International Engineering Journal For Research & Development

Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

AN OVERVIEW OF CYBER FORENSIC APPROACHES FOR CYBER SECURITY AND DATA SECURITY

M. G. Tingane
Innovation and Entrepreneurship Development Center,
Prof Ram Meghe College of Engineering and Management,
Badnera, Amravati, India
monali.tingane@gmail.com

M. S. Ali
Innovation and Entrepreneurship Development Center,
Prof Ram Meghe College of Engineering and Management,
Badnera, Amravati, India
softalis@gmail.com

A. P. Bhagat
Innovation and Entrepreneurship Development Center,
Prof Ram Meghe College of Engineering and Management,
Badnera, Amravati, India
amol.bhagat@gmail.com

Abstract-

Cyber Forensics is fairly new as a scientific discipline and deals with the acquisition, authentication and analysis of digital evidence. Although it is a relatively new field, the challenges and opportunities changed dramatically. Technology in general and computers specifically, since their introduction and dissemination into mainstream society, have benefited society, there is also a sinister, dark side to this technology when it is abused. In recent years, society has seen the rise in abuse of various kinds— personal or private and corporate, conducted with, through or by technology. Cyber threats are growing in number and complexity. Cyber warfare is becoming a reality. Therefore, it is important to continually study and improve all dimensions of cyber defense. For this purpose different systems, which deals with the detection of new unknown malicious attacks are reviewed in his paper. This paper deals with the comparative analysis of different detection techniques use in forensic analysis like unknown malicious microsoft office documents, geolocation, process memory investigation of the bitcoin clients electrum and bitcoin core, common database forensic investigation processes, network flow watermark for data exfiltration traceback, object-dependent methods to analyze the evidence of illegal activities, Identity-Based integrity auditing and data sharing, e-Supply chain digital forensic readiness systems, automated keyword extraction, dynamically analyzing and monitoring obfuscated android applications, analyzing chat logs using data mining and natural language processing techniques, forensics and deep learning mechanisms for botnets in Internet of Things, machine learning system for Cyber-Attack detection in Large-Scale Smart Grids, framework for detecting manipulated smartphone data, location-based social network homogenous network model etc. Both physical and remote attacks are considered in this analysis.

Keywords—Cyber Forensic, Malicious Attack, Cyber Defense, Forensic Analysis, Cyber-Attack Detection

I. INTRODUCTION

As computers become more advanced, so do criminal activities. Therefore, the computer forensics niche is in constant progression along with the technological advancements of computers. Years ago, most crimes had evidence that pertained to the physical world. Nowadays, digital evidence has become of paramount importance. Subsequently, forensic sciences extended their scope to include digital evidence, thus, a new domain was born – Cyber Forensics (CF) [1]. A major challenge in this field is coping with vast amounts of data during investigations now days the trend is that everything has become digital. For instance books, photos, letters and Long Playing records (LPs) turned into e-books, digital photos, e-mails and mp3s. Additionally, we now have smartphones providing Internet access virtually everywhere, which in turn increased the daily usage of social media like Facebook or Twitter. CF is a discipline that only started gaining notoriety in the scientific community over the last decade. Although it is a relatively new field, the challenges and opportunities changed dramatically during that time. To date, most of the research efforts in CF have focused on ways of extracting data that may become weighty evidence in the court of law [2].

Computer/Digital forensic is a growing field. It combines computer science concepts including computer architecture, operating systems, file systems, software engineering, and computer networking, as well as legal procedures. At the most basic level, the digital forensic process has three major phases; Extraction, Analysis, and Presentation. Nevertheless, there exist others forensic process models, each of them rely upon reaching a consensus about how to describe digital forensics and evidences [3]. Like any physical evidence, digital evidence needs to be validated for the legal aspects in the court of law. In order for the evidence to be accepted by the court as valid; chain of custody for digital evidence must be kept, or it must be known who exactly,

when, and where came into contact with the evidence at each stage of the investigation. Advancing the state of the art in the CF domain strongly depends on novel methods and algorithms that can help in the identification of evidence during a case to speed up the forensics process. Some scientific efforts have been pursued such as digital forensics triage in order to improve the overall digital forensics process. However, the field has some challenges to overcome in order to improve the state-of-the-art, which we discuss in the sections that follow.
Therefore, we focused on building a cybercrime forensics analysis for investigation of real-world cybercrime that can be applied to data mining of cybercrime. We constructed the review by including the categories cybercrime, evidence, laws, information on criminals and crime cases, based on the cybercrime in different cases. In the following Section 2, we discuss related studies concerning cyber forensic, the existing cyber forensics systems, and technology. In Section 3, we provide comparative analysis of different detection techniques use in forensic analysis, along with the areas in which it can be applied. In Section 4, we draw conclusions.

