Peertechz

ENGINEERING GROUP

TRENDS IN
Computer Science and Information Technology
OPEN ACCESS JOURNAL

ISSN: 2641-3086 DOI: https://dx.doi.org/10.17352/tcsit

Observational Study

A survey of machine learning applications in digital forensics

Hilmand Khan*, Sarmad Hanif and Bakht Muhammad

Department of Computer Science, CIIT, Islamabad, Pakistan

Received: 29 March, 2021
Accepted: 07 April, 2021
Published: 08 April, 2021

***Corresponding author:** Hilmand Khan, Department of Computer Science, CIIT, Islamabad, Pakistan, Tel: +923365272274; E-mail: hilmand90@gmail.com

Keywords: Access control management; P-DIFF; File fragment; Internet-of-things-dots; Convolution neural network

https://www.peertechzpublications.com

Check for updates

Abstract

We address the role of machine learning in digital forensics in this paper, in order to have a better understanding of where machine learning stand in today's cyber security domain when it comes to collecting digital evidence. We started by talking about Digital Forensics and its past. Then, to illustrate the fields of digital forensics where machine learning methods have been used to date, we recommend a brief literature review. The aim of this paper is to promote machine learning applications in digital forensics. We went through different applications of machine learning in different areas and analysed how machine learning can potentially be used in other areas by considering its current applications and we believe that the ideas presented here will provide promising directions in the pursuit of more powerful and successful digital forensics tools.

Abbreviations

ACM: Access Control Management; CNN: Convolution Neural Network; ML: Machine Learning; GPS: Global Positioning System; BSAF: Blockchain-assisted Shared Audit Framework; ODL: Optimal Deep Learning; IEHO: Improved Elephant Herd Optimization; API: Application Programming Interface

Introduction

Since the last decade of the 20th century, we witnessed a world-changing digital revolution. Mobile phones, Internet and many of the various digital technologies have become a part of our daily lives. At first, we were unaware of how significant those tools will be in the future but today they play an essential role in our daily lives and so do in our professional lives. This makes it obvious that most of our valuable information is going to be stored in digital form. In this age of Information Technology, the needs to change and enforce the laws are also changing. As a result, conventional crimes, especially those involving finance and commerce, are constantly evolving in response to technological advancements. In almost any investigation, a detailed analysis of computer systems and digital devices is becoming increasingly necessary in deciding the evidence.

This is where Digital forensic comes into the picture, to respond to law enforcement's clear and expressed needs in order to make the most of this emerging medium of electronic evidence, where machine learning can play a vital role by automating the time taking processes.

Digital forensics can be defined as a branch of forensic science dedicated to recover and investigate digital data. It is an evolving field that is always advancing to catchup with the changes in devices and how they are used for the identification, preservation, analysis, and recovery of data from computer systems and various other digital storages. The "Big digital forensic evidence" is today's major challenge for law enforcement agencies. The amount of data that needs to be analysed is rising all the time. A issue that needs to be solved is how to easily detect relevant file artefacts. In order to encourage further research in this field, we delve deeper into the role of machine learning in digital forensics applications in this paper, and provide an overview of the work already done in this direction.

Background

As a discipline, the study of cyber security started in the early 1970s. At the time, the discipline's approach was very strict, with a focus on the creation of theoretical models rather than the implementation of realistic implementations.

Citation: Khan H, Hanif S, Muhammad B (2021) A survey of machine learning applications in digital forensics. Trends Comput Sci Inf Technol 6(1): 020-024. DOI: https://dx.doi.org/10.17352/tcsit.000034

The work proposed by de Denning [1] is unquestionably one of the pillars of implementing machine learning in computer security.

Since then, a slew of new machine learning frameworks for computer security have been proposed [2], a real-time intrusion detection system having the capability to detect break-ins and penetrations by monitoring system audit records. The model also represented subject's behaviour with respect to object. There are numerous examples of effective machine learning applications in various computer security fields like the one proposed in [3] which clustered a network level behavioural malware by analysing malicious HTTP traffic for structural similarities. Since the first recorded internet-wide attack in 1988 (the "Morris Worm"), it has taken about 25 years of worldwide efforts (and multi-billion dollars) to get this far.

