.5 concludes this chapter.

Recent security breaches exhibit an incline towards the integrity cornerstone of the CIA (Confidentiality, Integrity, Availability) triad. Integrity of information becomes more crucial when it is about human health information. In this situation, post incident forensic capability is crucial. However, at the moment, the importance of forensics capable systems is surpassed by the need for secure systems. Rapid smart home and smart care implementations demand efficient security measures and forensic capable systems. Smart Aged Care Information Forensics System (SACIFS) aims to provide forensics capability to a sensor based aged care system which are prevalent around the world. Wearable sensor devices are implemented to monitor elderly individual's physical activity monitoring to assist in risky situations. However, these sensor networks are susceptible to data integrity attacks. We developed Smart Aged Care Information Forensics System (SACIFS), a machine learning based model to detect data integrity attack on human activity data, collected from wearable sensor devices. We validated the performance of our proposed model using a variety of data analysis procedures combined with feature selection, feature extractions, feature correlations and predictive modelling. The main contribution of this study is our machine learning based model SACIFS, which detects data alterations with 99.8666% accuracy. SACIFS is propitious and distinctive for data integrity checking in a smart care environment.

5.1 Background

Data integrity attack is a type of attack that aims to mislead the system or its users by altering some collected data of the system[77]. Salami and data diddling attacks are two examples of data integrity attacks, where a series of minor inconspicuous data alterations are performed that together result in a bigger breach. Data integrity attacks are a continuous challenge for Cyber Physical Systems (CPS), which use widespread sensing, networking, computation and control into physical spaces. Research community has developed tools to quantify the maximum perturbation that an attacker can introduce into a control system via a stealthy integrity attack on a subset of the sensors [78, 85]. United States Director of National Intelligence James Clapper place emphasis on the data integrity threats in late 2015 by stating that:
"While most of the public discussion regarding cyber threats today is focused on the confidentiality and availability of information, in the future, however, we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting

access to it."[4]
Moreover, Health Insurance Portability and Accountability Act of 1996 (HIPAA) also highlights the integrity concern of electronic protected health information(e-PHI) as follows[2]:
"A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed"

United Nations predicted that there would be 2 billion (22 % of the world population) older people by 2050[45, 112]. About 89% of elderly people will be likely to live independently, with about 80% of them having a chronic disease. These statistics show that many elderly people will rely on innovative and secure technological health-care/nursing solutions[59]. This research is motivated by the fact that this aged population around the world requires physical activity monitoring, to assist in precarious circumstances. Wearable sensor devices are now used to monitor elderly individuals in health-care and nursing home systems[24, 32, 34, 39, 62, 67]. Consequently, health-care applications are promising fields for wireless sensor networks, where patients are monitored using wireless medical sensor networks (WMSNs). Current WMSN trends concentrate on patient's reliable communication, patient's movement and energy-efficient routing. However, new technology deployment in health-care applications without security considerations, makes patient privacy vulnerable [63]. Data integrity attacks are one of the many security threats to these sensor networks. Therefore, in this research we contributed by focusing on the following objective:

- Use of machine learning algorithms to detect data integrity compromise in a smart aged care environment.

To achieve the stated objective, we aim to examine the associated research goals:

- Application of machine-learning to propose a Smart Aged Care Information Forensics System (SACIFS), for detection of integrity compromise of human activity data contributing towards enhanced trust in smart aged care concept.
- Performance enhancement of machine learning model by dimensionality reduction of data-set.

In this research, we used machine-learning capabilities to detect and predict the integrity compromise of data. Our work is based on the sensor data of 14 elderly (66 -86

years old) individuals that were monitored in a nursing home scenario. We combined the activity data of all 14 individuals to check the credibility of data, with the help of machine learning. We trained machine learning model on elderly individuals all movement data was recorded by the wireless sensor. Subsequently, we used correlation based feature extraction to select the most relevant features for our experiment.
This study is organised in eight[8] sections. Section 2 discusses the related work. Section 3 explains the research problem explanation, assumptions and data-set background. Section 4 describes the methodology of our proposed model. Section 5 discusses the effects of feature selection and data-set views on the model's performance. Section 6 and 7 provide details of training and testing of our model. Section 8 concludes the study.

5.2 Related work

According to Statista [3], during the last measured period (2014 - First Half of 2018) the majority of the 668 data breaches affected business and medical/health-care organisations. Out of which 309 attacks targeted retail while 181 were on health-care industry and the remaining 178 attacks besieged finance, government and education industries. Evidently, health-care industry has experienced the highest level of breaches in 2017 and it proves to be a worthwhile target for the cyber criminals. The industry has fallen prey to new variants of cyber breaches due to the sensitivity of customer information they handle and the relative deficiency of security awareness knowledge. Therefore, cyber criminals are more likely to steal or alter data from databases of hospitals and nursing homes because their security systems are generally obsolete.

Over the past decade, the health sector has progressed from manual paper-based systems to paperless electronic health management systems[10]. Many countries public health systems provide electronic patient records and health report portals, which are accessible around the globe. Such flexible health management systems are implemented by more than 200 American hospitals, while Canada and other countries are likely to implement similar technologies.

Health industry innovations, like use of sensors, actuators and IoT based health-care has exponentially changed the face of present health management. With all these advancements-future not only promises more technological dependency but also imposes serious security challenges to this arena[53].

One of the important rudiments for application of IoT-based health-care systems are utility and safety for users. In any IoT-based system, data gathering, mining, and

provision is carried out over the Internet[47]. Consequently, sensitive data compromise possibilities also widely exist. Moreover, IoT-based applications are particularly vulnerable due to two architectural aspects:

1. Wireless communication, which is prone to interception and eavesdropping.
2. IoT components are based on lightweight computing capabilities, thus they cannot afford resource-starved security and detection models for security.

In IoT based wireless communication, confidentiality of data does not ensure protection from external unwanted modifications. An adversary can manipulate some or more fragments of data within a packet. This compromised data can become an input to the system depicting a normal situation as an emergency or vice versa. In case of life-critical circumstances, this inability to detect integrity compromise becomes chaotic, since it can cause a superfluous alarm or overlooking a situation, which needs immediate attention. It is also important to understand and pin-point the root cause of integrity compromise, because it can go unnoticed during communication(e.g. salami attack).

Researchers in [76] explain cyber physical systems (CPS), which employ distributed networks of embedded sensors and actuators that interact with the physical environment. CPS are monitored and controlled by a supervisory control and data acquisition (SCADA) system. Now smart health management, smart energy management, process control systems and aviation systems use CPS in diverse applications. Authors in [76, 77] discussed the effect of integrity attacks on the sensors of the control systems by revisiting and adapting the Kalman filter, the linear quadratic gaussian (LQG) controller, and the x^2 failure detector. The authors acknowledge that a deception attack, which compromises the integrity factor, is more difficult to detect than a DoS (Denial of service) attack, which targets the availability factor. Therefore, smart aged care systems are susceptible to the threat of integrity attacks which are usually unnoticeable thus difficult to detect.

Another variation of cyber physical system is the body sensor network (BSN).It is one of the core implementations of IoT in health-care management systems. In a body sensor network, a patient is monitored using a collection of tiny powered and lightweight wireless sensor nodes. However, without adequate security, this useful technology in health-care applications can cause serious patient privacy concerns[27]. In [78, 81] authors discussed major security requirements in BSN-based health-care system. They divided all security requirements into two parts namely network security (authentication, anonymity, and secure localisation) and data security (privacy, integrity, and freshness). For network security requirements, they proposed a lightweight anonymous

authentication protocol, while for data security requirements OCB (offset codebook)[99] authenticated encryption mode is used. For digital health data, integrity and security issues are of critical importance. It becomes complicated when one aspect (integrity) puts the other counterpart (confidentiality) at stake. To ensure integrity of data, compression techniques cannot be applied, as in many cases, such techniques alter the data. However, confidentiality of patient data is clearly fundamental and desirable in order to raise public confidence in digital technologies.

For any smart health-care system, IoT and big data are the crucial building blocks. This big data originated from an IoT based health-care system carries many security risks. To detect and prevent the unauthorised use or modification of private information, rigorous research is essential in the direction of machine learning based systems as these systems are already showing promise in health industry for diagnostic aspects. However, in medical diagnostics IoT itself cannot provide rehabilitation treatments or construct medical resources [5]. Nevertheless, it can help in effective treatments by rapid diagnosis of patients, based on the diagnosis derived from historical data. In health diagnosis, the conditions of patients vary from one another even if they have similar symptoms. Therefore all the factors are taken into account, to generate an effective therapeutic regimen. A computer-aided tool relies merely on the data acquired by sensors and records of past similar cases, while self-learning methods can adapt, intelligently diagnose and recommend the treatments. Some self-learning algorithms, such as Artificial Neural Network (ANN), Genetic Algorithms (GA), Ant Colony Optimisation (ACO), and Simulated Annealing (SA), can be applied to analyse data and mine knowledge[5]. However, if the data fed into learning algorithms is compromised, they cannot generate accurate diagnosis. Therefore, we propose to use support vector machine (SVM) algorithm to detect whether the data is compromised or not. Support vector machine algorithm works robustly on large volumes of data and reports genuine results. Briefly, in this study we tested the promising algorithms like Support Vector Machine, Decision Tree (J48), Naive Bayes and K-Nearest Neighbours (KNN) to examine data credibility. Consequently this achieved better security and privacy of human individuals in a nursing environment.

In [79] researchers secured IoT based health-care data by using the learning based Deep-Q-Network approach. The introduced method inspects the IoT security issues such as authentication, malware detection, access control issue but data integrity assurance and integrity compromise detection is not addressed. This study examines the performance of Support Vector Machine, Decision Tree, Naive Bayes and K-Nearest Neighbour algorithm to predict the data integrity compromise. We also evaluated the effects of

dimensionality reduction and feature selection on the prediction capability of algorithms.

5.3 Research Problem and Data Collection

5.3.1 Research Problem

Smart aged care environments using wireless sensors to monitor movement of patients are susceptible to data alteration or misrepresentation. If such data change remains unnoticed, it can pose serious challenges to human lives and chaos in smart aged care environments. Therefore, a mechanism is needed to accurately identify these abnormal changes.

In this research we propose a model which indicates if the movement data of a patient is suspected of alteration. This data alteration could be an intentional act by an attacker or an unintentional sensor glitch/malfunction. To solve this problem, we propose to train and use machine learning algorithms for data change detection. We have also utilized feature selection to train the algorithms faster and reduce the complexity of the model. Different subsets of features are used to improve the accuracy of the model and to reduce over-fitting.

5.3.2 Research Scenario and Assumptions

Envision a smart aged care environment. Mr. X is an elderly individual with past history of falls in his room while performing routine activities. He is continuously monitored to detect any future fall incident. The aim is to give instant medical attention in case of a fall incident. On a certain day, false fall alerts may be sent to the carer of Mr. X, prompting the carer to respond to Mr. X room. Such incidents may be overlooked as a sensor glitch! Nevertheless, it could be an integrity attack threat.