II. RELATED WORK

Use of Geolocation for the Strategic Preincident Preparation of an IT Forensics Analysis is proposed in [4]. In the area of network forensics, the concept of "strategic preincident preparation" is receiving higher attention throughout the last years. Following the ideas of the strategic preparation, the central idea of this publication is to create, in advance, an optimal starting point on which a forensic investigation will be based on. For this purpose, this paper show how, with the use of geolocation, a good database can be created in advance that then allows much more comprehensive analysis of intrusions. Similar to the concept of IP reputation, define the concept of georeputation, which serves as the basis to determine the degree of the data recorded.

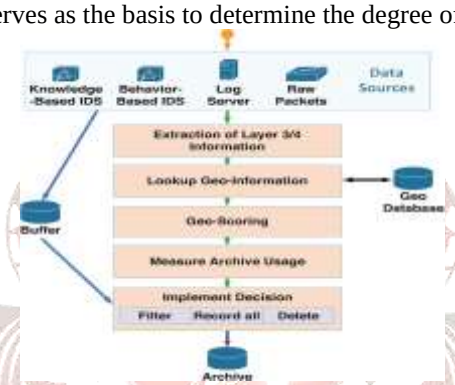

Fig. 1. Overview of the workflow of the architecture.

ALDOCX System is discussed in [5], Attackers usually use social engineering in order to encourage recipients to press a link or open a malicious web page or attachment. This study present ALDOCX – a framework and new structural feature extraction methodology (SFEM) that is aimed at the accurate detection of malicious Microsoft Word XML-based (∗.docx) files. ALDOCX is an active learning based framework for frequently updating the detection model with docx files. ALDOCX focuses on improving the detection mode by labeling the docx files that are most likely to improve the detection model's performance and, in so doing, enrich the signature repository with as many new malicious docx files as possible, thus enhancing the detection process. Specifically, the ALDOCX framework favors files that contain new content.

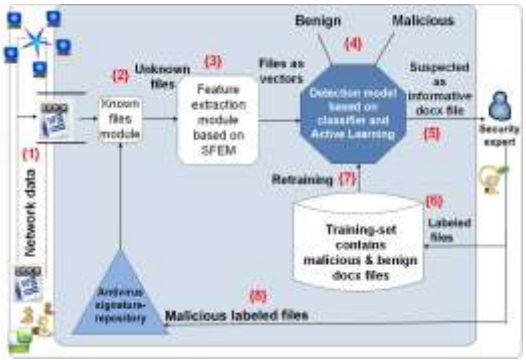

Fig. 2. ALDOCX framework

Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core is proposed in [6], with recent advances in Information and Communications Technologies (ICT) and pervasiveness of popular consumer devices (e.g. Android and iOS devices), digital and cryptocurrencies such as Bitcoin, Litecoin, Freicoin, and

Peercoin are becoming increasingly popular in e-commerce. Such currencies, however, can be abused by criminals. For example, it has been reported that Bitcoin was used to purchase illicit drugs online to pay criminals in return for the decryption key/password in ransomware incidents, and for money laundering and terrorism financing. It has also been reported that some Darknet marketplaces implement cryptocurrency wallets natively. Despite Bitcoins and other virtual currencies being a potential source of evidence, there has been limited research on virtual currency forensics. Existing forensic research on Bitcoins focus on the Blockchain, rather than Bitcoin enduser software or on the potential to forensically recover data using memory analysis. This gap is address in this paper. This paper, examine two popular Bitcoin clients, namely: Bitcoin Core and Electrum, and seek to recover artefacts relating to Bitcoin use from memory.

CDBFI processes are discussed in [7], Data are likely to be in different formats and of different sizes. Hence, the process or procedures that are used in a digital investigation directly impact the results of the examination. Selecting investigative processes that do not fit, potentially, leads to incomplete and/or loss of evidence. This incomplete or missing data may lead to indecisive consequences and give invalid conclusions. The diversity in scenarios and resulting details perceivably make it challenging, or even complicated, particularly for newer forensic investigators, to adopt accurate or proper investigation models Due to the lack of a generic/common database forensic investigation process model, this study provides a structure, referred to as the Common Database Forensic Investigation Process (CDBFIP), which unifies, facilitates, and shares knowledge of database forensic investigation processes among database users and practitioners. Unifying these processes in a single abstract diagram increases the knowledge available to users, newcomers, and practitioners.