Literature review

Machine learning algorithms have been used in a number of fields. A variety of strategies for designing intelligent systems to solve various digital forensics problems have been proposed in the field of information security. Grillo et al. proposed a method for identifying machine users in order to make it easier to distinguish confiscated devices [4]. The method leveraged the habits of particular user, skills level, online interests and searches, etc. Following user profiling, five distinct types of users were identified: casual users, Internet chat users, office worker users, seasoned users, and hacker users. This method assisted in prioritising the examination of confiscated devices. which resulted in minimizing the analysis time as forensic examiners had to examine only potentially relevant hard drive. Metadata has also been used for automatic forensic analysis in recent years. Garfinkel and Rowe [5] defined an approach that uses (file name, extension, path, size, access and modification time, hash codes, status flag and fragmentation) on a large volume to identify anomalies and suspicions in a file artefact. In 2013, Raghavan and Raghavan [6] demonstrated the use of metadata associations to identify the origin of downloaded files. In 2020 Asaf Varol, et al. [7] explained the role ML can play and how it can be used in analysing large datasets and revealing criminal behaviour and criminal intents by learning from previous activities, and help in predicting future criminal intents. S. Baskar et al. proposed [8] Blockchain-assisted Shared Audit Framework (BSAF) for the analysis of digital forensics data in internet of things platform. The proposed work detected source/cause of data scavenging attacks in virtualized resources. Francisca, et al. [9] reviewed applications of ML in object detection and classification. Mohamed Alhoseni, et al. [10] proposed a new IoT-enabled Optimal-Deep-Learning based Convolutional-Neural-Network (ODL-CNN) to assist in the process of suspect identification. The Improved Elephant Herd Optimization (IEHO) algorithm was used to optimise the hyper parameters of the DL-CNN model.

A digital forensics framework

For smart settings: Abbas Acar, et al. (2019) presented a novel automated forensic system for intelligent environments [11]. Modifier (ITM) and Analyzer are the two key components of this system (ITA). The ITM examines smart applications in order to find forensically important data inside them. The smart apps are then instrumented by inserting complex logs that, at runtime, send the forensic data to a secure Database (ITD). And, in case of an investigation, the (ITA) applies data processing and machine learning techniques on the ITD data to acquire the overall status of the environment. In the first experiment, both time-dependent and time-independent user actions and forensic behaviours were inferred. Initial results proved the effectiveness of the framework and the work is still in progress.

Access control

Recently, the major cause of data theft and system compromises has been the misconfiguration of access control systems, as quantified in this report by security analysis [12] and demonstrated by the newsworthy incidents listed in Table 1.

One of the key features missing today in ACMs is System administrators may use continuous behaviour validation to ensure that a system is behaving as expected after changing configurations. It is never a one-time initiative, but rather a continual process of adapting policy to evolving aspects of data and resource sharing.

The following are some of the most common scenarios in which system administrators must adjust the access control policy to accommodate changes to users, data, features, or domains.

- User transition: Within an entity or project, new users can join, or current users may leave or change roles.
- Changes in data: Parts of the data can become sensitive or begin to contain sensitive information that must be shielded from users who previously accessed the data.
- New functions, accesses, or facilities are added for the general public or a certain community of users to use
- Domain reorganisation: Data must be reorganised into new domains or subdomains.

P-DIFF, a realistic method for inferring access control behaviour and adjustments from access logs [13], was introduced by Cindy Moore, et al. (2019). P-DIFF will support sysadmins with the following two vital tasks:

Table 1: Recent publicly-reported security incidents caused by access control misconfiguration.