Assume Hacker Z, has taken access to the wireless sensor network and is manipulating the sensor data and creating false alerts. He is corrupting the data to create chaos and is a risk to precious human lives. This scenario requires a system, which learns the normal activity for Mr. X, his range of motion and his pattern of activities. Based on training data, this system is capable of detecting suspicious activity. Our machine learning based model SACIFS (Smart Aged Care Integrity Forensics System) learns from the historic activity data of Mr. X. It makes a profile of normal values of frontal, vertical and lateral axis acceleration for Mr. X. If the values deviate from the learned profile, SACIFS declares that the data has been compromised.

5.3.2.1 Threat Model

Our research is based on the activity data of elderly individuals. If the attributes of activity data are altered then accurate activity labelling is not possible, consequently, it will also affect the activity profile of a monitored patient. A small alteration in data can be chaotic for smart aged care services deploying similar methods, as the individuals activity data is the primary way to understand the usual profile of that patient. Therefore, this activity data is a high value asset for this research. The wireless antennas mounted in the monitored room and the sensor device attached to the clothing of patient are vulnerable to a denial of service attack, spoofing attack, while the movement data used for activity recognition is susceptible to data diddling attack as mentioned in Figure. 5.1. If the attacker changes the monitored attributes slightly (like data diddling) then the attack can go unnoticed. We addressed this aspect in our research. We trained our model on the individual's activity attributes resulting in activity profiling of every individual. As a result when a value different to the persons profile is received then our model identifies it as a compromised value.

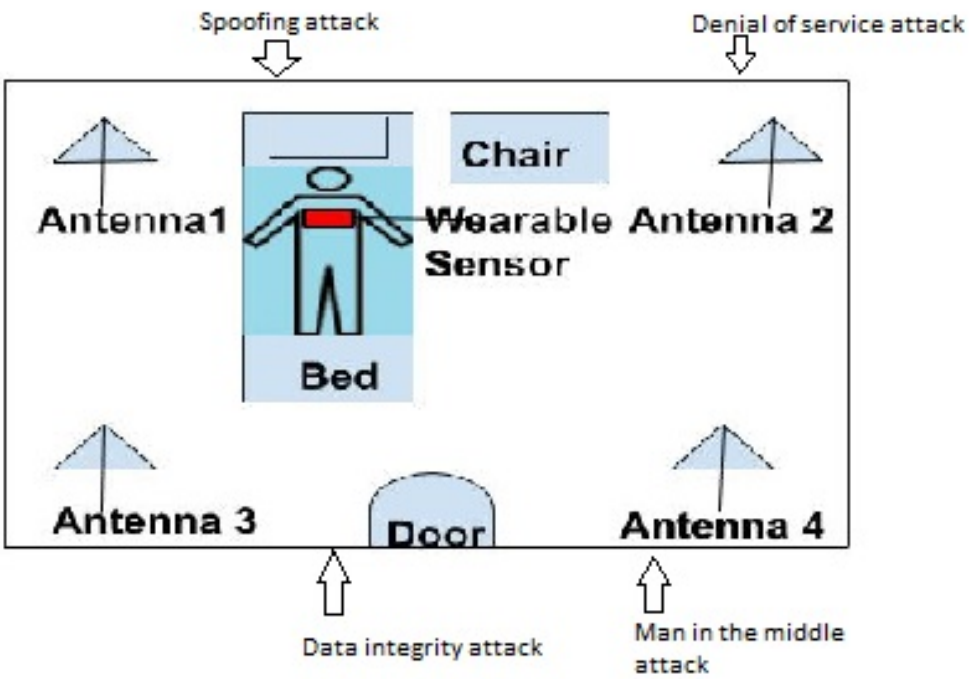

Figure 5.1: Proposed Model

5.3.3 Feature Selection Module

Exclusions: This research does not covers the denial of service attacks now.

Assumptions:

- Attacker has access to the monitoring network and the movement data.
- Our approach is applied to the selected data as of now, but it has the potential to be applicable to other types of tabular data.

5.3.4 Algorithm Implementation

SACIFS Algorithm is based on the machine learning approach [23]. It is implemented, trained and tested in WEKA environment. WEKA allows to enhance machine learning algorithm by tuning their parameters, called hyper parameters in a controlled environment. To improve the performance of our machine learning model we tuned the hyper parameters of different competitive machine learning algorithm. After understanding the best competitive model, we further enhanced its performance accuracy by training on larger data sets and testing the final model with unknown data. To interpret the results from tuning an experiment using statistical significance and criteria we showed our analysis and comparison between different algorithms.The model is finalised after passing though three machine learning modules which are classified as:

- Feature selection module (see 5.4.1)
- Training module (see 5.4.2)
- Testing module (see 5.4.3)

5.3.5 Data Collection

This section explains the background information about the data-set we have used for our research. This data-set is comprised of sequential motion data from fourteen healthy elderly people aged 66 to 86 years. All fourteen individuals used a battery-less, wearable sensor on top of their clothing (sternum level) for the recognition of activities in the clinical environment. In [108] authors presented and evaluated this novel method for mitigating the high falls risk associated with bed exits based on using an economical, privacy preserving and passive sensor enabled RFID[115] device. Their approach is

based upon a classification system built upon conditional random fields that requires no pre-processing of sensorial and RF metrics data extracted from an RFID platform.

Participants were allocated in two clinical room settings (S1 and S2). The setting of S1 (Room1) uses 4 RFID reader antennas around the room (one on ceiling level, and 3 on wall level) for the collection of data [56, 94]whereas the room setting S2 (Room2) uses 3 RFID reader antennas (two at ceiling level and one at wall level) for the collection of motion data. In this paper, we specifically used the S1 (Room 1) data as our training set.We depicted the room setting as the first block(left to right) in Figure 2.

We combined the data for all participants and analysed 52482 instances to train our model. The main attributes of the recorded data set are as follows:

- T: Time in seconds(from 0 rounded to the closest 0.025s)
- Fi: Frontal axis acceleration ; where i=I(ID of antenna reading sensor)1,2,3,4
- Vi: vertical axis acceleration
- Li: Lateral axis acceleration
- I: ID of antenna reading sensor
- Rssi: Received signal strength indicator (RSSI)
- P: Phase
- F: Frequency
- Act: Label of activity (1-sit on bed, 2-sit on chair, 3-lying, 4-ambulating)

5.4 Proposed Model and Research Methodology

SACIFS is based on the machine learning approach [23]. The model consists of a monitored room setup and three machine learning modules demonstrating completeness of our proposed scheme. In Fig. 5.1. first block (left to right) depicts the monitored room followed by the modules, which are classified as:

- Feature selection module
- Training module
- Testing module

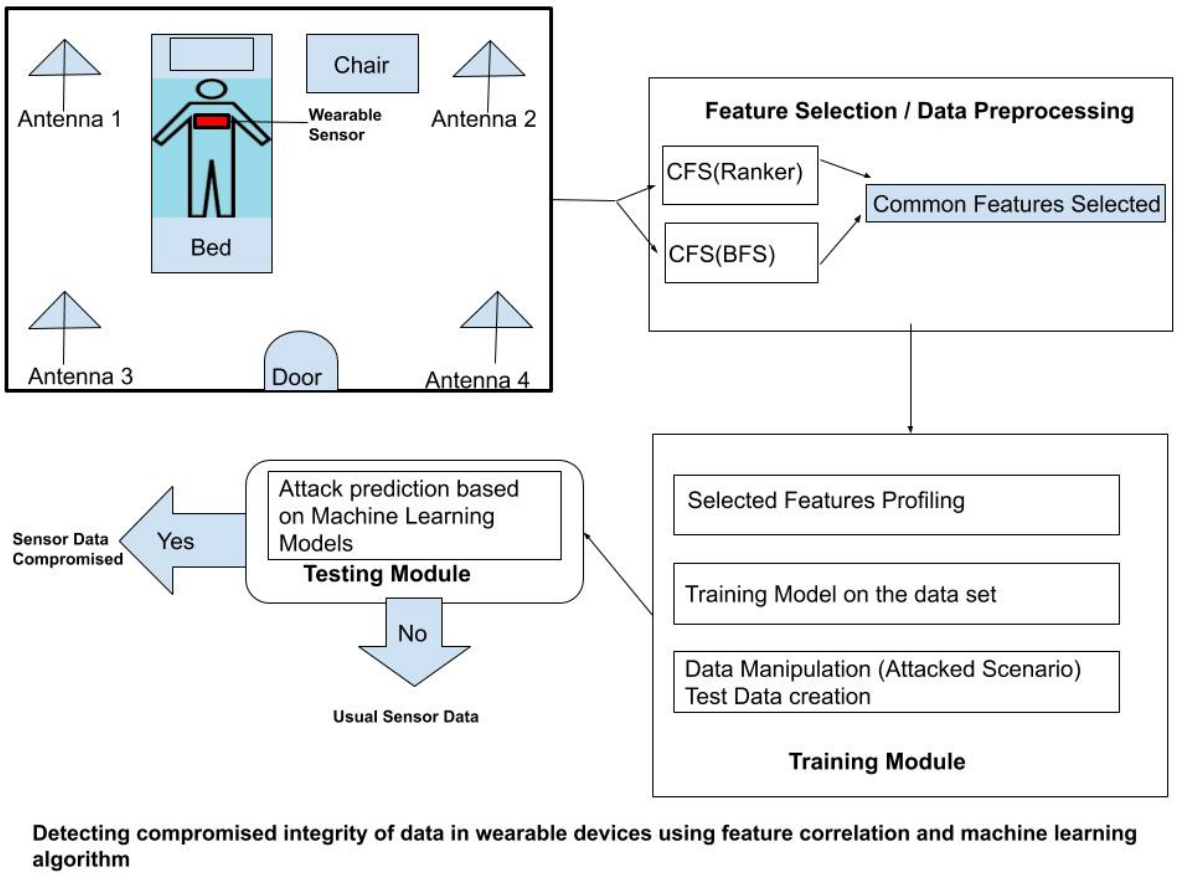

Figure 5.2: Proposed Model

5.4.1 Feature Selection Module

Feature selection module takes input in the form of sensor data from the first block of Fig. 5.1. As the sensor data contains a number of attributes, some attributes are more relevant for predictions. Therefore, to find interesting features of our data set, our feature selection module combines attribute evaluation algorithms and search mechanisms on data. The attribute evaluator algorithms used are correlation, information gain, gain Ratio, CFS (Correlation based feature selection) subset, while search algorithms used are ranker and best first mechanisms.CFS is Correlation based feature selection, it is an algorithm that uses an appropriate correlation measure and a heuristic search strategy. We performed feature selection by using four (4) different approaches. Our purpose for using a combination of techniques was twofold. First, it helped to obtain the most relevant attributes, which define our data-set. Second, these techniques gave us different views of our data-set, to gauge and observe the behaviour and performance of

machine learning models. The combination of attribute evaluators, search algorithms and the consequent data set view is in table. 5.1:

S.no	Attribute Evaluator	Search Algorithm	View Name	Feature Set
1	Correlation	Ranker	Data set M	Activity, La, Va, Freq, AID
2	Information Gain	Ranker		Fa, La, Va
3	Gain Ratio	Ranker		Va
4	CFS Subset Eval	Best First	Data set B	Va, La, Phase

Table 5.1: Attribute evaluators, search algorithms and consequent data-set view

Attribute Evaluators : Correlation, Information Gain, Gain Ratio and CFS Subset Eval. The correlation attribute evaluator ranks feature subsets according to a correlation based heuristic assessment function. The bias of the evaluation function is toward subsets that contain features that are highly correlated with the class and uncorrelated with each other. Two types of features are screened out:

1. Irrelevant features - they possess low correlation with the class.
2. Redundant features - they possess high inter correlation with one or more of the remaining features.