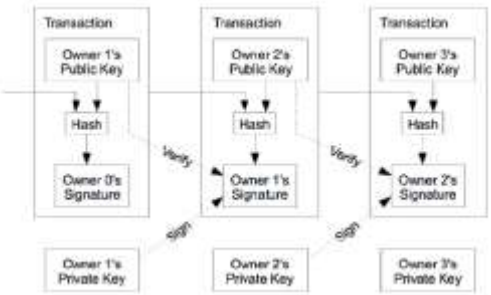

Fig. 3. Bitcoin chain of transactions.

[8] Proposes DROPWAT, This paper proposes DROPWAT, an invisible network flow watermarking technique for data exfiltration attacks, enabling the identification of the staging server that receives the exfiltrated data. DROPWAT is based on a completely new paradigm of injecting a watermark into the flow. The basic idea of our algorithm is to drop a few selected packets of a flow in order to alter the interpacket delay. It show that: (i) packet drop events can be identified, even in the presence of several stepping stones, and that they can be used as a way to convoy a watermark into traffic flows, (ii) natural packet loss and intentional packet drop events in the network cannot be distinguished from each other, and (iii) the watermark embedded with our technique is invisible under some assumptions. DROPWAT is evaluated under different network scenarios with different conditions of packet loss and throughput on real traffic on the Internet.

A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus is proposed in [9], the typical approach utilizes host based forensics techniques, which consists of some agents that embed a virtual machine. But this method has the risk of being attacked, and the ability to resist destruction is poor. This paper presents a real-time Correlation of host-level events in Cyber Range Service (C2RS) method. C2RS implements an out-of-band data capturing mechanism for greater attack resistance utilizing virtual machine introspection technology. This approach allows C2RS to isolate the data captured from monitored hosts. C2RS leverages these captured data by incorporating them into the Volatility framework to aid in simplifying the analysis of operating system memory structures. To aid the trainees aware the cyber security situational in cyber range, proposed an object dependent method to achieve the evidence of illegal activity. The proposed C2RS method is scalable and robustness, which makes this method more applicable to other tasks.

Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage is given in [10], it is important to accomplish remote data integrity auditing on the condition that the sensitive information of shared data is protected. Authors investigate how to achieve data sharing with sensitive information hiding in remote data integrity auditing, and propose a new concept called identity-based shared data integrity auditing with sensitive information hiding for secure cloud storage. In such a scheme, the sensitive information can be protected and the other information can be published. Design a practical identity-based shared data integrity auditing scheme with sensitive information hiding for secure cloud storage. A

sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file. Besides, that this scheme is based on identity-based cryptography, which simplifies the complex certificate management. The result shows that the proposed scheme achieves desirable security and efficiency.

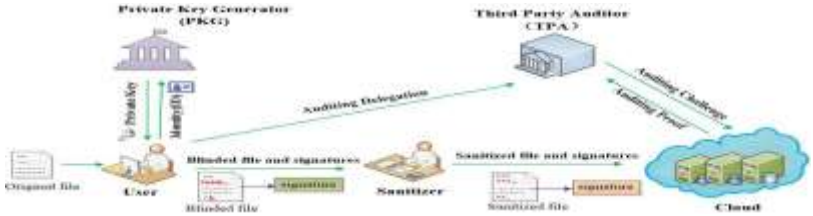

Fig. 4. The system model.

eSC DFR systems is discussed in [11], The problem pursued in this paper is that there are no DFR systems that are designed specifically for the eSC environment. Digital forensics is the use of specialized techniques for the extraction, preservation, identification, authentication, examination, analysis and documentation of digital information from any environment. This procedure is often called upon in response to the occurrence of an incident and not as a proactive process that is incorporated in the design of eSC systems. Industry's standard tools such as the EnCase forensic tool and the Forensic Tool Kit (FTK) application do not incorporate DFR properties in their specifications, which is a proactive forensic process. Therefore, in this paper, the authors present an eSC-DFR process model that can be viewed as the methodology for achieving DFR in an eSC environment and a system-design model that is to be used as a blueprint for the design of next-generation eSCDFR systems.