Time	Incident	Orginazation
2017.6	198 million US voter records leaked [39]	Deep Root analytics
2017.7	14 million customer records leaked [42]	verizon
2017.9	Half million vehicle records leaked [28]	SVR Tracking
2018.2	119,000+ personal IDs exposed [29]	FedEx
2018.3	42000 patients information leaked [17]	Huntingtown hospital
2018.4	63551 patients information breached [16]	Middletown medical
2019.1	24 million financial records leaked [19]	Ascension
2019.9	20 million citizen records exposed [76]	Novaestrat

Citation: Khan H, Hanif S, Muhammad B (2021) A survey of machine learning applications in digital forensics. Trends Comput Sci Inf Technol 6(1): 020-024.
DOI: https://dx.doi.org/10.17352/tcsit.000034

- Change validation. When P-DIFF detects changes of access control behaviour, it alerts system administrators about the changes identified.
- Forensic analysis. P-DIFF can also monitor all of the changes in behaviour caused by a malicious access. This offers information about when and what improvements made the access possible. Which assists the post-mortem analysis upon a security incident, those clues can help administrators narrowing down the record they need to investigate.

P-DIFF was tested using data from five real systems, two of which were from industrial companies. PDIFF detected 86 percent–100 percent of rule changes with an accuracy of about 89 percent for shift validation. In 85 percent–98 percent of the analysed cases, P-DIFF can pinpoint the root-cause shift that makes the target access for forensic examination.

Automated metadata-based

Classification: One of the most discussed challenge in digital forensics is the ever-increasing data. The majority of the data on the confiscated computers is usually unrelated to the investigation. Finding a needle in a haystack is equivalent to manually extracting vital data and suspicious files.

Du, Xiaoyu, and Mark Scanlon (2019) proposed a system for prioritising suspicious file artefacts automatically [14]. Rather than presenting the final analysis outcome, the toolkit predicts and advises that an artefact is possibly suspicious. It employs a supervised machine learning method that draws on the results of previously processed instances. The paper covers feature extraction, dataset generation, training, and evaluation. And additionally, a data extraction toolkit from disk images is outlined, this makes it simpler to incorporate this approach into the traditional investigative process and have it function in an automated manner.

In summary, they suggested an automated digital forensic data processing technique for prioritising investigation file artefacts, and they validated the methodology using an example scenario. A toolkit for data extraction, dataset creation, and pre-processing was developed. As a result, the procedure can be carried out automatically during the investigation. And Analysed and discussed the proposed solution for accelerating the processing of large volumes of digital evidence.

File fragment classification

In digital forensics, file fragment classification is a crucial step. Traditional machine learning is used to extract features such as Ngram, Shannon entropy, and Hamming weights, which is the most widely used method. These characteristics, however, are insufficient to distinguish file fragments. Qing Liao, et al. (2018) suggest a new method based on fragment to grayscale image conversion and deep learning to retrieve more hidden features and increase classification accuracy [15]. The deep Convolution Neural Network (CNN) model can extract about ten thousand features using multi-layered feature maps and non-linear connections between neurons. On the public dataset, the model was trained and checked. During the experiments, a classification accuracy of 70.9 percent was obtained, which is higher than previous works.

To summarise, grayscale images and deep learning were used to enhance the classification accuracy of file fragments. The findings were compared to representative results from previous research, revealing that this approach was more accurate. This approach appears to be promising, and it is worth further refining the model and techniques as a potential project.

Deep-features for multiple

Forensic tasks: Deep learning research indicates that deep features can generalise to seemingly unrelated tasks in some cases. Owen Mayer, et al. (2018) created deep feature learning techniques that can be applied to a range of forensic tasks, such as image distortion detection and camera model recognition [16]. They devised two methods for constructing deep forensic features for this purpose:

1. A transfer learning approach requires moving features from one task to another.
2. A multitask learning strategy, in which a single function extractor is designed for multiple tasks at the same time.

The experimental performance was evaluated in numerous scenarios, and it was found that:

1. Camera model identification tasks generalise well to manipulation detection tasks, but learned features tasks from manipulation detection do not generalise well to camera model identification tasks, meaning task asymmetry.
2. Shallower features are more task-specific, while deeper features are more task-general, indicating a feature hierarchy.
3. It is possible to learn a single, coherent feature extractor that is highly discriminative of multiple forensic tasks.