The accepted feature holds higher scope to predict class in area of the instance space as compared to other features. CFS feature subset evaluation function, can be defined as Pearson correlation coefficient [46]:

$$M_s = \frac{K\overline{R_{cf}}}{\sqrt{K + K(K-1)\overline{R_{ff}}}} \tag{5.1}$$

Ms is the heuristic merit of a feature subset **S** containing **K** feature
Rcf is the mean feature-class correlation (f **E** S)
Rff is the average feature-feature inter correlation. The numerator of the equation provides an indication of how predictive features are for the class while the denominator indicates the redundancy within the features.

CFS Subset evaluator assesses the value of a subset of attributes by considering the individual predictive ability of each feature along with the degree of redundancy between them. Subsets of features that are highly correlated with the class while having low inter-correlation are preferred [46]. As the correlation based feature selection also accounts for the inter correlation between features, it gives a different set of features while CFS Subset evaluator prefers the features that are highly correlated with the class,

but possess low feature to feature inter correlation. Information gain evaluator works reasonably for most cases, but in our scenario when there are only a few variables that have a large number of values. Information gain acts biased towards attributes with a large number of values as root nodes. Therefore, we also used gain ratio evaluator, which is a modification of information gain. It reduces bias of "information gain evaluator" by taking into account the number of branches that would result before making the split.

Attribute Search Mechanisms:

Ranker Search Method evaluates each attribute and lists the results in a rank order, while Best First Search Method starts with either no features or all features. Best first search can begin with the empty set of attributes and search forward, or begin with the full set of attributes and search backward, or start at any point and search in both directions.

Data-set views obtained from Feature Selection

Data-set view M: This data-set view is comprised of features yielded by correlation, information gain and gain ratio. We combined the features selected by three evaluators in dataset view "M" because feature set produced by information gain and gain ratio was subset of correlation method. Here the letter M denotes mean, because in all combination, the mean attribute ranking weight is used as the cut off value for feature selection as shown in Table .2.

Feature Selection Method	Attribute Evaluator	Correlation	Information Gain	Gain Ratio
	Search Algorithm	Ranker	Ranker	Ranker
Attribute Ranking Weights		0.024704	0.001211	0.767678
		0.016535	0.001108	0.002817
		0.011864	0.000682	0.001701
		0.010526	0.000512	0.000774
		0.009461	0.000318	0.000591
		0.00529	0.000157	0.000218
		0.003117		
		0.000871		
		0.000357		
Cut off Value (mean of weights)		0.009191667	0.000664667	0.128963
Selected Features		Activity, La, Va, Freq, AID	Fa, La, Va	Va

Table[2] Attribute Analysis For Feature Selection

Data-set view B is a result of CFS Subset evaluator, which evaluates the value of

a subset of attributes by considering the individual predictive ability of each feature along with the degree of redundancy between them. Subsets of features that are highly correlated with the class while having low inter correlation are preferred [46]. Moreover, for data-set B, CFS Subset evaluator is combined with best first search algorithm, which searches the space of attribute subsets by greedy hill climbing improved with backtracking.

5.4.2 Training Module

To train the model with our data-set, we performed the following steps. The detailed explanation of all the steps is provided in section 6:

1. Introduced a new class attribute within the data set named as Status which can hold a nominal value as 0-normal or 1-compromised.

2. Selected Features Profiling: Understand the normal profile of data, which means to find out the range of values for our selected features Fa, Va and La. (in our case we checked the normal values for Fa only). Mention the normal ranges for all the selected features)

3. Labelling of instances: Based on the normal profile values for our features, we assigned the label to all the instances. Example if the value of FA, VA or LA is other than the normal range, we marked that instance as "Attacked".

4. Classification: Trained the Support Vector Machines model (as obtained from the comparative analysis) by observation of the performance of the model on the supplied training data.

5.4.2.1 Compromised Data Sample Creation

Our data-set contained only the normal situation data when a patient or old individual in the nursing environment carries out usual activities. We determined the normal ranges of values for the attributes and trained the model on the usual and unusual values. We found out that most dominating fields were VA, LA and FA and the normal ranges for them are shown in table. 3.

Model was trained on our feature selected data-set(data-set B), that was selected from the phase 2 i.e. data-set B which contained Va, La, Phase, Status(Class attribute).

Label 1: "Sitting on bed"					
Fa Range		Va Range		La Range	
1.2921	-0.56048	2.0302	-0.094162	0.89856	-0.37858

Label 2: "Sit on Chair"					
Fa Range		Va Range		La Range	
1.1632	-0.666	1.3298	0.48	0.48805	-0.34437

Label 3: "Lying"					
Fa Range		Va Range		La Range	
1.5032	-0.032831	1.0656	-0.55349	1.2178	-0.48121

Label 4: "Ambulating"					
Fa Range		Va Range		La Range	
0.99901	-0.74808	1.5479	-0.27789	0.90996	-0.36718

Table[3] Normal Ranges of Fa, Va, La values

5.4.3 Testing Module

In testing module, we evaluated the prediction capability of our model on feature selected data-set (data-set B) and unseen data. This is to estimate the accuracy and effectiveness of models in differentiating between normal and compromised data.

For testing module, we used 10 fold cross validation to select the best model, which accurately predicts the status of data under consideration, as normal or compromised. Ten-fold cross validation is the best method for model selection, in real-world data-sets similar to our data-set [60]. Therefore ten folds (K=10) are preferred in classification problems even if computation power permits using more folds. In 10-fold cross-validation, the original sample is randomly partitioned into 10 equal size sub-samples. Out of the 10 sub samples, a single sub sample is retained as the validation data for testing the model, and the remaining (k-1) or 9 sub samples are used as training data. The cross-validation process is then repeated k=10 times (the folds), with each of the 10 sub samples used exactly once as the validation data. The 10 results from the folds can then be averaged (or otherwise combined) to produce a single estimation. The advantage of this method is that all observations are used for both training and validation, and each observation is used for validation exactly once [1, 18, 107]. In our analysis, we divided this problem into two (2) phases, to achieve the best model for our data-set.

Phase 1: Pre-feature selection Process In this phase, we performed analysis of algorithms behaviour on raw, standardised and normalised views of data-set. This phase provides

most effective algorithm and also the most suitable data-set view.
Phase 2: Post-feature selection Process Here analysis of algorithm's performance on two data-sets. First data-set is the view of data-set obtained from phase 1, on which our algorithms performed well, while second data-set is the feature selected data-set view (only containing selected features).

5.4.3.1 Phase 1: Pre-feature selection Process:

To analyse and expose the structure of our data-set classification problem to the machine learning models, we created different views of the data-set. Below are the details of the data-set views and the algorithm variations we analysed to obtain the best performing model on best data-set view for our analysis.

- Raw View (R)- This view contains data directly obtained from the sensor, without any normalisation and standardisation.
- Normalised View (N) - all the input attributes are normalised to the range 0 to 1. This view can help diverse algorithms that can be biased by the scale of the attributes (e.g. regression and instance-based methods)
- Standardised View (S) - each attribute has a mean value of 0 and a standard deviation (mean variance) of 1. This view may help algorithms that assume a Gaussian distribution in the input attributes (e.g. Logistic Regression and Naive Bayes)

Based on our literature review we selected five algorithms to compare their behaviour and performance on our variety of data-set views [14]. The algorithms analysed are ZeroR(for baselining), Support Vector Machine (SVM), Decision Tree (J48), Naive Bayes, K-Nearest Neighbours (KNN).

All the algorithms are tested on ten (10) performance criteria, namely Percent correct, Root mean squared error, Mean absolute error, Relative absolute error, True Positive rate, True negative rate, False positive rate, False negative rate, Mathews correlation and Area under ROC (AUC). However, five (5) out of ten (10) criteria reflected the model performance variations, therefore we only mentioned those criteria in this study in table. 4.

As shown in the comparison table of all the models, KNN performed consistently better than other algorithms. However, we observed that most of the algorithms did not reflect significant change in results on different data views(R, N, and S). Only Naive

	Performance Measure	Baseline		Best		Least	
1	Percent Correct	Model	ZeroR	Model	KNN	Model	Naive Bayes
		%age	99.97	%age	99.98	%age	99.92%
		View	All	View	All	View	All
2	Root Mean Sqr	Model	ZeroR	Model	KNN	Model	Naive Bayes
		Value	0.02	Value	0.01	Value	0.03
		View	All	View	All	View	N,S
3	Relative Absolute Error *	Model	ZeroR	Model	SVM	Model	Bayes Naive
		%age	100	%age	46.89	%age	189.61
		View	100	View	All	View	N
4	Mathews Correlation	Model	ZeroR	Model	KNN	Model	SVM
		%age	0	%age	0.40	%age	0
		View	All	View	All	View	All
5	Area under ROC	Model	ZeroR	Model	Naïve Bayes	Model	SVM J48
		%age	0.50	%age	0.95	%age	0.50
		View	All	View	R,S	View	All

Table[4] Model Performance Analysis Before Feature Selection

Bayes demonstrated sensitivity to different data views, e.g. Naive Bayes root mean square changed with varying data views although it was not the best performer in this criteria. For criteria, Area under ROC (AUC) value lies between 0.5 to 1 where 0.5 denotes a bad classifier and 1 denotes an excellent classifier. In our data analysis part 1, Naive Bayes outnumbered all the models with 0.95 % of the area under the curve on data-set R and data-set S, while 0.94% on data-set N. KNN performed better than other models in three (3) out of five (5) criteria. In analysis part 2, we will introduce feature-selected data-sets to the model and the raw data-set(R) to observe the variations in models behaviour.

5.4.3.2 Phase 2: Post-Feature Selection Process:

We observed from the models analysis part 1 that the majority of models worked best on the data-set R. Therefore, to understand the effects of feature selection. we used three views of our data-set as shown below:

- Data Set (M) - Selected features via mean Cut off as shown in table .2.
- Data Set (B) - Selected features via best first search
- Data set(R) - contains all the attributes

#	Performance Criteria	Best Performing Model + Percentage on Data View (M,B,R)		Least Performing Model + Percentage on Data View (M,B,R)	
1	Percent Correct	Model	SVM	Model	Naive Bayes
		%age	99.99	%age	99.92%
		Data View	B	Data View	R
2	Root Mean Sqr	Model	KNN	Model	J48
		Value	0.01	Value	0.02
		Data View	M,R	Data View	All
3	Relative Absolute Error	Model	SVM	Model	Naïve Bayes
		%age	17.82	%age	187.54
		Data View	B	Data View	R
4	Mathews Correlation	Model	SVM	Model	J48
		%age	0.72	%age	0
		Data View	B	Data View	All
5	Area Under ROC	Model	Naïve Bayes	Model	J48
		%age	1	%age	0.50
		Data View	B	Data View	All

Table [5]: Model Performance Analysis After Feature Selection

In the Accuracy criteria, SVM improved from 99.97% to 99.99% on the feature-selected data-set B, while 99.97 % was achieved on data-sets M and R. J48 accuracy showed no sensitivity to the three data types and gave 99.97% accuracy on all data-sets. Naive Bayes performed best on data-set B; in fact, it was the second best performer in terms of accuracy. Nevertheless, on data-set M and R, it was below the baseline with 99.93% and 99.92% accuracy as shown in table. 5. While KNN worked best with the data-set R (99.98%) and just achieved baseline performance with data-set M and B.