Use of Automated Keyword Extraction to Facilitate Team Discovery in a Digital Forensic Investigation of Electronic Communications is discussed in [12]; proposed techniques use machine learning and data-mining techniques to guide the

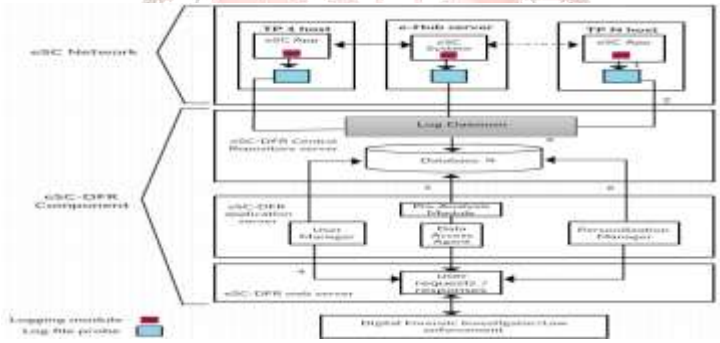

Fig. 5. Architecture of the ESC-DFR System

investigator's efforts. These techniques and tools save time and allow the investigator to more quickly find results that could lead to evidence. This paper shows that techniques used in team formation (TF) discovery can be applied to the Digital
Forensics (DF) task to automatically discover potential teams involved in the crime. This means that the investigator has a much smaller set of potential culprits to start investigating, than using more traditional investigation techniques. It also has the benefit that the investigator does not need to look at the data of potentially innocent persons whose data happens to form part of the corpus. This has positive implications for privacy. Further show that by using automated keyword extraction that TF can be further aided by identifying potentially telling keywords and phrases that identify persons within the corpus.

DexMonitor system is proposed in [13], A repackaging attack happens when a paid or free application in the market is illicitly reverse-engineered, modified, and then redistributed by attackers rather than its original developers. To address such issues, Android application developers use various obfuscation techniques to make their applications more difficult for attackers to dissect. Consequently, rogue application developers can also use these obfuscation techniques to hide malicious behaviors in an application. These techniques are widely used in Android application obfuscators. Static analysis of obfuscated Android applications is tedious and error-prone, and requires extensive analysis experience. In addition, static analysis can be easily defeated by encryption-based obfuscation techniques. Therefore, it is imperative to develop novel ways to analyze obfuscated applications. In addition, it would help achieve the following goals: (1) extraction of malicious applications'

hidden bytecode prior to any in-depth analysis; (2) measurement of the effectiveness of the obfuscators; and (3) understanding of design requirements for building more robust obfuscation techniques.

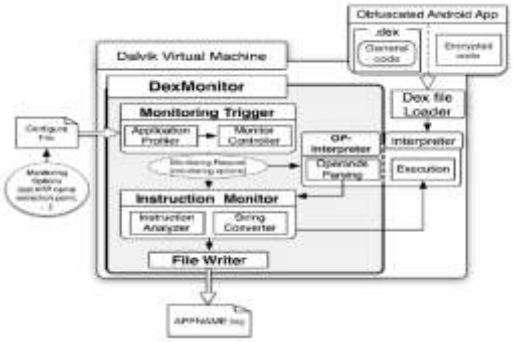

Fig. 6. The architecture of DexMonitor.

Wordnet-Based Criminal Networks Mining for Cybercrime Investigation is provided in [14], Most of the chat and IM systems have an archive feature that stores all conversations for later reference. If the investigator gets access to the archived conversations in confiscated computers or in public chat servers, those conversations can be helpful in crime investigation. However, manually analyzing a large volume of chat conversations to find evidence related to a criminal case is very tedious and time consuming. To address the limitations of existing forensic search tools, author propose a framework that extracts communities from a given chat log and uses agglomerative clustering to find and summarize the topics of interest in the identified communities. Crime investigators can perform a search query and see the results in the designed visualizer. The purpose of this data mining framework is to collect instinctive and interpretable evidence from a chat log to simplify and facilitate the investigation process, especially in the initial stage when there are not enough indications for the investigator to start with.

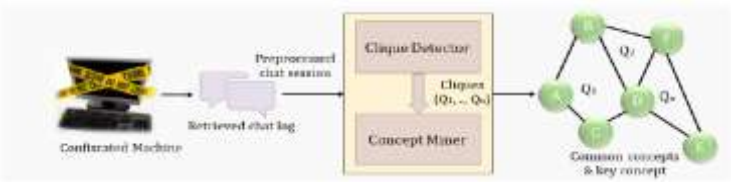

Fig. 7. Overview of the proposed framework.

[15] Proposes forensics and Deep Learning Mechanisms for Botnets in IoT, Attacks, Some botnets have been designed to launch several types of diverse cyber-attacks such as identity/data theft, where the Bot-code infecting a machine gathers sensitive user information and sends it to the botmaster, e-mail spamming, send fake e-mail, key logging, maleware propagation, or other Internet nodes. With such destructive attacks on the rise, it is clear that security and forensics in the IoT should become a priority for research. This paper, provide a comprehensive background for the IoT, botnets and forensics, followed by a taxonomy of recent methods for botnet identification and tracking. Provide a new definition for the IoT, which ABBA. Investigate the applicability of deep learning in network forensics, and the inherent challenges that appear when network forensics techniques are applied to the IoT. In addition, determine future directions for research related to performing forensics investigations of IoT powered botnets.