Furthermore, the findings revealed that when training data is small, unified feature extractors outperform targeted CNNs. These findings illustrate a few key points to keep in mind when using deep feature-based approaches.

IOT dots

The idea of a smart environment has been enabled by the cooperative use of IoT devices and sensors, and in these smart settings, a massive amount of data is produced as a result of the interactions between devices and users and their day-to-day activities. Such data can provide useful information about incidents and activities taking place within the system, and if analysed, can assist in identifying and holding those who violate security policies accountable. However, prior smart app programming frameworks lacked forensics capabilities for identifying, tracing, storing, and analysing IoT data. IoTDots, a novel automated forensic system for a smart world such as smart homes and smart offices [17], was developed by Leonardo Babun, et al. (2018).

Citation: Khan H, Hanif S, Muhammad B (2021) A survey of machine learning applications in digital forensics. Trends Comput Sci Inf Technol 6(1): 020-024.
DOI: https://dx.doi.org/10.17352/tcsit.000034

IoT dots consists of two main components

1. IoTDots- Modifier.
2. IoTDots-Analyzer.

IoTDots- Modifier analyses smart app source code at compile time, detects forensic-relevant content, and inserts tracing logs automatically. The logs are then stored in an IoTDots database at runtime. The IoTDots-Analyzer then processes data and applies machine learning techniques to retrieve useful and usable forensic knowledge from the devices' operation in the event of a forensic investigation. IoTDots were tested in a realistic smart office environment with 22 devices and sensors.

Also considered were ten separate instances of forensic practises and behaviours from users, software, and computers. The evaluation results show that IoTDots can detect user behaviours with an average accuracy of over 98 percent and user, system, and application actions with an average accuracy of over 96 percent.

IoTDots output was found to have no overhead for smart devices and very little overhead for the cloud server. It's the first lightweight forensic approach for IoT devices, combining the collection of forensically relevant data from a smart environment with forensic analysis using data processing and machine learning techniques. The IoTDots is available online.

Machine learning in textual documents and e-mail forensics

During digital forensics research, textual records and e-mails are unquestionably a significant source of evidence. Authorship authentication and attribution are essential tasks when dealing with emails. Several studies have previously been proposed to solve this issue by studying the structure of an e-mail document (for example, e-mail headers, words, lines, and sentences, etc.) as well as linguistic trends (for example number of characters, occurrences of punctuation, vocabulary, etc) [18.]. With promising results, clustering algorithms and SVM were used. For example, in [19] When extracting the e-mails of three separate writers from 156 addresses, an accuracy of 84 percent to 100 percent was achieved. Other methods have been suggested for the study of any textual document, not just emails.

The development of successful digital forensics techniques is now aided by the introduction of text clustering methods. However, the topic of an ever-increasing number of text sources and the amount of confiscated devices has become increasingly important over time. Many studies have suggested that this problem needs to be addressed right away. Bandar Almaslukh (2019) presented a thorough overview of text-clustering approaches of digital forensic research and looked into the complexities of high volume data on digital forensic techniques. Furthermore, a useful classification and comparison of text clustering methods commonly used for forensic analysis were given. The main problems, as well as solutions and potential research directions, are highlighted to help researchers in the field of digital forensics in the age of big data. He also described possible future work in the field of forensic analysis using text clustering in the age of big data, such as validating text clustering on real-world and large-scale data, investigating the automated method for cluster labelling and bilingual clustering, and so on. Based on clustering strategies, similar works are categorised into fifth groups. SSOM, Kernel k-means and subject-based clustering, LDA, and benchmarking various clustering algorithms are the groups. In the last two groups, several clustering strategies in the sense of digital forensics are compared. The applicability of clustering techniques used in the literature to analyse a large volume of text data, on the other hand, is investigated.