In Root Mean Squared Error, criteria only SVM, Naive Bayes and KNN showed some variations, SVM and Naive Bayes performed well on data-set B (0.01) while KNN performance improved on data-set M and R (0.01). Relative absolute error (RAE) for baseline model ZeroR exhibited no change for any data-set view. SVM had the lowermost RAE on data-set B, j48 classified better on data-set M and R; Naive Bayes got lowest errors on data-set B while KNN worked best on R. ZeroR was consistent with all three data-sets with 0.50 Area under ROC (AUC), while Naive Bayes yielded ideal AUC value of 1 on the data-set B and 0.95 on data-set M, R. KNN was the second best with 0.98 AUC at data-set B.

Because of analysis phase 2, Support vector machine (SVM) model reflected improved performance. It performed better than all the competitive models in three (3) out of

five (5) criteria. This analysis emphasised the capability of the Support vector machine algorithm to perform well even with less number of features (Selected features) as shown in Fig. 5.4.This capability is highly desired in the management of sensitive big data to reduce complexity and computational overheads. Moreover, analysis phase 2 also emphasised that the performance of all the models improved on data-set B (based on CFS Eval subset and Best first search).

	Performance Measure	Before Feature Selection		After Feature Selection	
1	Percent Correct	Best Model	KNN	Best Model	SVM
		%age	99.98	%age	99.99
		Data View	All	Data View	B
2	Root Mean Sqr	Best Model	KNN	Best Model	KNN
		Value	0.01	Value	0.01
		Data View	All	Data View	M
3	Relative Absolute Error *	Best Model	SVM	Best Model	SVM
		%age	46.89	%age	17.82
		Data View	All	Data View	B
4	Mathews Correlation	Best Model	KNN	Best Model	SVM
		%age	0.40	%age	0.72
		Data View	All	Data View	B
5	Area under ROC	Best Model	Naïve Bayes	Best Model	Naïve Bayes
		%age	0.95	%age	1
		Data View	R	Data View	B

Table [6]: Comparison of the Effect of Feature Selection and data set views on Algorithms

In our experiment, Support vector machine (SVM) is used from phase 2 due to its better performance on the major criteria. We used an 80% of the split, where 80% data (41985 instances) is used as training data and 20% (10496 instances) is used as test data. Our model estimated with an accuracy of 99.8666% with 10482 correctly classified Instances out of a total of 10496 instances. Although the root mean squared error and relative absolute error show a high value but in a classification prediction problem, only the percentage of correctly/incorrectly classified instances is considered. Correctly classified instances takes only into account whether a prediction is accurate or not, i.e.

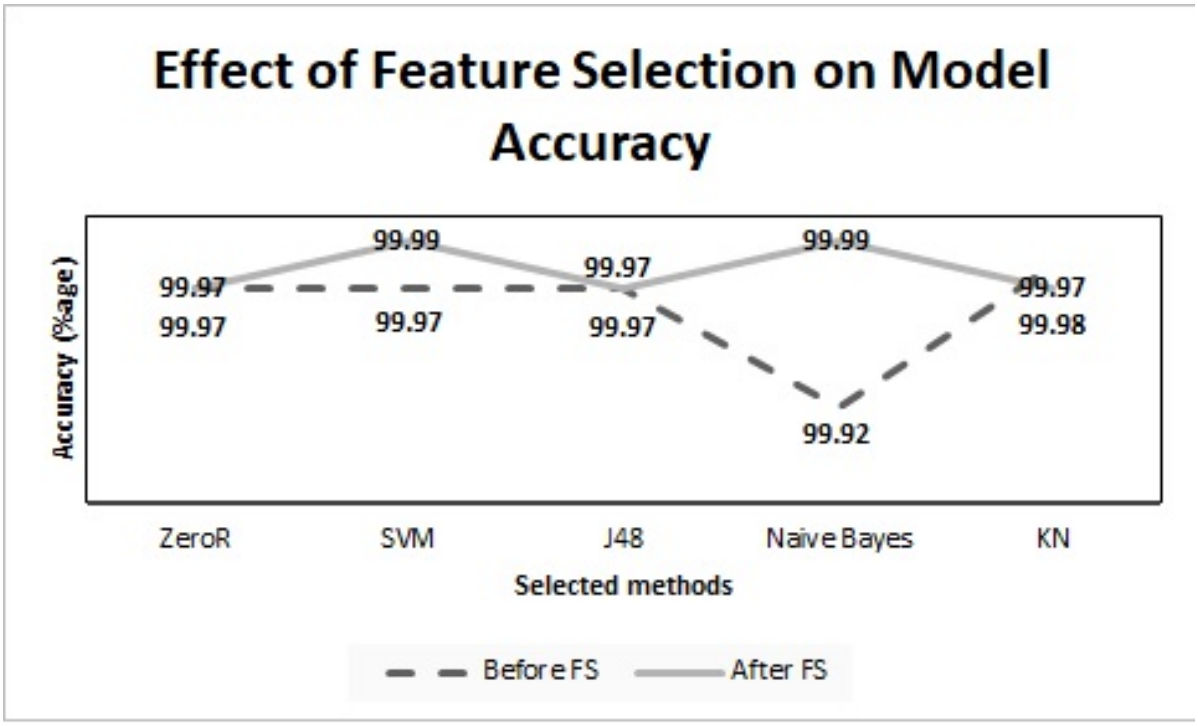

Figure 5.3: Effect of Feature Selection On Algorithms

predicting 2 instead of 1 is as incorrect as predicting 10000. This is because the class of the datum is wrong and there is no importance given to the magnitude of difference between classes. If we are performing a regression analysis then we predict a continuous quantity and the magnitude of difference matters. That is, if the actual value is 1 and the prediction is 2, the model is much better than when the prediction is 10000. Therefore in our model the error values in the prediction analysis are of less importance. In our scenario we achieved more correct predictions overall, but the ones that were wrong were further off the mark further. The major achievements of our experiments are:

- In our proposed model , we tested five machine learning algorithms. Our tests validated that Support vector machine algorithm performed better than all the competitive models in three (3) out of five (5) criteria.
- Our experiment validated the capability of Support vector machine algorithm to predict data alteration, even with fewer number of features. This capability makes it suitable for data integrity attack detection in an IoT based scenario, where the system must not be resource hungry.
- Our proposed model also validated that feature selection improves prediction

performance of most of the machine learning algorithms, as shown in fig. 2.

- Our experiment also highlights that testing machine learning with different data set views improves prediction performance of most of the machine learning algorithms as shown in table [6] and also helps in selecting the most suitable algorithm for a certain problem.

5.5 Conclusion

This research is motivated by the requirement for elderly individual physical activity monitoring, to assist in risky situations. Technological advancements like wearable sensor devices are now used to monitor elderly individuals in health-care and nursing home systems. This trend will continue to increase with smart home or smart health-care implementations. With all these advancements, the future not only promises more technological reliance but also imposes serious security challenges to this arena. Data integrity attacks are one of the many security threats to smart care concepts because the foundation is on sensors and actuators networks. In this article, we proposed a model for detecting sensor data integrity attacks with the help of machine learning algorithms. To the best of our knowledge, this scheme for machine learning usage for the security of human activity based systems against data integrity attacks is a novel approach.

In this research, sensor data is used to train the machine-learning model to understand the normal values of an individual positional attributes (vertical, frontal and lateral axis acceleration) in a constrained environment. We evaluated five (5) renowned machine-learning attributes for this model, namely ZeroR Algorithm (for baselining), Support Vector Machine (SVM) Algorithm, Decision Tree (J48) Algorithm, Naive Bayes Algorithm and K-Nearest Neighbours (KNN). We also compared the effect of feature selection on the performance of the model, which resulted in a confirmation that it actually improved the performance of the model in terms of accuracy. According to our analysis, Support vector machine algorithm performed well with the feature-selected data-set, which validates the capability of performance of this model with limited data. This made it appropriate for an IoT based environment where resource efficiency is a significant influence.

We foresee that machine learning has a long way to go in the health industry, not only for health oriented diagnosis purposes, but also for solving security and privacy challenges. With the above prospects of machine learning models, we anticipate that a smart and secure aged care system will be the future norm.

CHAPTER 6

DEEP LEARNING

In chapter 4 and 5, we discussed the use of mobile phone and sensor based data analysis for forensics analysis. In both chapters we used machine learning analysis and used various techniques to obtain valuable forensics information. In chapter 6, we have summarised our preliminary analysis of mobile phone data utilising artificial neural networks(ANN). This chapter is an extension of chapter 4, in this chapter multilayer perceptron (MLP) is used to classify the contacts of phone owner in strong, medium and weak relationship strength. The outline of this chapter is as follows:

Section 6.1 introduces deep learning and multilayer perceptron networks.

Section 6.2 discusses the data classification with MLP, this section uses the same data set which was utilized in chapter 4 .

Section 6.3 concludes this chapter..

6.1 Deep Learning using Multilayer Perceptron (MLP) for relationship classification

Deep Learning is a branch of machine learning concerned with algorithms inspired by the arrangement and function of brain called artificial neural networks(ANN)[64]. Modern state-of-the-art deep learning is based on many layers deep neural network models using the backpropagation algorithm[104]. In this research, we have used one of the most popular ANN techniques, Multilayer Perceptron Networks (MLP). We have tested MLP because it is most suitable for tabular data, while other ANN techniques, Convolutional Neural Network is used for image data and Long Short-Term Memory Recurrent Neural Network is appropriate for sequence data.

A multilayer perceptron (MLP) is a deep, artificial neural network. It is composed of more than one perceptron. They are composed of an input layer to receive the signal, an output layer that makes a decision or prediction about the input, and in between those two, an arbitrary number of hidden layers that are the true computational engine of the MLP. MLPs with one hidden layer are capable of approximating any continuous function. Multilayer perceptrons are often applied to supervised learning problems, they train on a set of input-output pairs and learn to model the correlation (or dependencies) between those inputs and outputs. Training involves adjusting the parameters, or the weights and biases, of the model in order to minimize error. Backpropagation is used to make those weigh and bias adjustments relative to the error, and the error itself can be measured in a variety of ways.