A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids is discussed in [16], This work, propose a smart grid anomaly detection method to extract the patterns of changes in FDI attacks. The revealed features are employed to detect the attacks in realtime. Symbolic Dynamic Filtering (SDF) is used to build a computationally efficient feature extraction scheme to discover causal interactions between the smart grids sub-systems through DBN. Mutual Information (MI), DBN and learning algorithms are used to detect unobservable cyber-attacks based on free energy as the anomaly index. Authors goal is to capture dependencies between variables through associating of a scalar energy to each variable, which serves as a measure of compatibility. The scalability of the proposed technique is examined on various IEEE test systems. The results show high accuracy and low false alarm under different operation conditions. The proposed method does not only relies on the pattern in the training data sets but it also uses the concept of free energy to differentiate between the energy level in the attacked and normal data sets. Therefore, even new and unseen attacked can be detected.

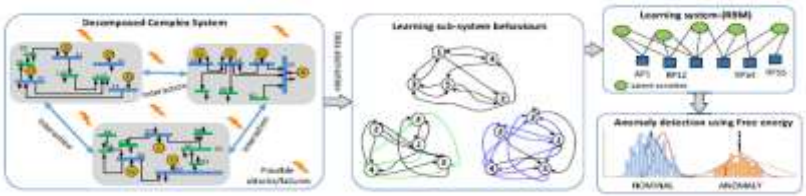

Fig. 8. Proposed framework for cyber-attack detection using unsupervised learning.

Evaluation Framework for Detecting Manipulated Smartphone Data is provided in [17], this paper attempts to establish an evaluation framework that assists with the identification of manipulated smartphone data on both Android and iOS platforms. To construct such a framework, it is necessary to determine what manipulative changes can be applied to smartphone data. The steps followed to perform the manipulation form a generic process to generalize the manipulation techniques. Such manipulation of smartphone data is essentially an attack on the data's integrity and is best described using an attack tree. Using the attack tree, key traces left behind due to the manipulation of smartphone data leads to the formulation of the evaluation framework, which provides key indicators for digital forensics professionals to identify and pinpoint manipulated smartphone data. Weights assigned to the indicators allow for the detection of manipulated smartphone data with a certain probability. The immediate challenges to address in this paper are thus the following: development of an effective and generic process to manipulate smartphone data on both Android and iOS platforms and construct an evaluation framework capable of detecting manipulated smartphone data.

Social Relationships and Temp-Spatial Behaviors Based Community Discovery to Improve Cyber Security Practices is discussed in [18], this paper proposes a LBSN homogeneous network model (LSHNM) based on users' social, temp-spatial and behavioural information. In order to solve community discovery problem in LBSN, one intuitive idea is to refactor the LBSN heterogeneous network. More specifically, it first deletes location vertices and all edges from original LBSN topology, and then creates new links between users based on user characteristics in LBSN community; finally community discovery algorithm can be directly applied to above new network topology. The first step is to analyze and clean the acquired LBSN data which is provided to other modules as data source. The next step is to quantify the similarity between users in LBSN from three characteristics: social relations, temp-spatial distribution and behavioral patterns. Then, LBSN homogeneous network topology is built based on above three characteristics similarity. Finally, high-speed and stable community discovery algorithm will be used to find multi-attribute community in LBSN with the help of above new topology.

Following section provides the comparative analysis.

