Surveying the Role of Machine Learning in Modern Digital Forensics Practices

VIJAYAVARMAN ARUNASALAM HARIKRISHNAN[1]
[1]Rochester Institute of Technology, Rochester, NY 14623 USA (e-mail: va7457@rit.edu)

ABSTRACT The increasing prevalence of cybercrimes and data breaches in the current digital age has elevated digital forensics in the cybersecurity landscape. The complexity and breadth of today's cyber threats often go beyond the capabilities of traditional forensic systems. Machine learning has become a powerful tool to close this gap and is transforming digital forensics systems. This paper provides an overview of the current state of research in the field and recent developments in this exciting confluence of digital forensics and machine learning. It aims to provide investigators and stakeholders with a deeper understanding of the critical role that machine learning plays in today's digital forensic investigations.

INDEX TERMS Digital Forensics (DF), k-Nearest Neighbor (k-NN), Machine Learning (ML), Support Vector Machine (SVM)

I. INTRODUCTION

Digital forensics, in simple terms, can be defined as the process of gathering, analyzing and preserving digital evidence. This information can be in any form of images, audio files, documents, etc. and can be from any device like computer hard drives, mobile phones, smart devices and other digital devices. The goals of digital forensics are evidence identification, criminal documentation, evidence collection and preservation, evidence packaging, and evidence transportation that does not involve deception.

A. CLASSIFICATION OF DIGITAL FORENSICS

The Department of Homeland Security of the United States has categorized digital forensics into five branches:

1) Computer forensics – Evidence found on computers and storage devices such as hard drives and flash drives is retrieved and stored.
2) Mobile device forensics – Digital evidence found on mobile and wearable devices, such as flash drives, fitness trackers and cell phones is captured and stored.
3) Network forensics – Analysis of logs to establish a link between network access and criminal activity.
4) Database forensics – Focuses on identifying, archiving, storing, replicating, analyzing and creating events that can have a negative impact on the integrity of the data.
5) Forensics data analysis – The purpose of forensic data analysis is to look for patterns in data that may indicate fraud, especially financial crimes.

B. CHALLENGES IN DIGITAL FORENSICS

The following are some of the key challenges of digital forensics:

1) **Large Data Volume** - In this digital era, with everyone having a smart device in their hand, the amount of data being generated is enormous which easily crosses gigabytes in a day. The data volume overwhelms the analysts and the investigators making it time-consuming and difficult to find evidence.
2) **Unpredictable Network Protocols** - The source IP, destination IP, MAC address, data packets, ports, email and every other detail can be modified and sent across a network. This makes it very difficult to pinpoint the exact IP or data packet to extract information with VPNs into the picture.
3) **Data Encryption** - With the focus on data security, every bit that is sent or received is encrypted. Encrypted data is often a hindrance for investigators, as they cannot directly access the content without decryption keys or passwords.
4) **Data Integrity** - It is essential to maintain the integrity of digital evidence. An alteration to evidence, whether accidental or intentional, may compromise its admissibility. Safeguarding the chain of custody is crucial.
5) **Non-compliance** - Sometimes, organizations or individuals will deny investigators access to their digital devices, servers, or systems, making it difficult for them to collect evidence. In addition, they may refuse to provide decryption keys for decrypting data. The destruction of data is also considered non-compliance.
6) **Cloud and Remote Data** - Data storage and cloud services have made accessing and preserving

evidence more difficult. Investigators must navigate legal and jurisdictional issues related to cloud data.

7) **Network and Cyberattacks** - As attackers use advanced techniques to conceal their identities and path- ways of entry, investigating network breaches and cyberattacks is complicated. Identifying the source of an attack can be difficult.

C. ROLE OF MACHINE LEARNING

Machine learning revolutionizes digital forensics by trans- forming the methods used to gather and examine digital evidence. By swiftly handling vast quantities of data, detecting patterns, and pinpointing irregularities, machine learning streamlines the investigative process. It plays a key role in data mining, allowing researchers to focus on the most relevant evidence, and it predicts and prevents cyber threats before they compromise the authenticity of the evidence. Its flexibility and ability to process a variety of data types from text to images makes it an invaluable tool for modern digital forensics and enhances the ability of investigators to solve complex cybercrimes.

D. ORGANIZATION OF THE PAPER

Section II of the paper discusses the various ML algorithms used in detail. It is followed by the various applications of the ML algorithms in different subdomains of Digital Forensics in Section III. The Future scope and the Conclusion are followed in Sections IV and V respectively.