Multilayer Perceptron [41] is comprised of at least one hidden layer or intermediate layer, one input layer and one output layer. We analysed important performance measures like accuracy, precision, recall , f-measure and area under curve(AUC) for MLP. The purpose is to understand the effect of the number of hidden layers, number of neurons in each layer and the dataset split percentage on the performance measures of MLP. We used WEKA to make different combinations based on:

1. Number of hidden layers to have in the neural network

2. Number of neurons to have in each layer

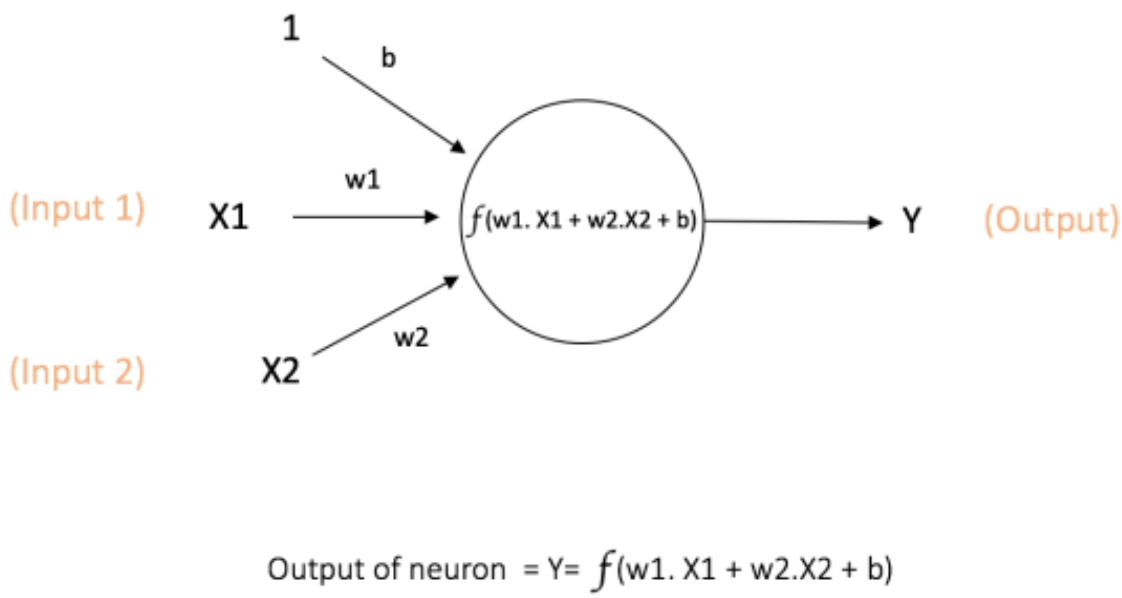

Figure 6.1: Single Neuron

6.2 Related Work

Multilayer perceptron (MLP) with one hidden layer is one of the most commonly used form of artificial neural networks. A well-trained MLP with appropriate number of nodes in its hidden layer is proven to have efficient and robust performance on patterns with high orders. Authors have formed an identification system, where MLP is utilized as a classifier to distinguish keyboard dynamics patterns of several people. A larger number of the neurons in the single hidden layer are examined empirically to reach the optimum number. The optimum number of hidden layer neurons has been found to be 44 and relevant equal error rate (EER) equal to 0.95% has been reported[97]. To obtain accurate results from MLP, the number of layers and included neurons used is crucial. However, there is no benchmark for the number of hidden layers and the neurons in them. This number varies with the type, structure and amount of training data and the inter-data correlations.

Researchers compared multilayer perceptron neural networks with support vector machine on heart diseases dataset of 303 patients. Their results show that using neural networks on a dataset with increased features usually results in better performance because the algorithm learns from data. The more scenarios it is presented with, it improves with time and learns from its historical data[80].

To discover network attacks efficiently, authors have proposed an end-to-end detection approach by implementing deep learning models to analyse payloads. They have proposed a convolutional neural network-based payload classification approach (PLCNN) and a recurrent neural network-based payload classification approach (PL-RNN) for use in attack detection. The two approaches learn feature representations from original payloads without feature engineering and support end-to-end detection. These approaches achieve accuracies of 99.36% and 99.98% when applied to the DARPA1998 dataset, respectively; these accuracies are comparable to or better than those of state-of-the-art methods. However, deep learning models have two problems. First, parameters adjustment of models with greater numbers of parameters is complex; i.e., model training is relatively difficult and requires some skill. Second, the interpretation of methods is not ideal as CNNs and RNNs behave like black boxes. Although these models usually achieve satisfactory results, it is difficult to explain the results they produce[66].

In [105] researchers analysed forensically the offline signatures and reported that MLP training time was high as compared to Random Forest. However, modification in pre-processing phases improved the results of MLP. Moreover, the increase in the number of signatures also enhanced the accuracy.MLP and Random Forest faced low memory heap problem with the large dataset, therefore 5 fold cross validation with larger datasets (10 users with forgery) was performed to resolve the issue.It proves that by increasing the number of training samples the accuracy will improve. Similar research is conducted using users' activities and profile information with MLP[58].

6.3 Data Classification with MLP

This section covers the MLP based deep learning analysis done with the same data set that we used in chapter 4. This chapter explores the relationship strength based onsocial networks. Using the linear combination of effective variables, they measured the link strength. Multilayer perceptron is a non-linear classifier. This method models the non-linear boundaries of classes. The structure of MLP might be different based on application; however, it includes one input layer, one output layer, and one or several hidden layers. At the training phase, a sample of training data enters the network in each step and MLP updates the weight of its links based on the inputs and corresponding output label. In this work, backpropagation learning algorithm was used for neural network training. This method performs based on spread of error from the output layer backwards and correcting link weights[101].

Initially we used 2 layers, because our data set is comparative, therefore it does not require many layers. Moreover, the number of hidden neurons used are between the size of the input layer(4 inputs) and the size of the output layer(2 outputs). Afterwards we increased the size of layers to 4 and 4 neurons in each layer; see Fig. 6.2. The epoch size is 500, learning rate 0.3 and momentum is 0.2.

MLP Hidden Layers	%age split	Accuracy	Precision	Recall	F-measure	AUC
Layer=1	50%	67.67%	0.458	0.677	0.546	0.781
Neurons=2	66%	33.25%	0.105	0.324	0.158	0.232
	80%	62.5%	0.391	0.625	0.481	0.261
Layer=1	50%	67.67%	0.458	0.677	0.546	0.340
Neurons=4	66%	32.35%	0.105	0.324	0.158	0.652
	80%	37.5%	0.141	0.375	0.205	0.496
Layer=2	50%	67.67%	0.458	0.677	0.546	0.316
Neurons=2,4	66%	32.35%	0.105	0.324	0.158	0.151
	80%	37.5%	0.141	0.375	0.205	0.635
Layer=2	50%	67.67%	0.458	0.677	0.546	0.505
Neurons=4,2	66%	32.35%	0.105	0.324	0.158	0.076
	80%	37.5%	0.141	0.375	0.205	0.784
Layer=4	50%	70.29%	0.494	0.703	0.580	0.638
Neurons=4,4,4,4	66%	28.98%	0.084	0.290	0.130	0.259
	80%	77.5%%	0.601	0.775	0.677	0.394

Figure 6.2: MLP Performance Analysis With Varying Layers And Neurons

Most of the performance measures except AUC have given high values when 50% split data is used, which is quite obvious as in this scenario 50% of the data is used to train the model while the other 50% is used as test data. This also emphasizes the back propagation aspect of deep learning; the model learns from its mistakes made with the test data. In 50% split, half of the data is used as test data so the performance of the model has improved. The table 10 clearly shows that model learned the dataset and change of layers and number of neurons is not making any changes in the results. However, area under the ROC curve (AUC) values is highest (0.784) with L=2 and N=4,2. This area actually represents the probability that a randomly chosen positive example is correctly rated (ranked) with greater suspicion than a randomly chosen negative example[20]. Area under ROC (AUC) value lies between 0.5 to 1 where 0.5 denotes a bad classifier and 1 denotes an excellent classifier.

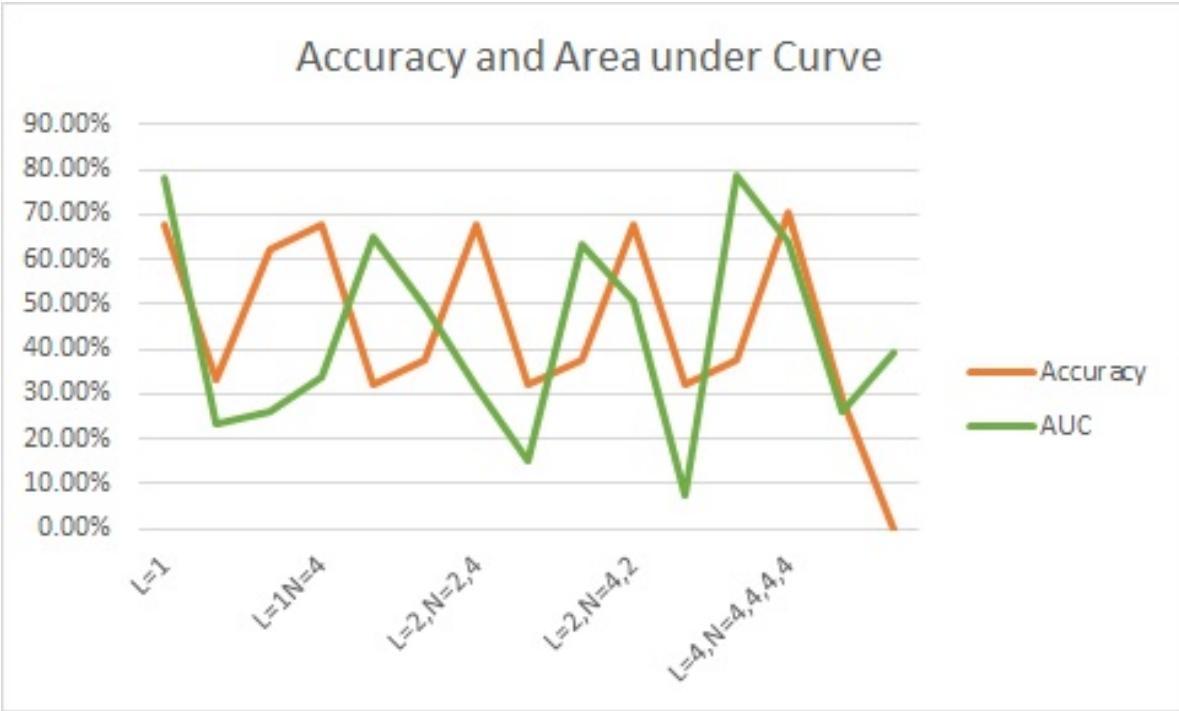

Figure 6.3: Accuracy Of MLP w.r.t Layers And Neurons

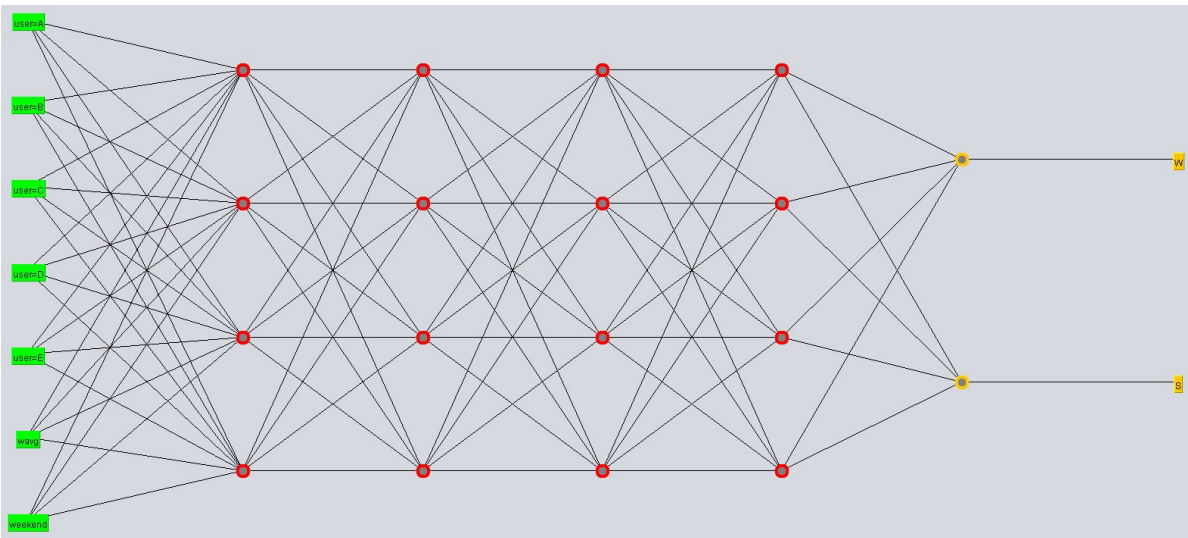

Figure 6.4: MultiLayer Perceptron With Layers=4 And Neuron=4

6.4 Conclusion

In this chapter, we performed data analysis using MLP to gauge its accuracy with relationship classification. This is our preliminary experimental work in the deep learning