III COMPARATIVE ANALYSIS OF DIFFERENT DETECTION TECHNIQUES USE IN CYBER FORENSIC

TABLE I COMPARATIVE ANALYSIS OF VARIOUS CYBER FORENSIC DETECTION TECHNIQUES

Title	Aim	Methodologies used	System Name	Purpose for which it is generated	Experimentation Carried Out	Features	Experimentation/ Survey Result
Using Geolocation for the Strategic Preincident Preparation of an IT Forensics Analysis	To investigates accuracy and reliability of geoinformation and provides its own geolocation architecture and a corresponding prototype.	Geobased Strategic preincident preparation	NA	Attack traceability and attribution in IT forensics	An architecture that uses geolocation and applies it to the topic of IT forensics was presented.	To create, in advance, an optimal starting point on which a forensic investigation will be based on (preincident)	The prototype and the evaluation have shown that the approach is useful in practice and therefore has a clear added value. On the other hand, we have also managed to increase the accuracy of the underlying geolocation algorithm significantly..
ALDOCX: Detection of Unknown Malicious Microsoft Office Documents Using Designated Active Learning Methods Based on New Structural Feature Extraction Methodology	Aimed at accurate detection of new unknown malicious docx files.	Machine-learning algorithms with Structural Feature Extraction Methodology	ALDOCX	To provide an improved updating solution for the detection model, as well as the anti-virus software .	Evaluated framework through three comprehensive experiments using the dataset built.	ALDOCX integrates active learning (AL) methods, which are designed to efficiently assist anti-virus vendors by better focusing their experts' analytical efforts	The evaluation results show that by using ALDOCX and SFEM, we achieved a high detection rate of malicious docx files (94.44% TPR) compared with the antivirus software (85.9% TPR)—with very low

						and enhance detection capability	FPR rates (0.19%).
Process Memory Investigation Of The Bitcoin Clients Electrum And Bitcoin Core	The aims is to identify potential sources and types of potential relevant data	The process memory of two popular bitcoin clients, bitcoin Core and electrum, is examined	NA	Bitcoin cryptocurrency is reportedly one widely used digital currency in criminal activities, this study forensically examined Bitcoin Core and Electrum, two popular Bitcoin clients	Artefacts obtained from the process memory are also studied with other artefacts obtained from the client device	Data of forensic interest can be extracted from memory by scanning the process memory fingerprints identified in this research or by searching fixed patterns with regular expressions (e.g. Bitcoin addresses or file paths).	Findings from this study suggest that both bitcoin Core and electrum's process memory is a valuable source of evidence, and many of the artefacts found in process memory are also available from the application and wallet files on the client device (disk).
CDBFIP: Common Database Forensic Investigation Processes for Internet of Things	This study aim to provide a structure, referred to as the CDBFIP	Evaluate real world IOT Cases	CDBPIF	CDBFIP, which unifies, facilitates, and shares knowledge of database forensic investigation processes among database users and practitioners .	Processes were grouped and refined based on common objectives to identify mutual investigation processes.	The proposed common investigation processes for database forensics was validated against nine existing database forensic models.	This analysis resulted in the Common Database Forensic Investigation Processes (CDBFIP)
DROPWAT: An Invisible Network Flow Watermark for Data Exfiltration Traceback	To develop an invisible network flow watermarking technique for data exfiltration attacks	Network Flow Watermarking technique	DropWat	To enable the identification of the staging server that receives the exfiltrated data	Experiments are conducted using the TOR anonymous network in place of the stepping stones	DROPWAT's embedding algorithm is based on a new paradigm to impress a watermark within a network flow.	Results show that the detection algorithm is able to identify an embedded watermark, achieving over 95% accuracy while being invisible
A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus	Implements out-of-band data capturing for greater attack resistance with virtual machine introspection technique	C2RS	NA	Provide an object-dependent method to analyze the evidence of illegal activity.	Extensive experiments is conducted to evaluate the functions and performance of C2RS in a dynamic service.	proposed C2RS method is scalable and robustness, which makes this method more applicable to other tasks	Experimental results shows that the proposed method is effective for real-time correlation of host-level events in cyber range service
Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage	To propose remote data integrity auditing to guarantee the integrity of the data stored in the cloud	Identity-based cryptography	NA	To makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden	Security analysis and performance evaluation is carried out.	The propose scheme is based on identity-based cryptography, which simplifies the complicated certificate management.	The security analysis and the performance evaluation show that the proposed scheme is secure and efficient.
Using a standard approach to the design of next generation e-Supply Chain Digital Forensic Readiness systems	It must be able to provide law enforcement/digital forensic investigators (DFI) with forensically sound and readily available potential digital evidence	Digital Forensic Readiness	eSCs DRF systems	To address the problem for the lack of a well-formulated DFR approach that can assist system developers in the development of e-supply chain digital forensic readiness systems	The authors elaborate more on the design of the remote probes and key factors to consider for system reliability and secure storage.	To design a high-level architecture of an eSC-DFR system that can provide useful data to digital forensic investigators and law enforcement agents to aid in digital forensic investigations.	The limitations identified in current DFR tools and the proposed eSC-DFR process model is created
Using Automated Keyword Extraction to Facilitate Team Discovery in a Digital Forensic Investigation	Simple information retrieval and keyword extraction	Information retrieval and keyword extraction	NA	TF task can be re-formulated to fit the DF arena: to commit a crime, the	Series of experiment is carried out.	the proposed techniques should not be considered to be an automated system for solving	Presented results using information retrieval techniques as well as using automated keyword