Machine learning in network

Forensics: Network forensics is a technique for tracking down cyber criminals by analysing and tracing back network data. As a minimum, network traffic collection tools like Iris, Net Intercept, Net Witness, SoleraDS5150, and Xplico should be deployed. Network forensics entails examining network traffic for the purpose of detecting intrusion and determining how the crime occurred, i.e., setting up a crime scene for analysis and replays. The process model was introduced by Kaur P (2018), and it was compared to current network forensic process models and frameworks. In addition, the study problems at different stages were highlighted [20].

Network traffic classification is also important for network surveillance, security analysis, and digital forensics. The computational demands imposed by analysing all IP traffic flows are huge without correct traffic classification. The number of flows that need to be analysed and prioritised for review can also be reduced by classifying them. An automated feature elimination method based on a feature correlation matrix [21] is presented by Jan Pluskal (2018). They also suggested an improved statistical protocol recognition system, which was compared to Bayesian network and random forests classification methods and found to be accurate and perform well. Each classification method is applied to a subset of features that are most suitable for the method. The methods are judged on their ability to recognise application layer protocols as well as the applications themselves. The random forests classifier produces the most promising results, while the proposed improved statistical protocol recognition approach offers an interesting trade-off between higher efficiency and slightly lower accuracy, according to the experiments.

Conclusion

In this paper, we looked at some of the ways machine learning can be used in digital forensics. How machine learning techniques can be further used in Digital forensics to reduce the hard work and we explored those various techniques to show what to expect in the future from machine learning applications of digital forensics. Finally, we looked at the areas of digital forensics that needs our attention so that we work in those areas in order to secure our working environment in all aspects.

Citation: Khan H, Hanif S, Muhammad B (2021) A survey of machine learning applications in digital forensics. Trends Comput Sci Inf Technol 6(1): 020-024.
DOI: https://dx.doi.org/10.17352/tcsit.000034

Future work

Today there are many other areas in digital forensics that needs the application of machine learning to increase efficiency and effectiveness of the process. One such area is Cloud Forensics. Cloud infrastructure vomits a huge number of logs. We create Application Logs, Cloud Operations Logs, System Host Logs, Perimeter (VPN packet trace) Logs, CI/CD DevOps Build and Release logs, and 3rd party API access logs just by setting up a simple system.

Any interaction, access, or API call generates a log. A medium-sized infrastructure (say, 100 hosts across all environments) with reasonable commercial use (20,000 unique visitors per day) produces more than 20GB of logs per day. The method of evaluating and examining all of this is labor-intensive and vulnerable to error. We could no longer depend on humans, with their limited processing capacity and inflexibility.

Let's go back to a daily log volume of 20 GB. It's a massive amount of information. An operating infrastructure is almost always either anomaly-free or relatively anomaly-free. Unless we're training an algorithm to differentiate between anomaly-full and anomaly-free logs, anomaly-free logs are typically tedious.

Computers can and will examine the entire 20 GB of data every day. Humans are unable to do so. A computer system's learning accuracy would also improve over time. In operational defence, precision is the name of the game. Security data will grow, particularly in the cloud, where you can turn up unlimited capacity in exchange for money. Finding a needle in a haystack would be difficult. All of the information can be read by computers.

This is where machine learning, our sidekicks, and invaluable resources, can come in handy on a wide scale. Over the last ten years, the security industry has done an outstanding job of turning large data pipelines into massive data stores for analytics. However, we assume it is now time to conduct the actual analytics.