domain and we expect to work further in this area in future. We have utilised the data set used in Chapter 4 for user relationship classification based on Mobile phone and Facebook data. Our work concluded that MLP is a good choice for data analysis if the input data size is huge because MLP performs better with greater sizes of data. The number of layers used are key to the success of this model, but there is no bench mark to confirm the standard number of layers to achieve accurate results. In future work, we plan to test the model with a larger size data set to verify the accuracy of MLP. However, present observations drawn from the analysis are as follows:

- With more layers and neurons, the accuracy is higher at an 80% split than at a 50% split, and poor at a 66% split.
- When we have fewer layers and neurons, the accuracy is higher at a 50% split than at an 80% split and poor at a 66% split.
- Area under the curve value is also corresponding with the accuracy, when we use deep MLP.
- Performance increases with the size of data as deep learning is for learning from the data , the more data we feed in, the better performance we get from the model.

CHAPTER 7

CONCLUSION AND FUTURE WORKS

7.1 Conclusions

In this thesis, we have explained how technology pervasiveness in our daily life has resulted in volumes of data generation. The most common contributors to this high volume big data are online social networks, mobile phones and smart IoT based environments. Our research focus is on acquiring these different types of data from a number of sources and using machine learning techniques to analyse this data. This intelligent and automated analysis aids digital forensics by obtaining rapid and detailed information about the individuals who actually produce that information either consciously or unconsciously. We have identified three core components of our research work namely:

- Data from diverse sources (Online social network, Mobile phones, Sensors)
- Digital forensics
- Machine Learning

Our research is a novel combination of digital forensics techniques and machine learning to assist forensics investigation. Most of the research with this combination is used for image analysis and understanding hidden information within visual data. However, our research work has used text-based statistics and metadata to drive our investigative conclusions. This thesis addresses the following research goals:

1. Acquisition of data from smart sources for information forensic as presently there is not any practical mechanism/framework available for IoT forensics

2. Analysis of acquired data using machine learning to obtain forensic artefacts

3. Practical implementation of IoT forensics framework(acquisition and analysis phase)

We have covered our three data sources as separate experiments now but we foresee that if all the three sources of data are combined together, efficiency and accuracy can be increased. This is because every individual makes use of social networks, mobile phones and now smart devices and environments.

We have achieved promising results in forensic triage using the Facebook messenger messages statistic, to identify the close contacts of a phone owner. Moreover, in the smart care environment, we have used sensor-based data to identify any suspicious change in the data along with key elements, which answer the questions often required by investigators.

In chapter 3, we have discussed how social networking information is useful to analyse and understand an individual's behavior. Information available via social networks serves as a good supplement for social engineering attacks and targeted phishing attacks. Law enforcing agencies can obtain digital evidence against criminals/suspects by using this social network activity and resultant data. We found out that a lot of challenges are faced in terms of in-depth data extraction from Facebook. The tools with the ability to get in-depth information usually require the authorization of targeted ID. For research purposes it is important to obtain consent from users whose accounts are used to extract information but if users give consent to use their id for research purpose, they do not use the same account for their usual activities. As a result, the purpose of the research remains unserved. Another challenge is Facebooks rapidly changing APIs and format, consequently making many research-based applications unserviceable. We propose arrangements and collaboration between the research community and online social networks to enhance the security mechanisms. Moreover, Social network data extraction, data reduction mechanisms and feature extraction algorithms development also needs attention. Chapter 3 highlighted that by combining information from social networks, mobile devices, wireless networks and global positioning systems can help in digging down to even finding a person in a building / room. To achieve such granularity requires exceptional co-relational mechanisms and accurate feature extraction.

In chapter 4, we gauged the machine learning classifiers to facilitate mobile forensics, specifically in terms of Facebook messenger artefact triaging. By using 199 data-instances and training three WEKA Classifiers (i.e. ZeroR, J48 and Random tree), we were able to classify the device owner's contact classification into weak, medium and strong (i.e. determine their mutual relationship strength). In this analysis, we employed three test options and three different classifiers. Future directions for this work include application of deep learning algorithms (Artificial neural network- ANN) to voluminous data sets.

Chapter 5 addresses the requirement of elderly individuals whose physical activity is monitored by employing sensors, to assist in risky situations. In this work, sensor data is used to train the machine-learning model to understand the normal values of an individual positional attributes (vertical, frontal and lateral axis acceleration) in a controlled environment. Five (5) prominent machine-learning attributes are used for this model, namely ZeroR Algorithm (for baselining), Support Vector Machine (SVM) Algorithm, Decision Tree (J48) Algorithm, Naive Bayes Algorithm and K-Nearest Neighbours (KNN). Moreover, we have evaluated the effect of feature selection on the performance of the model, which resulted in a confirmation that it actually improved the performance of the model in terms of accuracy. In our analysis, Support vector machine algorithm performed well with the feature-selected data-set, which validates the performance capability of this model with limited data, thus making it appropriate for an IoT based environment where resource efficiency is a significant influence.

7.2 Future Research Directions

Although there have been some developments in the field of digital forensics in recent years, there is still much room for further improvements and extensions in this area. Here, we outline some future directions for enhancing the machine learning based digital forensics presented in this thesis.

One of the prominent contenders to simplify digital forensics challenges is Artificial neural network based deep learning. Deep Learning is a branch of machine learning concerned with algorithms inspired by the arrangement and function of the brain called artificial neural networks(ANN)[64]. Deep learning learns from large amounts of data which makes it a potential research direction for Big Data. It allows machines to solve difficult problems even with a data set that is very diverse, amorphous and interrelated. Modern state-of-the-art deep learning is based on many layers deep neural network models using the back propagation algorithm[104]. One of the most popular ANN techniques

is Multi layer Perceptron Networks (MLP). MLP is most suitable for tabular data, while other ANN techniques such as Convolutional Neural Network are used for image data and Long Short-Term Memory Recurrent Neural Network is appropriate for sequence data. The accuracy of the deep learning models increases with the size of the training set, number of layers and the number of neurons in each layer. It is predictable that a larger data set will give significantly improved results. Deep learning models have been applied in a comprehensive range of artificial intelligence-related applications namely computer vision, facial verification, natural language processing and cybersecurity.

We foresee that deep learning as very impressive potential in digital forensics investigation and for making human-like decisions. Moreover, in smart environments, deep learning has scope for learning from human movement data; the learning can be identifying a person from his movement patterns and providing him with his preferred services or care. There are also privacy implications of machine learning technologies that need consideration. The role of federated learning in such context is very important. Federated Learning is a distributed machine learning approach which enables model training on decentralised data. Federated Learning enables mobile phones to collaboratively learn a shared prediction model while keeping all the training data on device, decoupling the ability to do machine learning from the need to store the data in the cloud. The goal is a machine learning setting where the goal is to train a high-quality centralised model with training data distributed over a large number of clients each with unreliable and relatively slow network connections.

To sum up, seamless integration of intelligence gathered from various data sources calls for more intelligent machine learning based solutions. These solutions can be a combination of the techniques reviewed and proposed in this thesis as well as new techniques, which cater to the needs of IoT and Big Data networks.

Appendix A

A.1

Number of Data Breaches in US
https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/

A.2

Health Insurance Portability and Accountability Act
`https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html?language=en`

A.3

https://www.skyhighnetworks.com/cloud-security-blog/data-integrity-the-next-trend-in-cyber-attacks/

Bibliography

[1] *Correlation*.
https://www.openml.org/a/estimation-procedures/1.
Accessed: 2018-11-27.

[2] *Health Insurance Portability and Accountability Act*.
https://tinyurl.com/u77m5ey.
Accessed: 2018-11-28.

[3] *Health sector data breaches*.
https://tinyurl.com/wq6l9yn.
Accessed: 2018-11-20.

[4] *United states. director of national intelligence james clapper's statement*.
https://tinyurl.com/rls4qgs.
Accessed: 2018-11-20.

[5] *The internet of things in healthcare: An overview*, Journal of Industrial Information Integration, 1 (2016), pp. 3 – 13.

[6] *Recognizing human behaviours in online social networks*, Computers Security, 74 (2018), pp. 355 – 370.

[7] D. Abbott, *Applied predictive analytics: Principles and techniques for the professional data analyst*, John Wiley & Sons, 2014.

[8] S. Agreste, P. De Meo, E. Ferrara, S. Piccolo, and A. Provetti, *Analysis of a heterogeneous social network of humans and cultural objects*, IEEE Transactions on Systems, Man, and Cybernetics: Systems, 45 (2014), pp. 559–570.

[9] L. M. Aiello, A. Barrat, R. Schifanella, C. Cattuto, B. Markines, and F. Menczer, *Friendship prediction and homophily in social media*, ACM Transactions on the Web (TWEB), 6 (2012), p. 9.

[10] O. Y. AL-JARRAH, P. D. YOO, S. MUHAIDAT, G. K. KARAGIANNIDIS, AND K. TAHA, *Efficient machine learning for big data: A review*, Big Data Research, 2 (2015), pp. 87–93.

[11] P. AMIRIAN, F. VAN LOGGERENBERG, AND T. LANG, *Data Science and Analytics*, Springer International Publishing, Cham, 2017, pp. 15–37.

[12] C. ANGLANO, M. CANONICO, AND M. GUAZZONE, *Forensic analysis of telegram messenger on android smartphones*, Digital Investigation, 23 (2017), pp. 31–49.

[13] F. J. APARICIO-NAVARRO, K. G. KYRIAKOPOULOS, Y. GONG, D. J. PARISH, AND J. A. CHAMBERS, *Using pattern-of-life as contextual information for anomaly-based intrusion detection systems*, IEEE Access, 5 (2017), pp. 22177–22193.