of Electronic Communications	techniques can be used to automatically discover potential teams from the data, while preserving privacy	techniques		culprit(s) may require the assistance of several other individuals, which implies that a team of some sort gets established.		a cyber-crime, these techniques should only act as a guide for the investigator	extraction which extracted phrases and keywords and ranked the relative importance of such phrases as an input to identifying candidate teams.
DexMonitor: Dynamically Analyzing and Monitoring Obfuscated Android Applications	Propose a novel approach to analyze Android applications by selectively intercepting Dalvik instructions	Dalvik Virtual Machine, Dalvik Bytecode Obfuscation	DexMonitor	implement a prototype, called DexMonitor, by modifying the Dalvik VM.	To evaluate the performance overhead of DexMonitor, used two benchmark applications, namely Android and SciMark.	Statically analyzing Android applications is tedious and requires tremendous expertise, an new approach to analyze Android bytecode is proposed here	This result ensures that all proposed tasks are reasonably performed
Wordnet-Based Criminal Networks Mining for Cybercrime Investigation	To analyze chat logs for crime investigation	Data mining and natural language processing techniques	NA	To extracts the social network from chat logs and summarizes conversation into topics	The validity of proposed framework is tested by , working in a joint effort with the cybercrime unit of a Canadian law enforcement agency.	Customized notion of a clique for criminal communities mining Concept identification without any prior knowledge, Flexibility to adopt domain knowledge	Experimental outcomes on real-life data and feedback from the law enforcement officers suggest that the proposed chat log mining framework meets the need for law enforcement agencies and is very effective for crime investigation
Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions	To provide a review of forensics and deep learning mechanisms	Deep Learning	NA	To investigate botnets and their applicability in the IoT environments	A review of forensics and deep learning mechanisms in the IoT environments in carried out here	Provide a new definition for the IoT, in addition to a taxonomy of network forensic solutions.	Review provides future direction for research in this field
A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids	An unsupervised anomaly detection based on statistical correlation between measurements is proposed.	Symbolic dynamic Filtering (SDF)	NA	Goal is to design a scalable anomaly detection engine suitable for large-scale smart grids	The simulation results on IEEE 39, 118, and 2848 bus systems verify the performance	A model-free approach, which can be employed in hierarchical and topological networks for different attack scenarios	The results show an accuracy of 99%, true positive rate of 98%, and false positive rate of less than 2%
Evaluation Framework for Detecting Manipulated Smartphone Data	To investigate the effects of manipulating smartphone data on both the Google Android and Apple iOS platforms.	Evaluation framework for Mobile forensic	NA	The purpose of this research study was to assist digital forensic professionals with the detection of manipulated smartphone data	It involves 3 distinct theoretical scenarios: deletion and modification of existing data, as well as a failed attempt to insert fabricated data.	Development of an effective and generic process to manipulate smartphone data and construct an evaluation framework capable of detecting manipulated smartphone data.	Results produced by the evaluation framework suggest the framework can assist with the detection of manipulated smartphone data.
Social Relationships and Temp-Spatial Behaviors Based Community Discovery to Improve Cyber Security Practices	To calculate the user similarity relations in multi-dimensional features	Non-negative matrix decomposition (NMF)	LBSN homogeneous network model (LSHNM)	To construct LBSN isomorphism network topology, which can be used to improve cyber security practices	Non-negative matrix decomposition (NMF) is used to find communities from above isomorphism network topology.	Proposes a LBSN homogeneous network model based on users' social, temp-spatial and behavioural information.	The experimental results show that the LSHNM can find more satisfactory community structures.

IV. CONCLUSION

In this paper, different cyber forensic detection techniques are analyzed. The features of all these systems are compared in TABLE 1. It includes analysis of malicious microsoft office documents, geolocation, process memory investigation, common database forensic investigation processes, network flow watermark for data exfiltration traceback, object-dependent methods to analyze the evidence of illegal activities, Identity-Based integrity auditing and data sharing, eSC DFR systems, automated keyword extraction, dynamically analyzing and monitoring obfuscated android applications, analyzing chat logs, forensics and deep learning mechanisms for botnets in IOT , machine learning system for Cyber-Attack detection, framework for detecting manipulated smartphone data, LBSN homogenous network model etc. Both physical and remote attacks are considered in this analysis.