II. MACHINE LEARNING TOOLS AND TECHNIQUES IN DIGITAL FORENSICS

This section is dedicated to describing some of the important machine-learning algorithms used in digital forensics [2].

A. SUPPORT VECTOR MACHINE

Support Vector Machine (SVM) is regarded as one the best and efficient technique in ML for cyber analysis. SVM is a supervised learning algorithm that aims to find a hyperplane that efficiently separates data points into classes. SVMs are robust and interpretable choice for various text classification and analysis tasks. It works by increasing the margin between adjacent data points (support vector). SVM is utilized for binary and multiclass classification tasks in digital forensics. It's particularly valuable for identifying patterns in data, such as distinguishing between benign and malicious files, or detecting attacks based on network traffic patterns.

B. THE K-NEAREST NEIGHBOUR

K-nearest neighbor (k-NN) is an unsupervised learning algorithm. k-NN is a straightforward algorithm that classifies data points by looking at the class of their k-nearest neighbors in the training dataset. It calculates the distance between data points and puts them into clusters of similar data points. Euclidean distance d (x, y) is most commonly used as the distance function. k-NN can be employed for clustering and classification tasks in digital forensics. For instance, it's useful in grouping similar files or identifying unusual user behavior by comparing it to the behavior of similar users.

C. NAÏVE BAYES CLASSIFICATION

Naïve Bayes is a probabilistic classification algorithm based on the conditional probability of a problem that calculates the probability of a data point belonging to a certain class based on its features, assuming independence between features. Naïve Bayes is applied in text and content analysis, making it highly efficient for tasks like spam detection, sentiment analysis, and email categorization in digital forensics.

D. DECISION TREE

A decision tree is a supervised learning algorithm for classification and regression applications. A decision tree breaks down a complex decision into simpler and interrelated decisions. These measures are presented as nodes and the relationships between them are presented as branches. At the end of each branch is a decision or prediction. Decision trees are useful in developing decision support systems in digital forensics. They help classify data, providing clear and interpretable insights into the decision-making process.

E. LOGISTIC REGRESSION

Logistic regression is a statistical technique specifically de- signed for making "yes" or "no" predictions. It helps deter- mine the likelihood of an event happening based on input variables. It does this by using the logistic function, which transforms data into a range between 0 and 1. Logistic regression is useful in digital forensics for tasks requiring binary choices. For instance, it can assist in determining the likelihood that a digital entity will be involved in a cyber incident. This simplifies the decision-making process in cyber investigations by evaluating different attributes linked to the entity and determining whether to proceed with a "yes" or "no" analysis.

F. POLYNOMIAL REGRESSION

Polynomial regression is a statistical method that helps us understand the connection between a target variable and other factors. It does this by using a polynomial equation with different powers of the factors. This approach is useful for handling complex, non-linear relationships in data. Polynomial regression is used in digital forensics to assess and forecast non-linear trends in data. Based on past data, it aids in comprehending and predicting future trends or behaviors, supporting trend analysis and well-informed decision- making.

G. HIDDEN MARKOV MODELS

Hidden Markov Models, or HMMs, are tools designed to analyze data sequences that hold hidden details. They function by transitioning between concealed states and making observations using probabilities. Essentially, they uncover patterns concealed within sequences. HMMs are used in digital forensics to analyze data sequences such as network traffic. These models aid in the deciphering of hidden states that correspond to different actions or behaviors. This makes it easier for investigators to identify abnormalities by helping them spot patterns or irregularities within the sequences.

H. ARTIFICIAL NEURAL NETWORKS

Artificial Neural Networks, known as ANNs, are complex systems built with interconnected layers of nods, inspired by the structure of the human brain. This work learns and adapts by processing data iterative, somewhat akin to how we learn from springs. ANNs are effective tools in digital forensics, used for a variety of tasks like data classification, malware detection, and picture analysis. Their ability to manage complex, non-linear interactions among data is what makes them so strong. They are excellent at identifying complicated patterns in digital data which makes them important when dealing with challenging issues in the field of digital forensics.

III. APPLICATION OF MACHINE LEARNING IN DIGITAL FORENSICS

This section elaborates the use of various Machine Learning algorithms and techniques in various Digital Forensics domain.

A. NETWORK FORENSICS

Network forensics is the process of collecting, analyzing, and interpreting digital information and network traffic data in order to investigate and respond to cybersecurity incidents. This subfield of digital forensics concentrates on analyzing network activity and communication to discover evidence of cyberattacks, data breaches, or malicious behavior. Organizations and law enforcement agencies use network forensics to comprehend attack methods, identify culprits, and prevent future incidents. [3]

Reference [11] talks about the use of k-NN and Naïve Bayes Algorithm for classification of network traffic to identify Denial of Service (DoS) attacks. The re- searchers have used the NSL-KDD and KDD Cup 99 as benchmark dataset in intrusion detection systems.