[14] H. ARSHAD, A. JANTAN, G. K. HOON, AND A. S. BUTT, *A multilayered semantic framework for integrated forensic acquisition on social media*, Digital Investigation, 29 (2019), pp. 147–158.

[15] H. ARSHAD, A. JANTAN, AND E. OMOLARA, *Evidence collection and forensics on social networks: Research challenges and directions*, Digital Investigation, 28 (2019), pp. 126 – 138.

[16] F. AZUAJE, *Witten ih, frank e: Data mining: Practical machine learning tools and techniques 2nd edition*, BioMedical Engineering OnLine, 5 (2006), p. 51.

[17] K. BARMPATSALOU, T. CRUZ, E. MONTEIRO, AND P. SIMOES, *Current and future trends in mobile device forensics- a survey*, ACM Computing Surveys, 51 (2018), p. 46.

[18] Y. BENGIO AND Y. GRANDVALET, *No unbiased estimator of the variance of k-fold cross-validation*, Journal of machine learning research, 5 (2004), pp. 1089–1105.

[19] L. BILGE, T. STRUFE, D. BALZAROTTI, AND E. KIRDA, *All your contacts are belong to us: automated identity theft attacks on social networks*, in Proceedings of the 18th international conference on World wide web, ACM, 2009, pp. 551–560.

[20] A. P. BRADLEY, *The use of the area under the roc curve in the evaluation of machine learning algorithms*, Pattern recognition, 30 (1997), pp. 1145–1159.

[21] L. BREIMAN, *Random forests*, Machine learning, 45 (2001), pp. 5–32.

[22] J. BROWN, A. J. BRODERICK, AND N. LEE, *Word of mouth communication within online communities: Conceptualizing the online social network*, Journal of interactive marketing, 21 (2007), pp. 2–20.

[23] A. L. BUCZAK AND E. GUVEN, *A survey of data mining and machine learning methods for cyber security intrusion detection*, IEEE Communications Surveys Tutorials, 18 (2016), pp. 1153–1176.

[24] M. BUETTNER, R. PRASAD, M. PHILIPOSE, AND D. WETHERALL, *Recognizing daily activities with rfid-based sensors*, in Proceedings of the 11th international conference on Ubiquitous computing, ACM, 2009, pp. 51–60.

[25] N. D. W. CAHYANI, N. H. AB RAHMAN, W. B. GLISSON, AND K.-K. R. CHOO, *The role of mobile forensics in terrorism investigations involving the use of cloud storage service and communication apps*, Mobile Networks and Applications, 22 (2017), pp. 240–254.

[26] L. CAVIGLIONE, S. WENDZEL, AND W. MAZURCZYK, *The future of digital forensics: Challenges and the road ahead*, IEEE Security & Privacy, 15 (2017), pp. 12–17.

[27] R. CHAKRAVORTY, *A programmable service architecture for mobile medical care*, in Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on, IEEE, 2006, pp. 5–pp.

[28] L. CHEN, L. XU, X. YUAN, AND N. SHASHIDHAR, *Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges*, in 2015 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2015, pp. 1132–1136.

[29] N. CHENG, S. CHEN, P. PATHAK, AND P. MOHAPATRA, *Long-term privacy profiling through smartphone sensors*, in 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, IEEE, 2015, pp. 639–644.

[30] M. CHERNYSHEV, S. ZEADALLY, Z. BAIG, AND A. WOODWARD, *Internet of things forensics: the need, process models, and open issues*, IT professional, 20 (2018), pp. 40–49.

[31] K.-K. R. CHOO, *The cyber threat landscape: Challenges and future research directions*, Computers & Security, 30 (2011), pp. 719–731.

[32] G. COHN, D. MORRIS, S. PATEL, AND D. TAN, *Humantenna: using the body as an antenna for real-time whole-body interaction*, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2012, pp. 1901–1910.

[33] M. CONTI, A. DEHGHANTANHA, K. FRANKE, AND S. WATSON, *Internet of things security and forensics: Challenges and opportunities*, Future Generation Computer Systems, 78 (2018), pp. 544 – 546.

[34] D. J. COOK, *Learning setting-generalized activity models for smart spaces*, IEEE intelligent systems, 2010 (2010), p. 1.

[35] S. COSTANTINI, G. DE GASPERIS, AND R. OLIVIERI, *Digital forensics and investigations meet artificial intelligence*, Annals of Mathematics and Artificial Intelligence, 86 (2019), pp. 193–229.

[36] F. DARYABAR, A. DEHGHANTANHA, AND K.-K. R. CHOO, *Cloud storage forensics: Mega as a case study*, Australian Journal of Forensic Sciences, 49 (2017), pp. 344–357.

[37] F. N. DEZFOULI, A. DEHGHANTANHA, B. ETEROVIC-SORIC, AND K.-K. R. CHOO, *Investigating social networking applications on smartphones detecting facebook, twitter, linkedin and google+ artefacts on android and ios platforms*, Australian Journal of Forensic Sciences, 48 (2016), pp. 469–488.

[38] C. P. DIEHL, G. NAMATA, AND L. GETOOR, *Relationship identification for social network discovery*, in AAAI, vol. 22, 2007, pp. 546–552.

[39] C. N. DOUKAS AND I. MAGLOGIANNIS, *Emergency fall incidents detection in assisted living environments utilizing motion, sound, and visual perceptual components*, IEEE Transactions on Information Technology in Biomedicine, 15 (2011), pp. 277–289.

[40] E. FERRARA, P. D. MEO, G. FIUMARA, AND R. BAUMGARTNER, *Web data extraction, applications and techniques: A survey*, Knowledge-Based Systems, 70 (2014), pp. 301 – 323.

[41] M. W. GARDNER AND S. DORLING, *Artificial neural networks (the multilayer perceptron),Äîa review of applications in the atmospheric sciences*, Atmospheric environment, 32 (1998), pp. 2627–2636.

[42] S. L. GARFINKEL, *Digital forensics research: The next 10 years*, digital investigation, 7 (2010), pp. S64–S73.

[43] I. GHAFIR, M. HAMMOUDEH, V. PRENOSIL, L. HAN, R. HEGARTY, K. RABIE, AND F. J. APARICIO-NAVARRO, *Detection of advanced persistent threat using machine-learning correlation analysis*, Future Generation Computer Systems, 89 (2018), pp. 349 – 359.

[44] E. GILBERT AND K. KARAHALIOS, *Predicting tie strength with social media*, in Proceedings of the SIGCHI conference on human factors in computing systems, ACM, 2009, pp. 211–220.

[45] P. GOPE AND T. HWANG, *Bsn-care: A secure iot-based modern healthcare system using body sensor network*, IEEE Sensors Journal, 16 (2016), pp. 1368–1376.

[46] M. A. HALL, *Correlation-based feature selection for machine learning*, (1999).

[47] M. HASSANALIERAGH, A. PAGE, T. SOYATA, G. SHARMA, M. AKTAS, G. MATEOS, B. KANTARCI, AND S. ANDREESCU, *Health monitoring and management using internet-of-things (iot) sensing with cloud-based processing: Opportunities and challenges*, in 2015 IEEE International Conference on Services Computing, June 2015, pp. 285–292.

[48] C. HASSENFELDT, S. BAIG, I. BAGGILI, AND X. ZHANG, *Map my murder! a digital forensic study of mobile health and fitness applications*, 2019.
cited By 0.

[49] K. S. HOON, K. C. YEO, S. AZAM, B. SHUNMUGAM, AND F. DE BOER, *Critical review of machine learning approaches to apply big data analytics in ddos forensics*, in 2018 International Conference on Computer Communication and Informatics (ICCCI), Jan 2018, pp. 1–5.

[50] M. HUBER, M. MULAZZANI, M. LEITHNER, S. SCHRITTWIESER, G. WONDRACEK, AND E. WEIPPL, *Social snapshots: Digital forensics for online social networks*, in Proceedings of the 27th annual computer security applications conference, ACM, 2011, pp. 113–122.

[51] IEEE, *IEEE IoT Towards Definition Internet of Things*.
`https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf`, 2015.

[Online; accessed 01-Nov-2019].

[52] J. IMGRABEN, A. ENGELBRECHT, AND K.-K. R. CHOO, *Always connected, but are smart mobile users getting more security savvy? a survey of smart mobile device users*, Behaviour & Information Technology, 33 (2014), pp. 1347–1360.

[53] S. M. R. ISLAM, D. KWAK, M. H. KABIR, M. HOSSAIN, AND K. KWAK, *The internet of things for health care: A comprehensive survey*, IEEE Access, 3 (2015), pp. 678–708.

[54] K. A. JALIL, M. H. KAMARUDIN, AND M. N. MASREK, *Comparison of machine learning algorithms performance in detecting network intrusion*, in 2010 international conference on networking and information technology, IEEE, 2010, pp. 221–226.

[55] A. JOSEPH AND K. J. SINGH, *Digital forensics in distributed environment*, in Cloud Security: Concepts, Methodologies, Tools, and Applications, IGI Global, 2019, pp. 1157–1177.

[56] D. M. KARANTONIS, M. R. NARAYANAN, M. MATHIE, N. H. LOVELL, AND B. G. CELLER, *Implementation of a real-time human movement classifier using a triaxial accelerometer for ambulatory monitoring*, IEEE Transactions on Information Technology in Biomedicine, 10 (2006), pp. 156–167.

[57] A. KARIM, R. B. SALLEH, M. SHIRAZ, S. A. A. SHAH, I. AWAN, AND N. B. ANUAR, *Botnet detection techniques: review, future trends, and issues*, Journal of Zhejiang University SCIENCE C, 15 (2014), pp. 943–983.

[58] E. KHADANGI, A. ZAREAN, A. BAGHERI, AND A. BAGHERI JAFARABADI, *Measuring relationship strength in online social networks based on users' activities and profile information*, in ICCKE 2013, 2013, pp. 461–465.

[59] J. KO, J. H. LIM, Y. CHEN, R. MUSVALOIU-E, A. TERZIS, G. M. MASSON, T. GAO, W. DESTLER, L. SELAVO, AND R. P. DUTTON, *Medisn: Medical emergency detection in sensor networks*, ACM Transactions on Embedded Computing Systems (TECS), 10 (2010), p. 11.

[60] R. KOHAVI ET AL., *A study of cross-validation and bootstrap for accuracy estimation and model selection*, in Ijcai, vol. 14, Montreal, Canada, 1995, pp. 1137–1145.

[61] N. KORONIOTIS, N. MOUSTAFA, E. SITNIKOVA, AND J. SLAY, *Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques*, in International Conference on Mobile Networks and Management, Springer, 2017, pp. 30–44.

[62] N. C. KRISHNAN AND D. J. COOK, *Activity recognition on streaming sensor data*, Pervasive and mobile computing, 10 (2014), pp. 138–154.

[63] P. KUMAR AND H.-J. LEE, *Security issues in healthcare applications using wireless medical sensor networks: A survey*, sensors, 12 (2011), pp. 55–91.

[64] Y. LECUN, Y. BENGIO, AND G. HINTON, *Deep learning*, nature, 521 (2015), p. 436.

[65] K. LEE, D. PALSETIA, R. NARAYANAN, M. M. A. PATWARY, A. AGRAWAL, AND A. CHOUDHARY, *Twitter trending topic classification*, in 2011 IEEE 11th International Conference on Data Mining Workshops, Dec 2011, pp. 251–258.