References

1. Bell DE, LaPadula LJ (1973) Secure computer systems: Mathematical foundations. Mitre Corp Bedford MA. Link: https://bit.ly/3fPT1rR
2. Denning DE (1987) An intrusion-detection model. IEEE Transactions on Software Engineering 222-232. Link: https://bit.ly/2OqgGUy
3. Perdisci R, Lee W, Feamster N (2010) Behavioral clustering of http-based malware and signature generation using malicious network traces. In NSDI 10. Link: https://bit.ly/3fKYMHz
4. Grillo A, Lentini A, Me G, Ottoni M (2009) Fast user classifying to establish forensic analysis priorities. In 2009 Fifth International Conference on IT Security Incident Management and IT Forensics. IEEE 69-77. Link: https://bit.ly/31TMOTG
5. Rowe NC, Garfinkel SL (2011) Finding anomalous and suspicious files from directory metadata on a large corpus. In International Conference on Digital Forensics and Cyber Crime. Springer, Berlin, Heidelberg 115-130. Link: https://bit.ly/3mBZRTz
6. Liao N, Tian S, Wang T (2009) Network forensics based on fuzzy logic and expert system. Computer Communications 32: 1881-1892. Link: https://bit.ly/3rTCOo1
7. Raina P (2021) A Privacy and Integrity Preserving Framework For Incorporating Intelligence In Digital Forensics.
8. Mohamed Shakeel P, Baskar S, Fouad H, Manogaran G, Saravanan V, et al. (2021) Internet of things forensic data analysis using machine learning to identify roots of data scavenging. Future Generation Computer Systems 115: 756-768. Link: https://bit.ly/39N2E6Q
9. Oladipo F, Ogbuju E, Alayesanmi FS, Musa AE (2020) The State of the Art in Machine Learning-Based Digital Forensics. Link: https://bit.ly/31UxLt8
10. Xiang C, Wu Y, Shen B, Shen M, Huang H, et al. (2019) Towards Continuous Access Control Validation and Forensics. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security 113-129. Link: https://bit.ly/2RebtjT
11. Babun L, Sikder AK, Acar A, Uluagac AS (2018) Lotdots: A digital forensics framework for smart environments. arXiv preprint arXiv:1809.00745. Link: https://bit.ly/3uyFut9
12. The Open Web Application Security Project. 2017. Jan. 2018. OWASP Top 10-2017: The Ten Most Critical Web Application Security Risks. Link: https://bit.ly/39OdF89
13. Xiang C, Wu Y, Shen B, Shen M, Huang H, et al. (2019) Towards Continuous Access Control Validation and Forensics. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security 113-129. Link: https://bit.ly/3cX3nVb
14. Du X, Scanlon M (2019) Methodology for the automated metadata-based classification of incriminating digital forensic artefacts. In Proceedings of the 14th International Conference on Availability, Reliability and Security 1-8. Link: https://bit.ly/2Oqh6u6
15. Chen Q, Liao Q, Jiang ZL, Fang J, Yiu S, et al. (2018) File fragment classification using grayscale image conversion and deep learning in digital forensics. In 2018 IEEE Security and Privacy Workshops (SPW) 140-147. Link: https://bit.ly/39P68WN
16. Mayer O, Bayar B, Stamm MC (2018) Learning unified deep-features for multiple forensic tasks. In Proceedings of the 6th ACM workshop on information hiding and multimedia security 79-84. Link: https://bit.ly/3mnku5G
17. Babun L, Sikder AK, Acar A, Uluagac AS (2018) Iotdots: A digital forensics framework for smart environments. arXiv preprint arXiv:1809.00745. Link: https://bit.ly/3cVSGIA
18. Iqbal F, Binsalleeh H, Fung BC, Debbabi M (2010) Mining writeprints from anonymous e-mails for forensic investigation. Digital Investigation 7: 56-64. Link: https://bit.ly/2PxFACt
19. De Vel O, Anderson A, Corney M, Mohay G (2001) Mining e-mail content for author identification forensics. ACM Sigmod Record 30: 55-64. Link: https://bit.ly/3wyLyU2
20. Kaur P, Bijalwan A, Joshi RC, Awasthi A (2018) Network forensic process model and framework: an alternative scenario. In Intelligent Communication, Control and Devices Springer, Singapore 115-130. Link: https://bit.ly/3dDKZQl
21. Pluskal J, Lichtner O, Rysavy O (2018) Traffic Classification and Application Identification in Network Forensics. In IFIP International Conference on Digital Forensics 161-181. Link: https://bit.ly/3rXQLBi

Citation: Khan H, Hanif S, Muhammad B (2021) A survey of machine learning applications in digital forensics. Trends Comput Sci Inf Technol 6(1): 020-024. DOI: https://dx.doi.org/10.17352/tcsit.000034