The authors devised their model with the dataset having 41 features, split into 70:30 proportion (training: test). They classified the attacks into four categories namely, "User to Root", "Root to Local", "DoS (Denial of Service attacks)", and "Probing at- tacks" with two behaviors “normal” and “attack”.

After running the model against k-NN and Naïve Bayes Algorithm, their results were compared using parameters like Accuracy, Recall, Precision, F-measure, Sensitivity, Specificity, Efficiency, Error rate and BCR values [Fig 1]. The performance of both algorithms in the classification and identification of anomalous traffic was determined with the use of the ROC curve. The ROC score for Naïve Bayes and k-NN was 0.97 and 0.99 respectively. The performance analysis of these two algorithms provides promising results and demonstrates that the use of ML in Network Analysis is efficient.

Sl. no	*Evaluation Parameter*	*KNN*	*Naïve Bayes*
1.	Accuracy	98.51	93.95
2.	Recall	97.8	95.54
3.	Precision	98.9	97.74
4.	F-measure	1.005	1.008
5.	Sensitivity	97.8	95.54
6.	Specificity	99.12	91.61
7.	Efficiency	98.48	93.95
8.	Error rate	1.50	5.27
9.	BCR	98.5	93.57

FIGURE 1. Features of performance evaluation

B. MOBILE FORENSICS

Mobile Forensics deals with recovering and preserving data from mobile phones. A structured

approach is always followed to recover, analyze and preserve the data without com- promising the integrity.

It begins with data extraction, where information like call logs, messages, and media is retrieved from the mobile device using specialized tools. Data preservation is crucial to maintaining evidence integrity and following established procedures. Subsequently, extracted data is analyzed to uncover pertinent information, such as communication records and app usage. Mobile forensics experts may also attempt to recover deleted data, as digital traces can persist. Decrypting and authenticating protected data is essential, sometimes re- quiring legal and ethical bypassing of security measures. The process culminates in a comprehensive report, documenting findings for use in legal proceedings or investigations.[5]

Reference [1] discusses about case study that talks about how ML provided accurate results in the analysis. A pedophile case study was taken into consideration. 21 mobile phone instances are utilized in the dataset; 2 of the phones belonged to non-pedophile users, and the other 19 were used by pedophile users. The outcomes demonstrate that the decision tree yields the most accurate outcomes.

Other examples talk about various papers where authors tried to perform disk analysis, file classification and file reconstruction using ML and they turned out to be good and efficient.

C. IOT FORENSICS

IoT forensics is a specialized field of digital investigation dedicated to handling cybercrimes and security incidents involving Internet of Things devices. It entails the collection, preservation, and analysis of digital evidence from IoT devices to uncover the nature of breaches, data compromises, or malicious activities. This involves scrutinizing device behavior, data recovery, analyzing network traffic, evaluating security protocols, and addressing the unique challenges posed by the diverse and resource- constrained nature of IoT devices. IoT forensics is be- coming increasingly crucial in a world where IoT devices are ubiquitous, helping in understanding, attributing, and mitigating security threats and privacy breaches.

Reference [4] discusses about a study that involved 41 IoT devices that looks at the prospect of using characteristics, independent of function or intent, to identify devices in a variety of contexts. The classification model employed logistic regression boosted with supervised ML (logitboost). Research has revealed that it is possible to classify devices into four groups with great performance and accuracy based on the traffic flow parameters of such devices.

D. CLOUD FORENSICS

Cloud forensics is the amalgamation of all the different forensics (i.e. digital forensics, network forensics, hardware forensics, etc.). It involves interactions among various cloud actors (i.e., cloud providers, cloud consumers, cloud brokers, cloud carriers, and cloud auditors) to facilitate both internal and external investigations. Legally it is multi-jurisdictional and multi-tenant situations. Cloud computing is the future. This paradigm offers significant economic benefits to the business entities. Due to this advancement, it has its challenges and threats which can jeopardize the business entity. Cloud computing has become a new battlefield for cyber- crime. To investigate these cases, we needed cloud forensics. [6]

Reference [9] talks about how ML was incorporated into an anomaly detection system in the cloud. On the technical end, several compute nodes running their custom Cloud Frame- work were used. A grid management system called JPPF was used for testing. The k-NN, Decision tree, and SVM algorithms were used and their results were documented. The k-NN with neighbor values five, six, and seven were tested[Fig 2]. It concluded that k-NN and Decision tree, provided with a small dataset performed well in terms of detecting anomalies. But SVM was a clear winner with accurate detection when provided with a large dataset.