[66] H. LIU, B. LANG, M. LIU, AND H. YAN, *Cnn and rnn based payload classification methods for attack detection*, Knowledge-Based Systems, 163 (2019), pp. 332–341.

[67] M. LUŠTREK AND B. KALUŽA, *Fall detection and activity recognition with machine learning*, Informatica, 33 (2009).

[68] A. MACDERMOTT, T. BAKER, AND Q. SHI, *Iot forensics: Challenges for the ioa era*, in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2018, pp. 1–5.

[69] F. MARTURANA, G. ME, R. BERTE, AND S. TACCONI, *A quantitative approach to triaging in mobile forensics*, in 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Nov 2011, pp. 582–588.

[70] F. MARTURANA AND S. TACCONI, *A machine learning-based triage methodology for automated categorization of digital media*, Digital Investigation, 10 (2013), pp. 193–204.

[71] A. E. MAXWELL, T. A. WARNER, AND F. FANG, *Implementation of machine-learning classification in remote sensing: An applied review*, International Journal of Remote Sensing, 39 (2018), pp. 2784–2817.

[72] M. McPherson, L. Smith-Lovin, and J. M. Cook, *Birds of a feather: Homophily in social networks*, Annual review of sociology, 27 (2001), pp. 415–444.

[73] Z. Minchev, *Cyber threats analysis in on-line social networks with a study on user response*, IT4Sec Reports, 115.

[74] Z. Minchev, *Challenges to human factor for advance persistent threats proactive identification in modern social networks*, Information Security, 34 (2016), pp. 123–136.
Name - North Atlantic Treaty Organization–NATO; Copyright - Copyright Pro-Con Ltd. 2016; Last updated - 2019-07-10; SubjectsTermNotLitGenreText - Bulgaria.

[75] U. ML, *UCI Machine Learning Repository*.
`http://archive.ics.uci.edu/ml/datasets/Activity+recognition+with+healthy+older+people+using+a+batteryless+wearable+sensor`, 2016.
[Online; accessed 01-Nov-2017].

[76] Y. Mo, R. Chabukswar, and B. Sinopoli, *Detecting integrity attacks on scada systems*, IEEE Transactions on Control Systems Technology, 22 (2014), pp. 1396–1407.

[77] Y. Mo and B. Sinopoli, *On the performance degradation of cyber-physical systems under stealthy integrity attacks*, IEEE Transactions on Automatic Control, 61 (2016), pp. 2618–2624.

[78] Y. Mo and B. Sinopoli, *On the performance degradation of cyber-physical systems under stealthy integrity attacks*, IEEE Transactions on Automatic Control, 61 (2016), pp. 2618–2624.

[79] P. Mohamed Shakeel, S. Baskar, V. R. Sarma Dhulipala, S. Mishra, and M. M. Jaber, *Maintaining security and privacy in health care system using learning based deep-q-networks*, Journal of Medical Systems, 42 (2018), p. 186.

[80] P. Naraei, A. Abhari, and A. Sadeghian, *Application of multilayer perceptron neural networks and support vector machines in classification of healthcare data*, in 2016 Future Technologies Conference (FTC), Dec 2016, pp. 848–852.

[81] J. W. Ng, B. P. Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, and G.-Z. Yang, *Ubiquitous monitoring environment for wearable and*

implantable sensors (ubimon), in International Conference on Ubiquitous Computing (Ubicomp), 2004.

[82] H. A. NGUYEN AND D. CHOI, *Application of data mining to network intrusion detection: classifier selection model*, in Asia-Pacific Network Operations and Management Symposium, Springer, 2008, pp. 399–408.

[83] N. NOURELDIEN AND I. YOUSIF, *Accuracy of machine learning algorithms in detecting dos attacks types*, Science and Technology, 6 (2016), pp. 89–92.

[84] F. ORUJOV, R. MASKELIŪNAS, R. DAMAŠEVIČIUS, W. WEI, AND Y. LI, *Smartphone based intelligent indoor positioning using fuzzy logic*, Future Generation Computer Systems, 89 (2018), pp. 335–348.

[85] L. PAGLIARI, R. MIRANDOLA, AND C. TRUBIANI, *A case study to elicit challenges for performance engineering of cyber physical systems*, in Proceedings of the 8th ACM/SPEC on International Conference on Performance Engineering Companion, ACM, 2017, pp. 217–222.

[86] H. PARSONAGE, *Computer forensics case assessment and triage*, 2009.

[87] T. R. PATIL AND S. SHEREKAR, *Performance analysis of naive bayes and j48 classification algorithm for data classification*, International Journal of Computer Science and Applications, 6 (2013), pp. 256–261.

[88] QSR, *NVivo For Windows*.
`http://www.qsrinternational.com/nvivo-product/nvivo11-for-windows`, 2017.
[Online; accessed 03-Feb-2017].

[89] QSRINTERNATIONAL, *NVivo For Windows*.
`http://www.qsrinternational.com/nvivo-support/faqs/what-is-ncapture`, 2017.
[Online; accessed 03-Feb-2017].

[90] D. QUICK AND K.-K. R. CHOO, *Impacts of increasing volume of digital forensic data: A survey and future research challenges*, Digital Investigation, 11 (2014), pp. 273–294.

[91] ——, *Pervasive social networking forensics: intelligence and evidence from mobile device extracts*, Journal of Network and Computer Applications, 86 (2017), pp. 24–33.

[92] D. QUICK AND K.-K. R. CHOO, *Digital forensic intelligence: Data subsets and open source intelligence (dfint+osint): A timely and cohesive mix*, Future Generation Computer Systems, 78 (2018), pp. 558 – 567.

[93] S. RAGHAVAN, *Digital forensic research:current state of the art*, CSI Transactions on ICT, 1 (2013), pp. 91–114.

[94] K. RAPP, C. BECKER, I. D. CAMERON, H.-H. KÖNIG, AND G. BÜCHELE, *Epidemiology of falls in residential aged care: analysis of more than 70,000 falls from residents of bavarian nursing homes*, Journal of the American Medical Directors Association, 13 (2012), pp. 187–e1.

[95] P. P. RAY, *A survey on internet of things architectures*, Journal of King Saud University-Computer and Information Sciences, 30 (2018), pp. 291–319.

[96] P. REFAEILZADEH, L. TANG, AND H. LIU, *Cross-validation*, in Encyclopedia of database systems, Springer, 2009, pp. 532–538.

[97] A. REZAEI AND S. MIRZAKUCHAKI, *A recognition approach using multilayer perceptron and keyboard dynamics patterns*, in 2013 First Iranian Conference on Pattern Recognition and Image Analysis (PRIA), March 2013, pp. 1–5.

[98] B. RIEDER, *Studying facebook via data extraction: the netvizz application*, in Proceedings of the 5th annual ACM web science conference, ACM, 2013, pp. 346–355.

[99] P. ROGAWAY, M. BELLARE, AND J. BLACK, *Ocb: A block-cipher mode of operation for efficient authenticated encryption*, ACM Transactions on Information and System Security (TISSEC), 6 (2003), pp. 365–403.

[100] V. ROUSSEV, C. QUATES, AND R. MARTELL, *Real-time digital forensics and triage*, Digital Investigation, 10 (2013), pp. 158–167.

[101] D. E. RUMELHART, G. E. HINTON, AND R. J. WILLIAMS, *Learning representations by back-propagating errors*, nature, 323 (1986), pp. 533–536.

[102] M. SABHNANI AND G. SERPEN, *Application of machine learning algorithms to kdd intrusion detection dataset within misuse detection context.*, in MLMTA, 2003, pp. 209–215.

[103] M. B. SALEM, S. HERSHKOP, AND S. J. STOLFO, *A survey of insider attack detection research*, in Insider Attack and Cyber Security, Springer, 2008, pp. 69–90.

[104] J. SCHMIDHUBER, *Deep learning in neural networks: An overview*, Neural networks, 61 (2015), pp. 85–117.

[105] A. S. SHAH, M. SHAH, M. FAYAZ, F. WAHID, H. KHALID KHAN, AND A. SHAH, *Forensic analysis of offline signatures using multilayer perceptron and random forest*, International Journal of Database Theory and Application, 10 (2017), pp. 139–148.

[106] P. SINGLA AND M. RICHARDSON, *Yes, there is a correlation:-from social networks to personal behavior on the web*, in Proceedings of the 17th international conference on World Wide Web, ACM, 2008, pp. 655–664.

[107] M. STONE, *Cross-validatory choice and assessment of statistical predictions*, Journal of the royal statistical society. Series B (Methodological), (1974), pp. 111–147.

[108] R. L. S. TORRES, D. C. RANASINGHE, Q. SHI, AND A. P. SAMPLE, *Sensor enabled wearable rfid technology for mitigating the risk of falls near beds*, in 2013 IEEE International Conference on RFID (RFID), April 2013, pp. 191–198.

[109] A. UMAIR, *Facebook Usage Survey*.
`https://goo.gl/forms/V999FzcsKQwEadKv1`, 2017.

[110] A. UMAIR, P. NANDA, AND X. HE, *Online social network information forensics: A survey on use of various tools and determining how cautious facebook users are?*, in 2017 IEEE Trustcom/BigDataSE/ICESS, IEEE, 2017, pp. 1139–1144.

[111] A. UMAIR, P. NANDA, AND X. HE, *Online social network information forensics: A survey on use of various tools and determining how cautious facebook users are?*, in 2017 IEEE Trustcom/BigDataSE/ICESS, Aug 2017, pp. 1139–1144.

[112] N. UNIES, *World population ageing 2013*, New York, United Nations, Department of Economic and Social Affairs, Population Division, n¬∞$ST/ESA/SER.A/348$,(2013).

[113] D. WALNYCKY, I. BAGGILI, A. MARRINGTON, J. MOORE, AND F. BREITINGER, *Network and device forensic analysis of android social-messaging applications*, Digital Investigation, 14 (2015), pp. S77 – S84.
The Proceedings of the Fifteenth Annual DFRWS Conference.

[114] S. WATSON AND A. DEHGHANTANHA, *Digital forensics: the missing piece of the internet of things promise*, Computer Fraud & Security, 2016 (2016), pp. 5–8.

[115] R. WEINSTEIN, *Rfid: a technical overview and its application to the enterprise*, IT professional, 7 (2005), pp. 27–33.

[116] R. XIANG, J. NEVILLE, AND M. ROGATI, *Modeling relationship strength in online social networks*, in Proceedings of the 19th international conference on World wide web, ACM, 2010, pp. 981–990.

[117] T. Y. YANG, A. DEHGHANTANHA, K.-K. R. CHOO, AND Z. MUDA, *Windows instant messaging app forensics: Facebook and skype as case studies*, PLOS ONE, 11 (2016), pp. 1–29.

[118] I. YAQOOB, I. A. T. HASHEM, A. AHMED, S. A. KAZMI, AND C. S. HONG, *Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges*, Future Generation Computer Systems, 92 (2019), pp. 265–275.

[119] S. YU, G. WANG, AND W. ZHOU, *Modeling malicious activities in cyber space*, IEEE network, 29 (2015), pp. 83–87.