REFERENCES

[1] Casey, E. (2011). *Digital evidence and computer crime: forensic science, computers and the internet*. Academic press.
[2] Garfinkel, S., Farrell, P., Roussev, V., & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. *digital investigation*, *6*, S2-S11.
[3] Michael W. Andrew "Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media" Proceedings of the 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering SADFE 2007.
[4] Robert Koch, Mario Golling, Lars Stiemert, and Gabi Dreo Rodosek, "Using Geolocation for the Strategic Preincident Preparation of an IT Forensics Analysis", IEEE SYSTEMS JOURNAL, VOL. 10, NO. 4, pp. 1338-1349, DECEMBER 2016.
[5] Nir Nissim, Aviad Cohen, and Yuval Elovici," ALDOCX: Detection of Unknown Malicious Microsoft Office Documents Using Designated Active Learning Methods Based on New Structural Feature Extraction Methodology", IEEE Transactions On Information Forensics And Security, Vol. 12, No. 3, pp. 631-646, March 2017.
[6] Luuc Van Der Horst, Kim-Kwang Raymond Choo, Nhien-An Le-Khac, "Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core", Special Section on Research Challenges and Opportunities in Security And Privacy of Blockchain Technologies, Volume 5 , Pp. 22385-22398, October 5, 2017.
[7] Arafat Al-Dhaqm, Shukor Razak, Siti Hajar Othman, Kim-Kwang Raymond Choo, William Bradley Glisson, Abdulalem Ali, Mohammad Abrar, "CDBFIP: Common Database Forensic Investigation Processes for Internet of Things", Special Section On Intelligent Systems For The Internet of Things, VOLUME 5, pp. 24401-24416, October 13, 2017.
[8] Alfonso Iacovazzi , Sanat Sarda, Daniel Frassinelli, and Yuval Elovici, "DROPWAT: An Invisible Network Flow Watermark for Data Exfiltration Traceback", IEEE Transactions On Information Forensics And Security, Vol. 13, No. 5,Pp. 1139-1154, May 2018.
[9] Zhihong Tian, Yu Cui, Lun An, Shen Su, Xiaoxia Yin, Lihua Yin, And Xiang Cui, "A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus", Special Section on Novel Learning Applications and Services For Smart Campus, VOLUME 6, pp. 35355-35364 , June 12, 2018.
[10] Wenting Shen, Jing Qin, Jia Yu , Rong Hao, and Jiankun Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage", IEEE Transactions on Information Forensics And Security, Vol. 14, No. 2, Pp. 331-346, February 2019.
[11] D.J.E. Masvosvere, H.S. Venter, "Using a standard approach to the design of next generation e-Supply Chain Digital Forensic Readiness systems", Proceedings of Information Security South African (ISSA) 2015, Johannesburg, IEEE, Vol.107 (2), 104-120, June 2016.
[12] W.J.C. van Staden and E. van der Poel, "Using Automated Keyword Extraction to Facilitate Team Discovery in a Digital Forensic Investigation of Electronic Communications", Proceedings of Information Security South African, Johannesburg, IEEE, Vol.108 (2), pp. 45-55, June 2017.
[13] Haehyun Cho, Jeong Hyun Yi, Gail-Joon Ahn, "DexMonitor: Dynamically Analyzing and Monitoring Obfuscated Android Applications" IEEE Access, VOLUME 6, pp. 71229-71240, November 16, 2018.
[14] Farkhund Iqbal, Benjamin C. M. Fung, Mourad Debbabi, Rabia Batool, Andrew Marrington, "Wordnet-Based Criminal Networks Mining for Cybercrime Investigation", IEEE Access, VOLUME 7, pp. 22740-22755, January 9, 2019.
[15] Nickolaos Koroniotis, Nour Moustafa, Elena Sitnikova, "Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions", IEEE Access, Vol. 7, pp. 61764- 61785, May 14, 2019.

[16] Hadis Karimipour, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo, and Henry Leung, "A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids", IEEE Access, Vol. 7, pp. 80778-80788, May 31, 2019.
[17] Heloise Pieterse, Martin Olivier, and Renier van Heerden, "Evaluation Framework for Detecting Manipulated Smartphone Data", Springer International Publishing, Vol.110 (2), pp. 67-76, June 2019.
[18] Jiuxin Cao, Weijia Liu, Biwei Cao, Pan Wang, Shancang Li , Bo Liu, Muddesar Iqbal, "Social Relationships and Temp-Spatial Behaviors Based Community Discovery to Improve Cyber Security Practices", IEEE Access, VOLUME 7, pp. 105973-105986, July 30, 2019.
[19] Colin Urquhart, Xavier Bellekens, Christos Tachtatzis, Robert Atkinson, Hanan Hindy, And Amar Seeam, "Cyber-Security Internals of a Skoda Octavia vRS: A Hands on Approach", IEEE Access, VOLUME 4, pp.1-13, 2016.