E. SOCIAL MEDIA FORENSICS

Social media forensics is a specialized area of ‘digital forensics that focuses on tracing digital information, interactions, and activity on social media platforms. It involves collecting, analyzing, and storing digital evidence from social media accounts and posts to disclose legal, criminal, or investigative data, as well as other online activities. Social media forensics has an important role to play in resolving cases. Researchers use a variety of techniques and tools to analyze social media content, identify users, and analyze digital footprints to support regulatory or investigative efforts. [7]

Natural Language Processing Models (NLP) and Neural Networks are the best when it comes to text analysis and that is used here in Reference [8]. The unsupervised NLP model picks topics from blogs, mails, conversations and performs feature extraction using them. Reference [8] identified that Deep Neural Networks had better scope in social media analysis.

F. LINK ANALYSIS

Link analysis is a technique that examines and visualizes connections between entities, such as individuals, organizations, or data points. It involves using graphical representations, like network diagrams, to visually show relationships and associations among these entities. Patterns, trends, and potential insights can be unveiled through link analysis, which may not be immediately apparent in tabular data. It is widely used in areas like law enforcement, intelligence, fraud detection, and social network analysis to reveal hidden relationships and enhance decision-making. [10]

Machine learning (ML) can enhance link analysis by automating the process of identifying, categorizing, and analyzing links and entities in large and complex datasets. ML algorithms can assist in recognizing patterns and anomalies within the data, helping investigators or analysts uncover valuable information. ML has the capability to automatically classify relationships (e.g., familial, business, social) between entities, detect suspicious connections, or predict future links based on historical data. This automation and predictive capability provided by ML can significantly improve the efficiency and accuracy of link analysis in various domains.

G. CRIME ANALYSIS AND PREDICTION

Crime analysis and prediction using machine learning (ML) is a rapidly growing area in law enforcement and criminology. It uses ML algorithm data analysis to study historical crime data, identify patterns, and make predictions about future criminal activities. By analyzing various factors like location, time, and types of crimes, law enforcement agencies can allocate resources more efficiently, deploy personnel to areas with higher predicted crime rates, and ultimately work to prevent and address criminal activities more proactively. This innovative approach has the potential to enhance public safety and improve the effectiveness of law enforcement efforts.

Numerous machine learning methods, like random forests, naïve Bayes, and SVMs, might be useful in this process; however, the effectiveness of these algorithms will depend on how experienced the analyst is in data preparation.

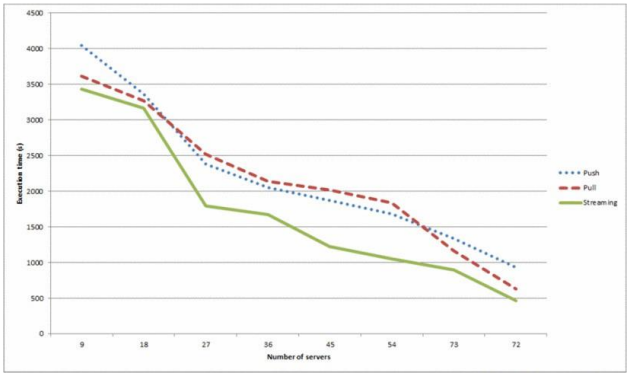

FIGURE 2. Running time on JPPF with 7 neighbors

H. MALWARE ANALYSIS

Malware analysis is the process of analyzing and disaggregating malicious software (malware) to understand its functionality, behavior, and potential impact. This study helps cybersecurity professionals and researchers identify malware patterns, identify vulnerabilities, and develop countermeasures. Machine learning (ML), which is widely used in malware analysis automates and accurately performs malware detection and classification. It plays a crucial role in defending against cyber threats, and developing countermeasures to protect computer systems and networks from malicious software. ML algorithms can be trained on large data sets known as malware samples to identify patterns and tendencies, making it easier to identify malicious MLs that were previously undetected.

The authors of [1] discovered that C4.5 and k-Neural Networks (k-NN) are the best algorithms for malware analysis after analyzing the static properties of portable executable binaries using several ML methods on the datasets VX Heaven and VirusShare. Similar to this, ML approaches are also used in [6] to analyze the incidence of static characteristic "opcode" in order to learn about unknown malwares. Among the techniques employed are Logistic Model Tree (LMT), Naïve Bayes Tree (NBT) RF, J48 Graft, and REPTREE. The best results were obtained with LMT, NBT, and J48 Graft.

IV. FUTURE SCOPE

The future scope of research in machine learning (ML) within digital forensics is promising and multifaceted, spanning various domains. In network forensics, ML can be harnessed to develop advanced intrusion detection systems, improving real-time threat identification. For mobile forensics, ML holds the potential to enhance data extraction and recovery techniques, especially in the context of encrypted and protected data on mobile devices. In IT forensics, ML can facilitate more efficient and accurate analysis of system logs and event data, aiding in the identification of security incidents. Cloud forensics research may lead to improved methods for detecting and mitigating complex cloud-based cybercrimes. Social media forensics could benefit from ML in identifying patterns of online behavior and uncovering hid- den connections within vast social networks. Link analysis and crime analysis and prediction are poised to become more data driven, enabling proactive measures against criminal activities. Finally, in malware analysis, ML can bolster the identification and classification of ever-evolving malware threats, leading to more robust cybersecurity practices.

V. CONCLUSION

To sum up, the incorporation of machine learning (ML) methodologies into numerous areas of digital forensics presents a viable approach to managing the always-changing terrain of cyber threats and illicit activities. The potential for machine learning (ML) to automate and improve the examination of digital evidence is obviously connected with the fu- ture of digital forensics research as explored across network, mobile, IT, cloud, social media, link, and criminal analysis in this paper. Researchers and practitioners in these fields can increase the accuracy of evidence extraction, anticipate criminal activity, and detect and respond to cybercrimes by utilizing the power of machine learning algorithms. Experts in machine learning and digital forensics working together will play a crucial role in influencing cybersecurity going for- ward, ultimately guaranteeing a safer and more secure digital environment. Our methods and instruments for countering the risks that come with technological improvements must also progress along with technology. The future lies in in- novation, as the combined strengths of machine learning and digital forensics will strengthen our position in the constantly changing field of digital security.

REFERENCES

[1] S. Qadir and B. Noor, "Applications of Machine Learning in Digital Forensics," 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2), Islamabad, Pakistan, 2021, pp. 1-8, doi: 10.1109/ICoDT252288.2021.9441543.

[2] A. M. Qadir and A. Varol, "The Role of Machine Learning in Digital Forensics," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116298.

[3] A. Tiwari, V. Mehrotra, S. Goel, K. Naman, S. Maurya and R. Agarwal, "Developing Trends and Challenges of Digital Forensics," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-5, doi: 10.1109/ISCON52037.2021.9702301.

[4] S. Rizvi, M. Scanlon, J. Mcgibney and J. Sheppard, "Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions," in IEEE Access, vol. 10, pp. 110362-110384, 2022, doi: 10.1109/ACCESS.2022.3214506.

[5] L. Peng, X. Zhu and P. Zhang, "A Machine Learning-Based Framework for Mobile Forensics," 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 2020, pp. 1551-1555, doi: 10.1109/ICCT50939.2020.9295714.

[6] M. R. Theertani, N. Valeti, D. Solanki and K. A. Kumar, "Applications of Machine Learning in Cloud Forensics," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 1-11, doi: 10.1109/ICSCSS57650.2023.10169719.

[7] B. Basumatary and H. K. Kalita, "Social Media Forensics - A Holistic Review," 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2022, pp. 590-597, doi: 10.23919/INDIACom54597.2022.9763129.

[8] V. Pawar and D. V. Jose, "Evidence Acquisition in Social Media for Cyber Crime," 2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP), Bengaluru, India, 2022, pp. 1-6, doi: 10.1109/CCIP57447.2022.10058653.

[9] A. Pătraşcu, M. -A. Velciu and V. V. Patriciu, "Cloud computing digital forensics framework for automated anomalies detection," 2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics, Timisoara, Romania, 2015, pp. 505-510, doi: 10.1109/SACI.2015.7208257.

[10] S. Rath, T. Das, I. Astaburuaga and S. Sengupta, "Less is More: Deep Learning Framework for Digital Forensics in Resource-Constrained Environments," 2023 11th International Symposium on Digital Forensics and Security (ISDFS), Chattanooga, TN, USA, 2023, pp. 1-6, doi: 10.1109/ISDFS58141.2023.10131803.

[11] A. V. Kachavimath, S. V. Nazare and S. S. Akki, "Distributed Denial of Service Attack Detection using Naïve Bayes and K-Nearest Neighbor for Network Forensics," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 711-717, doi: 10.1109/ICIMIA48430.2020.9074929.